AUTOMATED INSTALLATION
ENTRY (AIE) NEXT

SYSTEM PERFORMANCE SPECIFICATION

22 July 2022

Version 1

Product Manager Force Protection Services (PM FPS)
5900 Putnam Road
Fort Belvoir, VA 22060-5420

DISTRIBUTION STATEMENT C: Distribution authorized to the Department of Defense and U.S. DOD contractors only by specific authority of AR 380-5; and date of determination is the approval date of this document. This publication is required for administrative and operational purposes. Other requests for this document shall be referred to ATTN: SFAE-IEW-TF, Product Manager Force Protection Systems 5900 Putnam Road, BLDG 365 Fort Belvoir, VA 22060.

Intentionally Left Blank

PREPARED BY

LOMAN.STEPHEN.JOHN.1292909698 Digitally signed by LOMAN.STEPHEN.JOHN.1292909698
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=LOMAN.STEPHEN.JOHN.1292909698
Date: 2022.07.22 17:05:52 -04'00'

MAJ STEPHEN J. LOMAN Date
Assistant Product Manager – Automated Installation Entry
Product Manager, Force Protection Systems

REVIEWED BY

DONEY.MICHAEL.V.1228710608 Digitally signed by DONEY.MICHAEL.V.1228710608
Date: 2022.07.26 09:52:46 -04'00'

MICHAEL V. DONEY Date
Program Officer, Installation Physical Security Systems
Product Manager, Force Protection Systems

CONCURRENCE

BROOKER.CURTIS.ELLIOT.1255076767 Digitally signed by BROOKER.CURTIS.ELLIOT.1255076767
Date: 2022.07.27 17:27:04 -04'00'

CURTIS E. BROOKER Date
LTC, IN
Product Manager, Force Protection Systems

REVISION HISTORY

Version	Date	Revision History
0.1	28 May 2021	Preliminary Draft
0.2	14 Apr 2022	Verification Table
0.3	18 July 2022	OPMG Review

Table of Contents

1 INTRODUCTION

1.1. PURPOSE

The objective of the Automated Installation Entry (AIE) Program is to provide a cost-effective system that enhances security of Installation Access Control Points (IACPs), automates identity authentication and verification of authorized registered personnel entering the Installation, minimizes guard force requirements, maintains or increases pedestrian and vehicle throughput with enhanced security and allows for adaptation of increased authentication requirements at high threat levels.

AIE-3 consists of Fixed-Full (Tier 1) and Wireless Handheld configurations (Tier 2). Fixed-Full configuration is typically installed at large installations after the US Army Corps of Engineers (USACE) Access Control Point Equipment Program (ACPEP) site preparation is complete. ACPEP design is described in the Access Control Point (ACP) Standard and Standard Design document. The Handheld configuration is installed at small to medium sized installations that do not require the Fixed-Full configuration.

1.2. SCOPE

The AIE System will be installed at designated DoD/Army Installations and provide automated access control for vehicular traffic and pedestrians that have been enrolled in the system and are authorized access In Accordance With (IAW) the Department of Defense (DoD), Army and Installation Commander's policies. The system will be modular and scalable to allow future extensions to other security, access control and force protection systems. The system will be configured in a flexible architecture to support future upgrades through incorporation of technical insertions. The AIE System will be used at US Military locations in Continental United States (CONUS) and Installations Outside the Continental United States (OCONUS).

The system will be consistent with policy and strategic goals and objectives of Senior Commanders and Garrison Commanders/Installation Commanders/Facility Directors for Installation physical access control to:

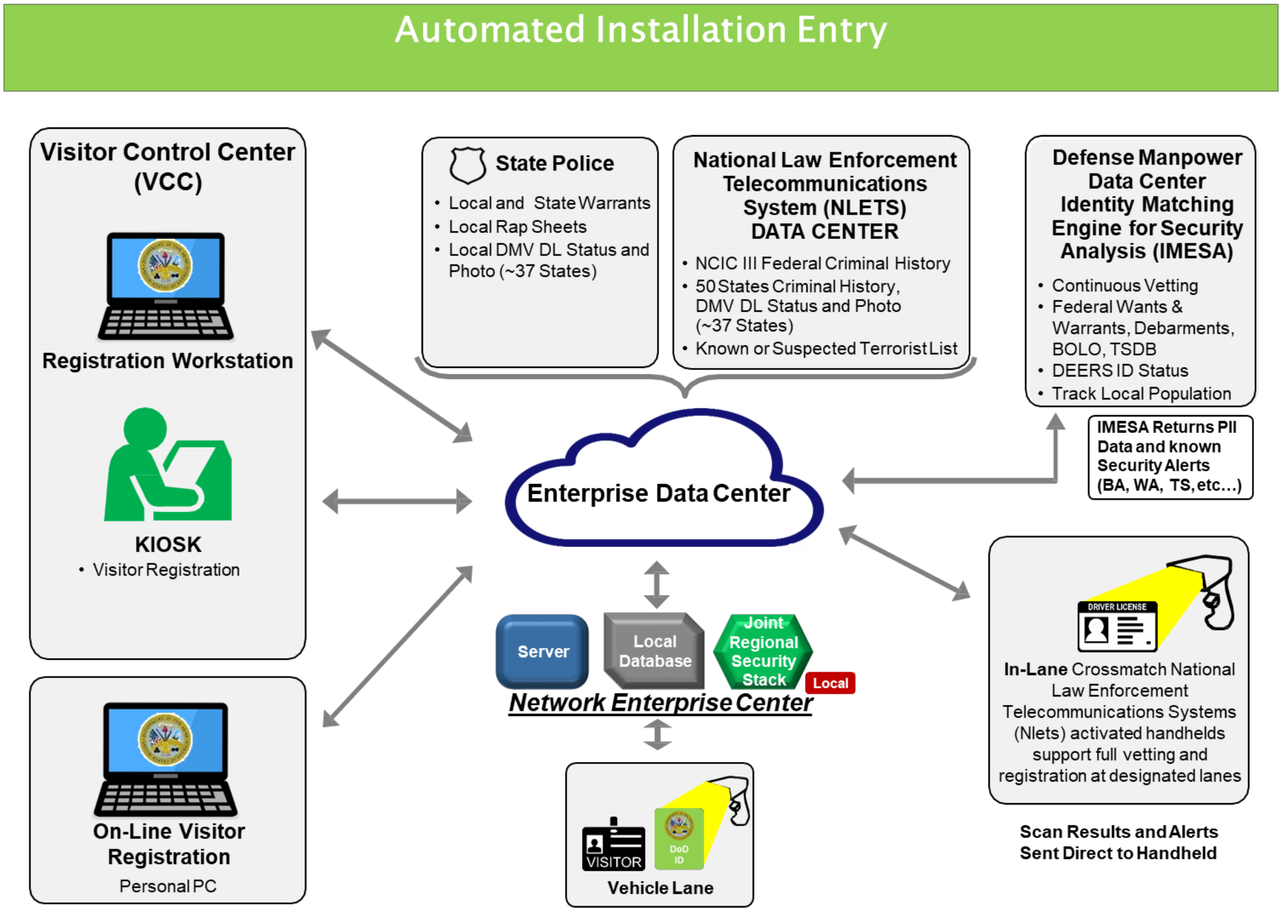
- Reduce risks to institutional missions;
- Minimize impacts to operational readiness by detecting potential Insider Threats; and
- Support enterprise-level resource planning, programming activities and Headquarters Department of the Army (HQDA) policy and program synchronization.

At the Installation level, Army security forces primarily consisting of Department of the Army Civilian Police (DACP), Borrowed Military Manpower

(BMM), and Department of the Army Security Guards (DASG), will use AIE at IACP locations (to include Visitor Control Center (VCC) operations) to:

- Maintain the local site population database;
- Make fitness-for-access determinations;
- Take appropriate actions in response to unfavorable fitness determinations resulting from the presence of derogatory information from authoritative Government databases (e.g., official personnel, industrial security, criminal justice information, non-criminal justice information data sources);
- Scan credentials (i.e., identification cards, driver licenses, etc.) to authenticate the identity and authorize access for individuals seeking Installation access;
- Report consistent Installation access control data and system use information.

The figure below represents the system concept and operational planning aspects for AIE solutions:


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
DRIVER LICENSE
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

2 APPLICABLE DOCUMENTS

2.1 GENERAL

The documents listed in this section are specified in section 3 of this specification. This section does not include documents cited in other sections of this specification or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements of documents cited in section 3 of this specification, whether or not they are listed here.

2.2 GOVERNMENT DOCUMENTS

2.2.1 Specifications, Standards and Handbooks

The following specifications, standards and handbooks of the exact revision listed below form a part of this specification to the extent specified herein.

FIPS PUB 140-3 Security Requirements for Cryptographic Modules, March 22, 2019

FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013

Copies of these documents are available online at http://quicksearch.dla.mil/qsSearch.aspx or from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094

2.2.2 Other Government Documents, Drawings and Publications

The following form a part of this specification to the extent specified herein. Unless otherwise specified, anomalies are cited in the solicitation or contract.

DoD Directive 8500.01, Cybersecurity, March 14, 2014 (Incorporating Change 1, effective October 7, 2019)

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014

DoDI 5200.08 CE-03, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), Incorporating Change 3, 20 November 2015.

DOD 5200.08 Volume 3, Physical Security Program: Access to DOD Installations, Change 1, September 18, 2020

DoD 5200.08-R, Physical Security Program, Incorporating Change 2, October 19, 2020

Army Access Control Points Standard Design, September 2020

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

Army Regulation 25-2, Army Cybersecurity, April 4, 2019

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

Army Regulation 700-127, Integrated Product Support, October 22, 2018

Criminal Justice Information Services (CJIS) Electronic Biometric Transmission Specification (EBTS) July 2, 2013

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F Information Assurance (IA) and Computer Network Defense (CND) February 9, 2011

Federal Highway Administration (FHWA), Manual on Uniform Traffic Control Devices for Streets and Highways Rev 2, May 2012

American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1 ANSI/ITL 1-2011 Updated 2015

Unified Facilities Criteria (UFC) 4-022-01, Security Engineering: Entry Control Facilities/ Access Control Points

Unified Facilities Criteria (UFC) 4-022-02, Change 1, Electronic Security Systems, 11 September 2019

2.3 NON-GOVERNMENT PUBLICATIONS

The following specifications, standards and handbooks of the exact revision listed below form a part of this specification to the extent specified herein. Unless otherwise specified, anomalies are cited in the solicitation or contract.

Identity Matching Engine for Security and Analysis (IMESA) Interface Control Document (ICD) 1.3v11

PM FPS Configuration Management Plan v4.1, June 4, 2020

2.4 ORDER OF PRECENDENCE

Unless otherwise noted herein or in the contract, in the event of a conflict between the text of this document and the references cited herein the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3 REQUIREMENTS

The Government has an active AIE Enterprise Data Center solution that stores user records locally and in the Cloud. The AIE-NEXT System shall utilize and build upon the existing AIE-3 hardware and software to maintain and build upon existing capabilities. The primary objectives are:

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

The System shall provide reliable and timely vetting and registration of personnel and automatic processing of vehicle and pedestrian traffic at Army ACPs throughout Continental United States (CONUS) and Outside Continental United States (OCONUS). System shall continue to interface and be operational from Installation to Cloud AIE Enterprise Data Center.

The System is intended to support Army physical security Installation access control needs for at least the next 10 years. System size, capacity, functionality and flexibility must be sufficient to support the growth and changing needs of the Army. Reference the diagram below for the notional AIE high-level functional architecture.

The System shall leverage a hybrid cloud solution of Network Enterprise Center (NEC) and enterprise Cloud. This approach will provide the ability for the Installation to continue to operate during the loss of external communications, as well as minimizing the total number and size of the servers on the Installation. The architecture will include a cache box for smaller Installations, and for larger Installations, deploy more robust Database/Domain Controller servers for continuity of operations**.** The larger Installation solution must be aligned to Army Directive 2016-38 to support technology to reduce data center footprint and Army's future Cloud initiatives**.**

3.1 REGISTRATION

Each AIE Installation operates a Visitor Control Center (VCC) utilizing AIE registration stations for registering users. Also, within the VCC are freestanding visitor kiosks that can register visitors. Visitors may Pre-Register using an online web-based capability prior to arriving at the VCC. AIE also provides Automatic and Visitor In Lane Registration (reference section 3.2.6) at the ACP lanes for specific individuals holding valid credentials. (See Appendix B for a list of authorized credentials.) Additionally, Portable Registration is used for remote registration of groups at pre-determined locations. During the registration process, the system collects unique personal identification information to include Name, photo, signature, fingerprint, Date of Birth (DOB), expiration date of credential, and unit of assignment. This information is used to vet the individual against authoritative databases and then register the user upon successful vetting into IoLS for continuous vetting.

3.1.1. Registration Process

3.1.1.1 The System shall perform verification of the user's (user is defined as personnel presenting credentials to gain access onto an Installation) credentials when the user presents a valid credential during visitor vetting and AIE registration. Verification will ensure the credential is valid by checking against authoritative databases.

3.1.1.2 The System shall vet DoD credentials against authoritative databases through IoLS including Defense Enrollment Eligibility Reporting System (DEERS), the local population database, NCIC Wants and Warrants, Terrorist Screening Database, and out to the Federal Bridge, and will populate registration fields without the operator having to re-key information.

3.1.1.3 The system shall vet visitor requests against NLETS, DMV, and State/local Government authoritative databases.

3.1.1.4 The System shall deny registration to personnel who receive negative results from authoritative databases and shall proceed with the registration process for those receiving positive results.

3.1.1.5 The System shall provide Administrator override capabilities to register personnel who have negative results from authoritative databases. The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication (PUB) 201 compliant credential for personnel access control during registration, vehicle lane operations and pedestrian portal operations.

3.1.1.6 The System shall be capable of reading information from a DoD Common Access Card (CAC), Department of Defense (DD) Form 2 (all types), DD Form 1173, DD Form 1173-1 and DD Form 2765 cards (for reserve and retired, uniformed services privilege card, dependent card and DoD privilege card), Defense Biometric Identification System (DBIDS), Uniformed Service ID (USID), Transportation Worker Identification Card (TWIC), Veteran Health Identification Card (VHIC), and verifying credentials with DEERS.

3.1.1.7 The System shall be capable of reading 1-D and 2-D bar-coded information issued by local Installations.

3.1.1.8 The System shall have the capability to limit locally issued credentials to access only Installations from which the credential was issued.

3.1.1.9 The System shall allow input at the time of registration of the Force

Protection Condition (FPCON) levels at which the individual is authorized to enter the facility.

3.1.1.10 The System shall be capable of identifying if individuals are allowed Trusted Traveler (TT) privileges IAW Army Regulation (AR) 190-13 and applicable Installation policies and regulations. The System shall include additional Trusted Traveler types as signified:

a. B – Presidential Appointee
b. H – Medal of Honor Recipient
c. K – Non-Appropriated Funds (NAF) Employee
d. V – Reservist/National Guard

3.1.1.11 The Registrar shall be capable of designating a user's TT privileges based on applicable Installation policies and regulations.

3.1.1.12 The System shall be capable of linking multiple approved credentials to an individual user Personal Information Record (PIR).

3.1.1.13 The System shall be able to identify classes of users. Classes of users include US Military (Active, Guard and Reserve), Foreign Military, Civilian Government Employee, Contractor, Dependent Resident, Survivor Access Card, Non-Resident and Retiree (Military and Government Civilian).

3.1.1.14 The System shall allow individuals to belong to more than one class of users.

3.1.1.15 The System shall be capable of querying user for input, allowing user to enter information and collecting credential information, digital photo, signature and fingerprint data for all registrants.

3.1.1.16 The System shall allow registration of individuals with names up to 30 characters for first, middle, and last name.

3.1.1.17 The System shall store all valid forms of identification for users. The System shall be able to electronically read an individual's driver's license or state issued identification card and display information embedded on the credential for the enrollment operator to visually compare and confirm against the data printed on the card.

3.1.1.18 The System shall provide a fully integrated capability for single sign-on for the registration station for registration activities.

3.1.1.19 The System shall have a portable registration station capability.

3.1.1.20 The System shall provide the capability for the registrar to select, from a list of all Installation ACPs and Pedestrian Gates, the ACP(s) and date/time that a user will be allowed to enter. Default configuration is access to all ACPs.

3.1.1.21 The System shall deny registration and visitor passes to personnel registering as visitors who receive negative results from authoritative databases and debarment lists and shall proceed with the registration process for those visitors receiving positive results.

3.1.1.22 The System shall electronically read and record information from an individual's passport, driver's license or state issued identification card into the System database and issue a visitor pass.

3.1.1.23 The System shall display captured information and populate fields required in a visitor pass.

3.1.1.24 The System shall allow the Registrar to manually enter and update user personal information into the Registration System including access denied and debarments.

3.1.1.25 The System shall electronically capture the signature of an individual and a digital photo for visual comparison with the signature and photo on the individual driver's license and store the signature and photo in the System database.

3.1.1.26 The system shall register the visitor into AIE and IoLS for continuous vetting.

3.1.1.27 The System shall generate long-term badges (plastic) and short-term visitor passes (paper) and allow Registrar to assign expiration date and time.

3.1.1.28 The System shall enable the unique enrollment of at least 5,000,000 (scalable up to 50,000,000) personal information records.

3.1.2. Visitor Control Center (VCC) Registration

3.1.2.1 The System shall provide a registration capability at the installation VCC staffed by approved registrars.

3.1.2.2 The System shall display information obtained from credentials along with a captured digital image of the credential holder to the enrollment operator.

3.1.2.3 The System shall be capable of reading fingerprints, recalling templates for each individual enrolled in the database and authenticating the individual's identity by their fingerprint with the registration database.

3.1.2.4 The System shall have the capability to accept no fingerprints and continue the enrollment process.

3.1.2.5 The System fingerprint collection subsystem shall conform to the Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000.

3.1.2.6 The System shall print a visitor pass (paper and plastic). The pass shall print at the VCC registrar printer per local policy.

3.1.3. Kiosk

3.1.3.1 The System shall provide a self-contained, freestanding self-service visitor kiosk solution for Installations that experience high visitor throughput rates. This system shall allow the user to complete the visitor request process within 2 minutes.

3.1.3.2 The System shall support an on-line integrated and automated registration kiosk for visitor requests made at a Visitor Center to increase registration throughput.

3.1.3.3 The System shall integrate with the existing AIE registration process to submit record, track, analyze and process visitor applications**.**

3.1.3.4 The System shall scan and read visitor identification credentials (REAL ID compliant driver's license, enhanced driver's license, or non-driver's identification card issued by a State, territory, possession, or the District of Columbia) including capturing the applicant's photo and entering additional information to complete the registration process This feature must be customizable to support changes in policy and guidance.

3.1.3.5 The System shall allow visitors to be verified for a one-day or long-term pass (8 day).

3.1.3.6 The System shall provide visitors to be re-issued a (one-time) paper pass with the original expiration date when the Visitor Pass or AIE badge is forgotten or lost.

3.1.3.7 The System shall print a visitor pass (paper and plastic). The pass shall print at the kiosk or VCC registrar printer per local policy.

3.1.3.8 The System shall provide the visitor with visual status display/printed information at the completion of the interaction, and/or instructions.

3.1.3.9 The System shall notify visitors of request status and other informational details.

3.1.3.10 The System shall keep a kiosk transaction log.

3.1.3.11 The System shall interface with the National Law Enforcement Telecommunications System (NLETS) to query visitor identification credentials against authoritative criminal justice information systems (National Crime Information Center – Interstate Identification Index (NCIC-III) and driver record databases. The NLETS interface shall also provide a primary and secondary communication path to NCIC-III in support of fitness determination decisions.

3.1.3.12 The System shall incorporate biometric authentication (facial recognition) methods to support identify proofing. Visitor credential vetting shall include Department of Motor Vehicle (DMV) checks. Photo from the DMV is compared to photo of the individual presenting the credential at the kiosk. List of acceptable credentials are below:

a. Common Access Card (CAC)
b. USID
c. Non-CAC local or Regional DoD Credential issued by the local Installation or region.
d. Non-CAC Local or Regional DoD Credential issued by another Installation or region. (ex. DBIDS).
e. REAL-ID compliant driver's license, enhanced driver's license, or non-driver's identification card issued by a State, territory, possession, or the District of Columbia
f. US Passport
g. Transportation Worker Identification Card (TWIC)
h. Veterans Health Identification Card (VHIC)
i. Federal Personal Identity Verification (PIV)

j. Non-Federal PIV-I

3.1.3.13 The System shall include anti-counterfeiting analysis of credentials such as driver's licenses and non-driver's identification cards. Example of anti-counterfeiting may include a combination of physical verification of the credential and electronic verification through DMV.

3.1.3.14 The System shall be capable of detecting a REAL ID-state compliant driver's license and request a second form of identification if not compliant. This feature must be customizable to support changes in policy and guidance.

3.1.3.15 The System shall print short-term visitor passes for visitors who successfully complete the visitor control process with an acceptable purpose and a duration <=8 days. The registrar shall receive denied access notification for further adjudication.

3.1.3.16 The System shall generate reports on kiosk usage data to support periodic and on-demand VCC reporting requirements. The reports shall include:

a. Number of registrants flagged for review due to facial recognition mismatches verified by the VCC agent.
b. Time required for a registrant to receive a visitor pass.
c. Total number of kiosk applicants by date and time (daily counts)
d. Total number of kiosk applicants denied a pass

3.1.3.17 The System shall re-issue visitor passes with the original expiration date when a user goes back to the kiosk to get a new pass that was lost/forgotten/stolen.

The Kiosk system shall automatically cancel the barcode of the previously issued pass when the new pass is issued.

3.1.3.18 The System shall send text messages or emails (online only) on pass application status (approvals, ready for pickup). Visitors are directed to contact the VCC upon denied access results.

3.1.3.19 The System shall provide the capability to print approved passes of online applicants that successfully complete the registration process when the applicant presents the credential at the kiosk.

3.1.3.20 The System shall interface with the online web registration solution that allows for administrative access to:

a. Customize the terms of service text on the kiosk
b. Customize the text messages/emails to visitor applicants
c. Customize reason for visit
d. View applications and revoke passes
e. Create transaction audit reports.

3.1.4. Online

3.1.4.1 The System shall provide a secure web-based visitor registration capability allowing visitors to submit a request for vetting and registration for a visitor pass via the internet.

3.1.4.2 The system shall integrate with the existing AIE registration process to submit record, track, analyze and process visitor applications.

3.1.4.3 The System shall provide the ability to route the request to a queue for the CJIS certified Registrar to submit for vetting.

3.1.4.4 The System shall notify the applicant when the process is complete and allow the applicant to print a paper pass upon successful vetting. Applicants who receive a negative vetting result shall be directed to contact the VCC.

3.1.4.5 The System shall allow the local system administrator to modify the Visitor Pass expiration date based on the Installation's Concept of Operations (CONOPS).

3.1.4.6 The system shall vet to NLETS for online registrations. Upon successful vetting results, the visitor shall be registered into the AIE database for continuous vetting and issued a visitor pass.

3.1.4.7 The system shall provide an administrative portal for AIE Installations to manage pre-registration settings.

3.1.4.8 The system shall query the visitor to confirm citizenship and allow the visitor to proceed to visitor request form to complete entry upon a positive response.

3.1.4.9 The system shall designate mandatory fields for data entry.

3.1.4.10 The system shall allow AIE Installations to designate sponsors.

3.1.4.11 The system shall allow designated sponsors to invite visitors.

3.1.4.12 The system shall provide for sponsored visitors to have their information validated by the sponsor before being submitted for background vetting.

3.1.4.13 The system shall include a Sponsor’s Certification Statement: “I certify that the applicant meets the justification requirements and that they require a PASS as indicated in order to perform assigned duties, conduct official business or visit family/friends. I understand my role as the sponsor and ensuring the PASS is retrieved upon expiration or prior to expiration if it is no longer required. If I fail to do so, my ability to be an approved sponsor can be removed.”

3.1.4.14 The system shall accept a valid Driver’s License (which complies with Public law 109-13 (The REAL ID Act of 2005)) and user profile information, if the visitor is a U.S citizen.

3.1.4.15 The system shall accept a valid Passport (passenger) and user information if the visitor is a U.S citizen.

3.1.4.16 The system shall require manual verification of pre-registration visitor information before being submitted for background vetting by CJIS certified personnel.

3.1.4.17 The system shall vet visitor request against NLETS, DMV, and State/local Government authoritative databases.

3.1.4.18 The system shall provide the capability for the site administrator to select a workflow that would upon successful vetting results, a) send a SMS (text Message) notification to the visitor to proceed directly to the gate and present their Driver License for the guard to scan, b) direct the visitor to come into the VCC for either a photo if one is not on the pass or verification of the pass, or c) print a pass. Upon negative vetting results, the visitor will be instructed to contact the VCC.

3.1.4.19 The system shall allow for up to six customizable reasons (Graduation, Hospital, MWR, Exchange/Comm, Work/Business, Other) for visit. If “Other” is specified as one of the reasons for visit, it shall require a specific reason to be entered of up to 30 characters. The reason selected shall allow the user to enter additional detail up to 30 characters.

3.1.4.20 The system shall allow each reason for visit to have a customizable pass duration of no longer than 8 days. The expiration date shall match the pass duration. Visitors should be directed to the visitor center registrar for long-term passes.

3.1.4.21 The system shall provide for a post-registration survey to capture visitor feedback and allow for survey report generation. The survey report shall be stored in the enterprise data center and provided as Dashboard report.

3.2 ACCESS CONTROL POINT (ACP)

The ACP is a corridor at military Installation entrances through which all vehicles and pedestrians must pass when entering or exiting the Installation. The ACP is responsible for the physical security and validation of all personnel entering DOD Installations. Although verification and access challenges may vary from one Installation to another, the AIE program establishes access control and validation processes that facilitate standardization of ACP operations. For Tier I, to accomplish ACP entry processing, vehicle lanes are equipped with several components to control credentials validation and vehicle movement. Lane traffic signals inform drivers which lanes are operating. A license plate camera, located on the rear of the traffic lane records a live image of the vehicle license plate. Vehicle Pedestals, located at each lane, contain intercom, CAC readers, barcode readers, gate arms, and driver cameras. The Intercom provides two-way audio communication between the vehicle lane, the remote monitoring station and ACP guards.

Tier 2 is a hand-held system without the installation of fixed-lane equipment while providing the full functionality of authentication of registered personnel. The primary benefit of the Tier 2 approach is to provide AIE capability to Installations not requiring the full Tier 1 capability to achieve a level of AIE capability consistent with their Installation’s entry control requirements.

3.2.1 Vehicle Lane Operations

3.2.1.1 The System shall read Federal PIV credentials during vehicle lane and pedestrian portal operations.

3.2.1.2 The System shall provide the System Administrator the capability to select the FPCON level.

3.2.1.3 The System shall provide the Operators the capability to configure the ACP and site using a selectable menu to increase the following access criteria for the

FPCON requirements: automatic registration, and Essential Personnel at any FPCON Level.

3.2.1.4 The System shall provide the capability to produce and display all reports for Installations and ACPs from the central monitoring workstation.

3.2.1.5 The System shall provide the capability for a FIPS 201 compliant wireless Handheld capable of reading PIV, PIV-1, CAC, DD Form 2, Defense Biometric Identification System (DBIDs), state driver's license, Veteran Health Identification Card (VHIC), Survivor Access Card, Transportation Worker Identification Card (TWIC) and displaying user data and image.

3.2.1.6 The System shall provide the capability for the wireless Handheld to operate continuously for 12 hours.

3.2.1.7 The Handheld device shall have a pistol grip.

3.2.1.8 The System shall provide the capability for digital/network video storage that allows transfer to removable media.

3.2.2 Tier 1

3.2.2.1 The System shall be capable of using fixed lane equipment and wireless handheld readers to perform credential verification functions at ACPs.

3.2.2.2 The System shall allow the operator from the Guard Booth or Gate House to switch to manual control of pedestrian and vehicular lane operations.

3.2.2.3 The System shall provide continuous digital/network video surveillance of pedestrian portal and vehicle lanes.

3.2.2.4 The System shall record digital/network video of all access control transactions that occur for 30 days and the ability to store 180 days of events requiring intervention.

3.2.2.5 The System shall provide simultaneous operation of pedestrian portal and vehicle lanes.

3.2.2.6 The System shall compare applicant information against the access denied list and display the result alerting gate guard when a denied individual attempts to gain access. The access denied list shall be automatically updated to each ACP upon status change.

3.2.2.7 The System shall prominently identify to the lane control guard whether the driver is allowed Trusted Traveler privileges.

3.2.2.8 The System shall prominently display information to the Gate House and Guard Booth for all events where vehicle operator information does not match with registered information or are invalid and the guard is prompted to manually check or stop the vehicle.

3.2.2.9 The System shall display descriptive information to the Guard Booth, Gate House and central remote location for all access denial events

3.2.2.10 The System shall provide an integrated traffic light (green, red).

3.2.2.11 The System shall provide a traffic hold capability that allows the Lane

Guard to hold all traffic and allow a vehicle to turn around.

3.2.2.12 The System gate arm shall not rise automatically, and traffic light remains red for drivers who are denied Trusted Traveler (TT) privileges.

3.2.2.13 The System shall be capable of lowering the traffic arm and shall take no more than one second in all required environmental conditions. Rising of the traffic arm shall take no more than three seconds in all required environmental conditions.

3.2.2.14 The traffic arm controller shall have a waterproof housing.

3.2.2.15 The traffic arm assembly shall be capable of manual override operation in the event of a malfunction due to mechanical failure, main power outage and/or backup power supply failure.

3.2.2.16 The traffic arm drive assembly shall be directly linked to the gear motor by a heavy-duty connecting rod. Override stops shall be provided to limit the gate arm travel in vertical or horizontal position and shall operate through 90 degrees.

3.2.2.17 The traffic arm assembly shall be capable of a minimum of 500 duty cycles per hour. The traffic arm assembly shall consist of a hollow aluminum, wood, steel or fiberglass material assembly with a minimum length of nine feet.

3.2.2.18 Each traffic arm shall be equipped with an obstruction detector that will automatically reverse the traffic arm motor when an obstruction is detected. The traffic arm shall be covered with retro reflective red and white sheeting. See FHWA SA-89-006 for proper orientation of sheeting.

3.2.2.19 The System shall digitally capture the front, driver and license tag of the vehicle.

3.2.2.20 The System shall provide the capability for archived video to be viewed at the Gate House and central monitoring workstation.

3.2.2.21 The System shall have the capability to login and display ACP transactions at the Gate House.

3.2.2.22 The System shall have the capability for ACP, lane and Pedestrian Portal monitoring and control at the Guard Booth.

3.2.2.23 The System shall have the capability at the Guard Booth and Gate House for selectable override control of all lanes and Pedestrian Portal per ACP.

3.2.2.24 The System shall have the capability for selectable override control of each ACP on the Installation at the central monitoring workstation.

3.2.2.25 The Tier 1 vehicle lane shall provide a minimum lane throughput of six authorized vehicles per minute.

3.2.3 Tier 2

3.2.3.1 The Tier 2 sites/ACPs/lanes shall be able to be upgraded to AIE Tier 1 sites/ACPs.

3.2.3.2 The System shall provide the capability for the wireless Handheld to operate continuously for 12 hours.

3.2.3.3 The Handheld device shall have a pistol grip, ruggedized casing, and protective shield over screen display.

3.2.3.4 The System shall provide the capability for a FIPS 201 compliant wireless Handheld capable of reading PIV, PIV-1, CAC, DD Form 2, Defense Biometric Identification System (DBIDs), state driver's license, VHIC, Survivor Access Card, Transportation Worker Identification Card (TWIC) and displaying user data and image.

3.2.3.5 The Tier 2 (handheld) vehicle lane operation shall provide a maximum response time of 2 seconds from credential scan to handheld display. This is for registered credentials and does not include in-lane registration.

3.2.4 Cellular Wireless

3.2.4.1 The System shall provide for a cellular access control point consisting of a cellular wireless bridge, firewall, Wireless Access Point (WAP), uninterruptible power supply (UPS), and associated cables. The cellular capability may be installed at a fixed location with insufficient communication infrastructure to support Tier 1 or Tier 2 configuration.

3.2.4.2 The System shall be capable of using First Net when available or other cellular service provider.

3.2.4.3 The System shall be able to maintain continuous connectivity.

3.2.4.4 The System shall provide a deployable cellular access control point in a pelican case with protective form containing one (1) each cellular wireless bridge, firewall, WAP, UPS, and associated cables.

3.2.4.5 The system shall be mobile, easily able to setup up and operational within 15 minutes.

3.2.4.6 The system shall be able to support wireless scanning, remote registration and emerging technologies (Facial Recognition).

3.2.5 Automatic and Visitor In Lane Registration

3.2.5.1 The System shall have the capability to allow CAC, Teslin card, and DBIDS holders to use their authorized credential to automatically register at both Fixed Full and Handheld vehicle lanes within <= 5 seconds.

3.2.5.2 The System shall have the capability to allow Driver’s License holders to use their authorized credential to vet and register at the Handheld vehicle lanes.

3.2.5.3 The System shall have the capability to allow the vehicle operator to present an authorized credential at the lane and retrieve the information from the CAC memory, 1D or 2D bar code and vet against authoritative databases.

3.2.5.4 The System shall have the capability to allow the vehicle operator to present an authorized credential at the lane, retrieve the information from the CAC memory, 1D or 2D bar code and vet against NCIC III.

3.2.5.5 The System shall provide the capability, upon positive vetting response, to query vehicle operator for photo if not provided via vetting process. This data will be stored with the user PIR data file.

3.2.5.6 The System shall deny registration for personnel who receive a negative response from vetting process.

3.2.5.7 The System shall display information obtained from credentials along with a captured digital image of the credential holder to the enrollment operator.

3.3 SERVER OPERATIONS

3.3.1 Enterprise Data Center

3.3.1.1 Cloud Server

3.3.1.1.1 The System shall leverage a hybrid cloud solution of Network Enterprise Center (NEC) and enterprise Cloud operations.

3.3.1.1.2 The System shall consist of enterprise data center server capability to support cloud-hosted operations for fixed full and handheld configurations.

3.3.1.1.3 The System shall have failover capability for high availability.

3.3.1.1.4 The System shall host all AIE user data.

3.3.2 Local

3.3.2.1 Large Server

3.3.2.1.1 The System shall support site ACP server installed in the NEC to support ACP operations at large size sites.

3.3.2.1.2 The ACP site server shall contain a copy of the site user data required for access.

3.3.2.1.3 The site ACP site server shall be installed in the NEC to support ACP operations at large size sites.

3.3.2.2 Cache Box

3.3.2.2.1 The System shall support site ACP Cache Box installed in the NEC to support ACP operations at small to medium size sites.

3.3.2.2.2 The Cache Box shall contain a copy of the site user data required for access.

3.3.2.2.3 The site ACP Cache Box shall be installed in the NEC to support ACP operations at small to medium size sites.

3.4 COMMUNICATION

AIE is an Information System Enclave. AIE fiber/network architecture/topology infrastructure shall be designed for CONUS-OCONUS installations by logical separation to maintain Information System enclave posture and gain necessary approvals from the U.S Army Network Enterprise Technology Command (NETCOM) and other DoD managed networks to integrate into each designated Army CONUS-OCONUS Installation site facility by logical separation to maintain Information System enclave posture. AIE enterprise network access to the NIPRNet will be IAW DoD and Army policy and guidance. Currently, access is via the network Top-Level Architecture (TLA)/ Joint Regional Security Stack (JRSS) managed by NETCOM and/or Joint Department of Defense entities (National Guard/US Army Corp of Engineers/ Joint Army-Air Force-Navy-Defense Information Systems Agency and any Non-Standard sites) to include computer network defense (CND) protection for AIE.

3.4.1 Interfaces

3.4.1.1 The System shall use standard communication protocols and communication links.

3.4.1.2 The System program software shall electronically connect with in-state and out-of-state law enforcement sources and local DMV databases.

3.4.1.3 The System program software shall electronically connect to the enterprise data center servers to transmit and receive user data

3.4.1.4 The System shall electronically connect to IoLS for access to authoritative databases.

3.4.1.5 The System shall request updates of user records through IoLS every 15 minutes.

3.4.1.6 The System shall provide the capability to selectively share access denied list/debarment lists with IoLS.

3.4.1.7 The System shall provide a local database that tracks the local population to support verification and security alerts obtained from the Continuous Information Management Engine (CIME) via IoLS. Note: Locals are defined as persons that fall under any of that fall under any of the following three categories:

a. Does not have a digital identity in DoD-wide DEERS;
b. Does not have a DoD ID card;
c. Does not have a DoD Electronic Data Interchange Personal Identifier (EDIPI).

Local persons include those non-DoD persons with credentials that can be federated to the DoD local access personnel that have not been issued a credential that can be federated and persons issued a local access card

3.4.1.8 The System shall provide the capability to electronically share local population information with other DoD and federal Systems.

3.4.1.9 The System program software shall electronically connect to in-state and out-of-state law enforcement and DMV data sources.

3.4.1.10 The System shall provide a web-based interface to support user database search for designated agencies. The information available to search shall include, but is not limited to, biographic and biometric identity information, credential information, physical access permissions information, security alert information, and access history ("scan" or "swipe" history) information. Such access shall be read-only.

3.4.1.11 The System shall implement Internet Protocol version 6 (1Pv6) on public facing servers and services providing for dual stack operations of IPv4 and IPv6 in parallel.

3.4.2 Infrastructure

3.4.2.1 The System shall provide a network architecture compliant with Army standard network communication guidance. (i.e. Joint Regional Security Stack (JRSS) Installation Campus Area Network (ICAN) modernization guidance)

3.4.2.2 The System shall establish system enclave utilizing Installation Network infrastructure only for transport purposes.

3.4.2.3 The System shall be designed to integrate with existing infrastructure and networks.

3.4.2.4 The System shall provide fiber optic cable from the ACP to the point of debarkation of Installation's fiber optic cable that is approximately 500 feet.

3.5 CYBERSECURITY

3.5.1 The System shall implement the National Institute of Standards and Technologies Special Publication (NIST SP) security controls prescribed in DoD Instruction (DoDI) 8510.01 Risk Management Framework for DoD IT, which are reflective of an overall security categorization as defined in Committee on National Security Systems Instruction (CNSSI) 1253, and AR 25-2, (CS) and display a privacy act statement at appropriate user interfaces.

3.5.2 The System shall implement system security measures sufficient to attain and maintain Authorization to Operate (ATO) IAW DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology, AR 25-2 and pamphlets and the Network Enterprise Technology Command (NETCOM) RMF: Assess and Authorize TIP dated 2 June 2016.

3.5.3 The System shall use secure encrypted communications over the NIPRNET network of at least AES-256.

3.5.4 The System shall encrypt data at rest IAW with DoD Policy Memorandum, "Encryption of Sensitive Unclassified Data At Rest on Mobile Computing Devices and Removable Storage Media," dated July 7, 2007, DoDI 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," dated April 24, 2007, as supplemented by ASD Nll/DoD CIO memorandum, same subject, dated June 2, 2006, DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," dated April 18, 2006.

3.5.5 The System shall ensure data concurrency of all System components among physical installations with secure network connectivity and be able to store encrypted data and eliminate duplicate information.

3.5.6 The System shall provide the capability to automatically install security patches IAW an approved DoD Patch Management Policies process utilizing Information Assurance Vulnerability Management (IAVM).

3.5.7 The System shall provide Host Based Security System (HBSS), per JTF-GNO CTO 07-12.

3.5.8 The System shall provide a hierarchical Organizational Unit (OU) structure that is adaptable and sustainable.

3.5.9 The System shall provide the capability to use PKI certificates (CAC logon) on workstations, servers and tools for managing, renewing, and revoking certificates and related services and support IAW DoD Policy for Public Key Infrastructure (PKI) and Public Key (PK) Enabling.

3.5.10 The System shall remain current with the latest Army Gold Master standard.

3.5.11 The System shall provide a secure operating environment IAW Defense Information System Agency (DISA) guidelines and standards.

3.5.12 The System shall provide WSUS, Solarwinds, and SPLUNK capabilities.

3.5.13 The System shall provide capabilities for monitoring/updating Information System & Environment Changes, performing Corrective Actions, updating Security Controls as needed, conducting periodic Security Control Assessments, conducting Remediation Actions, accomplishing Security Status Reporting and ensuring Risk Determination and Acceptance.

3.5.14 The system shall be configured and maintained IAW Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG).

3.5.15 The system shall utilize highest approved FIPS algorithm in place to encrypt all devices to include System logs.

3.5.16 The system shall be configured to use Secure File Transfer Protocol.

3.5.17 The system shall be configured and implement secure network implementation in accordance with DODI 8531.01 to include but not limited to support vulnerability assessment and analysis (network discovery, network and host vulnerability scanning, penetration testing).

3.5.18 The system shall implement Internal Network scanning and Monitoring/ update tools.

3.5.19 The system shall implement threat, vulnerability and attack notification, and take corrective action to mitigate potential vulnerabilities to the system and DODIN (Department of Defense Information Networks) as part of Comprehensive Vulnerability Management consisted with repeatable Vulnerability Management Process.

3.5.20 The system shall be configured and implemented IAW NIST 800-53, DoDI 8500.01, Cybersecurity, – DoDI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), – DoDI O-8530.1 “Support to Computer Network Defense (CND)”, – DoDI 8551.01, Ports, Protocols, and Services (PPSM).

3.5.21 The system shall be configured to comply with current and future Computer

Network Defense (CND) directives.

3.5.22 The system shall be configured IAW DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling and Public Key Encryption.

3.5.23 The system shall be configured to comply with DoD Network and Cyber Security TASKORDs, ARCYBER OPORDS, FRAGOs, CTOs.

3.5.24 The System shall be configured and ready to meet DOT&E requirement for Defense Business Systems such as Cooperative Vulnerability and Penetration Assessment (CVPA). A CVPA is an overt and cooperative examination of the system to identify all significant cyber vulnerabilities and the level of capability required to exploit those vulnerabilities. CVPAs are conducted in the intended operational environment with representative system operators, system/network administrators, and local cyber defenders present to assist the test team in their evaluation.

3.5.25 The system shall be configured to meet Adversarial Assessment (AA) Protect, Detect, React, and Restore (PDRR) requirements. AA evaluate the ability to protect the system/data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity.

**To provide operational impact and comprehensive PDRR data collection, both local and non-local network defenders should participate during the AA. Systems which include continuity of operations (COOP) in system’s Concept of Operations should include a COOP demonstration as part of the restore evaluation. The AA shall be conducted in concert with other operational testing but might require dedicated test time or assets that do not compete for time or resources with other operational test objectives. A CVPA and AA will normally be required as part of any operational test or assessment that supports a fielding decision.

3.5.26 The System shall be configured and maintained to meet Command Cyber Readiness Inspection (CCRI) with no or limited notice. The system is subject to any unscheduled inspections IAW DoD entity's cyber posture that includes a detailed assessment of its Information Assurance programs, the non-classified and classified IP networks, and the critical cyber and physical assets that support these networks.

3.6 SUSTAINMENT

Sustainment providers will support all product generations regardless of the final number of sites or locations. Components of AIE-3 will be designed for minimal operator maintenance. AIE sustainment provider maintenance service will include all on site field level maintenance, above basic operator maintenance tasks, and all sustainment level maintenance. AIE sustainment providers will determine if replacement of inoperative AIE system components is more economical than repair. Maintenance personnel will be certified in the maintenance and repair of the specific type of equipment installed and qualified to accomplish work promptly and satisfactorily. It is extremely important that AIE-3 equipment be repaired as rapidly as possible since it has the mission of protecting both personnel and highly sensitive assets.

3.6.1 Reliability, Availability, Maintainability (RAM)

3.6.1.1 The System shall provide Uninterruptible Power Supply (UPS) to supply power to the AIE System components in the event of power loss.

3.6.1.2 The System UPS shall operate in a climate-controlled environment to provide critical AIE System components with a minimum of 15 minutes operating power until emergency generators are operational.

3.6.1.3 The System UPS shall provide AIE critical system components with a minimum of six hours of power at Installations with no generator power. Critical components include: Site Server, ACP Equipment, Lane Equipment and Registration Systems.

3.6.1.4 The System (defined for RAM as one ACP with two vehicle lanes) shall be configured and installed to operate continuously and yield a Mean Time Between Failure (MTBF) of 1,440 hours. A failure is defined as a loss of System functional capability.

3.6.1.5 The System (one ACP with two vehicle lanes) shall be configured and installed to operate continuously and yield a Mean Time Between Critical Failure (MTBCF) of 10,000 hours. A critical failure is defined as a failure that renders a System unusable. The System cannot automatically validate or verify the credentials presented at the ACP.

3.6.1.6 The System (one ACP with two vehicle lanes) shall be configured and installed to operate continuously and yield an Operational Availability (A_o) of 97%. A_o is expressed as the Mean Time Between Downing Event (MTBDE) divided by the sum of MTBDE and Mean Down Time (MDT). MTBDE is the average time between events that bring the RAM System down, including failures, critical failures, preventive maintenance and training. MDT is the average total elapsed time to fully restore the RAM System to an operational state because of a downing event, including active maintenance time, logistics delay time and administrative delay time: A_o = MTBDE + (MTBDE + MDT)

3.6.1.7 The probability of the System granting entry to an unauthorized individual (false acceptance rate) shall be less than 0.1 percent.

3.6.1.8 The probability of the System denying entry to an authorized individual (false rejection rate) shall be less than 1.0 percent.

3.6.1.9 The System shall be designed such that a lane failure will result in the gate arm safely moving to the up position to enable manual entry.

3.6.1.10 The System shall allow for upgrades of hardware and software with minimal System disruption and cost.

3.6.1.11 The System shall maintain spares for all mission critical components that are readily available to field users.

3.6.1.12 The System components shall be designed to be maintained using commercially available tools and equipment. Components shall be arranged and assembled so they are accessible to maintenance personnel in order to perform operator level maintenance.

3.6.1.13 The System shall be designed to operate with no more than eight hours of initial or refresher training.

3.6.1.14 The Registration System shall have an A_o of 97% (the Registration System as defined for RAM shall be two Registration Workstations).

3.6.1.15 The Registration System shall be configured and installed to operate continuously and yield MTBF of 1,440 hours. A failure is defined as a loss of Registration System functional capability.

3.6.1.16 The Site Server System shall have an A_o of 97% (the Site Server System as defined for RAM shall consist of the Primary and Secondary Site Servers).

3.6.1.17 The Site Server System shall be configured and installed to operate continuously and yield MTBF of 1,440 hours. A failure is defined as a loss of Site Server System functional capability.

3.6.1.18 The System shall conduct a graceful shutdown in the event of power loss and automatically restart upon restoration of power.

3.6.2 Health and Status

3.6.2.1 The System shall provide a RAM analysis tool supporting current and future AIE sites that evaluates system help desk data to create dashboard data analytics, performance & process improvements, as well as a Dashboard map display

3.6.2.2 The RAM analysis tool shall generate cumulative and individual site Reliability, Availability, Maintainability, and Cost (RAM-C) Sustainment metrics providing the following:

a. Materiel Availability (A_m) - uptime of the total system population

b. Operational Availability (A_o) – a percentage of time that systems within an operating unit are operationally capable of performing an assigned mission.

c. Lifetime Operational Availability (A_o): Lifetime Operational availability measurement of the "real" average availability over the lifetime of a given AIE site, and includes all experienced sources of downtime, such as administrative downtime, logistic downtime, etc. The A_o percentage is calculated as Uptime (days) / Operating Life (Days).

d. “Snapshot" Operational Availability (A_o): "Snapshot" operational availability allows one to view A_o within a selected "window" of time. It enables one to change the operating cycle to a given month, week, etc. The calculation for "snapshot" A_o remains the same, but the operating cycle is variable based upon the user's input.

e. Mean Time Between Failures (MTBF): Time between failures under normal operations.

f. Mean Time Between Critical Failures (MTBCF): Time between critical component/system failures.

g. Reliability; Probability that the system will perform without failure over a specific interval, under specified conditions.

h. Average Ticket Age: This provides the average age (days) of every open ticket. This essentially speaks to how long tickets are "on-the-shelf" before being resolved.

i. Number of Tickets: This provides a count of all tickets at enterprise-and-site-levels.

j. Field Service Representative (FSR) Closure Rate: Provide relative "efficiency" of each FSR's performance. This number is calculated as # of Tickets Successfully Closed / # of Tickets Attempted for each FSR.

3.6.2.3 The System RAM analysis tool shall provide a dashboard that includes an AIE site hyperlink for identifying ticket status and color codes for identifying Full Mission Capable (FMC), Partially Mission Capable (PMC), and Not Mission Capable (NMC). The RAM tool shall provide for automated data updates every 24 hours

3.6.2.4 The System RAM analysis tool shall not be proprietary in nature and shall be a Commercial off the Shelf (COTS) solution.

3.6.2.5 The System RAM analysis tool shall provide a cost-effective, supportable, and integrated COTS software that enables all AIE users the ability to operate the tool using the same software baseline.

3.6.2.6 The System RAM analysis data shall be maintained at the enterprise level and made available via web services to designated personnel.

3.6.2.7 The System shall provide component and network monitoring capability indicating system performance. (i.e. Health and Status)

3.7 CONTROL AND MONITORING

The AIE-3 System will provide performance logging, performance monitoring, network monitoring, and central reporting to detect and diagnose system problems.

3.7.1 Dashboard

3.7.1.1 The System shall provide Dashboard Installation level reports and the roll-up of data to Dashboard.

3.7.1.2 The System shall provide the capability to produce and display all Installation reports from a central remote location.

3.7.1.3 The System shall provide a Public facing Dashboard in column header format that displays current totals of Registered Persons, DOD Credentials Registered, Visitor Credentials Registered, VHICs Registered, Survivor Access Cards, and Foreign Military Registered by Installation. The totals are updated monthly.

3.7.1.4 The System shall capture and display Installation performance dashboard metrics.

3.7.1.5 The System shall provide Initial Visitor Vetting and Registration dashboard, which displays In-Lane Registrations, In-Lane Vetting, In-Lane Denials, VCC Registrations, VCC Vetting, VCC Denials, Web Registrations, Web Vetting, Web Denials, Kiosk Registrations, Kiosk Registrations, Kiosk Vetting, Kiosk Denials, Total Registrations, Total Vetting, and Total Denials. This report only applies to visitors and excludes all DOD credentials registrations that rely on IoLS for verification.

3.7.1.6 The System shall provide the ability to display Vetting Denials by user category (CAC holders, Other DOD Credentials (Teslin cards), Visitors/Others (which includes VHIC holders)) and denial type (Terrorist Screening Database (TSDB) hit, Active warrants, Debarments).

3.7.1.7 The System shall display total hourly scan count by site, ACP, lane, and cumulative system total.

3.7.1.8 The System shall provide data filters on select fields including Date/Time ranges and Averages by site, ACP, lane, and cumulative system total.

3.7.1.9 The System shall provide the ability to manage system Interfaces, attributes, and frequency of information.

3.7.1.10 The System shall provide the system administrator the capability to manage user access to the dashboard including the assignment of user access controls and permissions.

3.7.1.11 The System shall be compatible with the latest version of the Army standard web browser and may include Internet Explorer, Edge, and Chrome.

3.7.1.12 The System shall provide hourly display updates.

3.7.1.13 The System shall provide the ability to capture and display active warrant/TSDB hits provided via Continuous vetting.

3.7.1.14 The System shall provide the ability to capture and display active warrant/TSDB hits provided via Initial Vetting.

3.7.2 Reporting

3.7.2.1 The System shall support Installation Access Control Data Reporting.

3.7.2.2 The System shall have the capability to generate and email a formatted report.

3.7.2.3 The System shall generate the following filterable formatted reports by name, date, and time:

a. All Denied History Report (by name combination, SSN, DOB, EDIPI, category type, and date/time);

b. All Visitor Pass Report (by name combination, SSN, DOB, EDIPI, category type, and date/time);

c. Individual Scan History (by name combination, SSN, DOB, EDIPI, category type, and date/time);

d. Registered Persons Transaction Report (by name combination, SSN, DOB, EDIPI, category type, and date/time)

e. ACP Scan/Transaction Report (by name combination, SSN, DOB, EDIPI, category type, and date/time)

f. Installation Scan Count Report (Installation/ACP/Lane/Handheld) (by total, category type, date, and time);

g. Escort Visitor Pass Report;

h. Personnel entered into debarment list (total, category type);

i. Handheld Report; and,

j. NCIC III transaction report including the FBI Number.

3.7.3 Video Management

3.7.3.1 The System vehicle lane digital/network video surveillance subsystem shall record from three fixed locations, overview, driver view, and the vehicle license plate.

3.7.3.2 The System vehicle lane digital/network video surveillance subsystem shall record the vehicle driver's face, during vehicle lane transaction, ranging from a height of 3ft. to 7ft. from the ground.

3.7.3.3 The System shall display a real time video or image to the lane control guard of the vehicle driver’s face.

3.7.3.4 The lane digital/network video surveillance subsystem shall provide 24 hour/7 day per week video imagery with the capability to store images for seven days and the ability to store 180 days of events requiring intervention.

3.7.3.5 The video surveillance system shall be viewable from the Central Monitoring Workstation with the ability to download or capture video for Law Enforcement actions.

3.7.3.6 The system shall allow video play/pause functionality for all cameras simultaneously during video playback.

3.7.3.7 The system shall provide video forward search speed up to 16x during playback.

3.7.3.8 The system shall provide video forward and backward frame by frame on playback and magnification (zoom) feature.

3.7.3.9 The system shall provide a multi-camera video export to a single file for use on a non AIE workstation.

3.7.3.10 The system shall provide Date/Time stamp on downloaded video footage on the video stream.

3.7.3.11 The system shall conform to industry standard for quick movement and slow motion video.

3.7.4 Data Mining

3.7.4.1 The System shall mine data to search, analyze and report data across the AIE enterprise for improvement opportunities in the following areas:

a. Trouble tickets for root cause patterns and trends and installations

b. Component (both HW and SW) issues and replacements for highest occurrence and consumption, and trends over time

c. Identify longest open trouble tickets and identify their common characteristics.

d. Analyze daily lane throughput at each ACP and Installation and identify trends and changes in traffic volume.

e. Analyze registration nodes to identify trends and usage.

f. Generate weekly Pareto charts to focus on highest occurring problem areas indicating need for process improvement.

3.7.5 Data Analytics

3.7.5.1 The System shall provide the following Installation Metric capabilities for the user to view and export:

a. Processing time between select system nodes for selected date and time frames for In-Lane Vetting and Registration, Kiosk Vetting and Registration, On-line Vetting and Pass Issuance, Visitor Center Workstation Vetting and Registration Processing Time, Handheld and Pedestal continuous evaluation processing time.

b. Total system transactions for selected date and time frames for In-Lane Vetting and Registration, Kiosk Vetting and Registration with issuing of Pass if successfully vetted, On-line Vetting and issuing of Pass if successfully vetted, Visitor Center Workstation Vetting and Registration Processing Time, Handheld and Pedestal.

c. Initial vetting Denials by user category (Contractors, U.S. Visitors, Family members, Foreign Visitors, Totals) and Denial type TSDB hit, Active Warrant, Debarments totals).

d. Number of National Crime Information Center – Interstate Identification Index (NCIC-III) Initial Vetting Granted vs. Denied by site and cumulative system total.

e. Vehicle scans by site, ACP, lane, and cumulative system total.

3.7.6 Artificial Intelligence

3.7.6.1 The System shall utilize artificial intelligence for the following:

a. Analyze network connectivity and identify trends, and alarm when parameters exceed normal values.

b. Analyze equipment breakage and replacement intervals and establish predictive maintenance intervals.
c. Analyze ACP throughput and alarm when normal values exceed.

3.8 SYSTEM CHARACTERISTICS

3.8.1 Safety

3.8.1.1 The System shall be safe to operate and maintain.
3.8.1.2 All System components shall be protected against the effects of lightning, power surges and stray electrical charges or emissions.
3.8.1.3 The System shall protect personnel against electrical shock.

3.8.2 Physical

3.8.2.1 The System shall operate using local commercial power.
3.8.2.2 The System shall use standard interface connectors for all computer processors and peripherals supporting the computer resources and will not require proprietary links, connectors or cables.
3.8.2.3 The System shall have non-proprietary interfaces.
3.8.2.4 The System components shall be interoperable, modular and scalable products that can be tailored to accommodate future hardware and software upgrades.
3.8.2.5 The System shall consist of commercial components.
3.8.2.6 The System computers shall be state-of-the-market.
3.8.2.7 The System shall provide nameplates for major components of the System.

Nameplates shall have the manufacturer's name, address, type or style, model, and serial number identified on the equipment. Nameplates shall be located on the equipment in an easily viewed location whenever possible.

3.8.3 System Design

3.8.3.1 The System shall be able to change within 5 minutes from one FPCON level to another for controlling vehicle and pedestrian access.
3.8.3.2 The System shall have the capability from selectable menu to change access criteria for FPCON levels.
3.8.3.3 The System shall be capable of identifying and removing duplicate PIR data for Registrants.
3.8.3.4 The System shall be able to immediately communicate PIR data to each ACP, each automated entrance lane to include Handhelds and the visitor center.

3.8.3.5 The System shall provide uninterrupted entry control processing despite loss of data connectivity from the network or site server.

3.8.3.6 The System shall be capable of recording, reporting and screen-printing of all System events on electronic media to include pedestrian and vehicle throughput Data.

3.8.3.7 The System shall provide pre-established reports and user-defined and user configurable formatting for all reports.

3.8.3.8 The System shall record date, time, location and identity of all personnel granted access in the access control events records.

3.8.3.9 The System shall store access control event records for 30 days. NCIC-III transaction records shall be stored for three years.

3.8.3.10 The System shall conform to National Fire Protection Association (NFPA) 70 standards.

3.8.3.11 The System shall be able to discriminate between individual switches, sensors, entry control devices and report status to the Network Management Workstation, central monitoring workstation and Registration Station.

3.8.3.12 The System will utilize a maximum of 60% of the provided computer memory, storage and computing speed.

3.8.3.13 The System shall be able to access the registration data of all other facilities within the AIE network.

3.8.3.14 The System shall provide remote monitoring and control of all ACPs from the central monitoring workstation.

3.8.3.15 The System shall have the capability to function with different configurations with the traffic light functioning; Gate Arm up and Gate Arm down; Automatic Registration, and Credential Only.

3.8.3.16 The System shall provide the capability to import an access Be On the Look Out (BOLO) denied list from a text file, Excel spreadsheet, or document format into the AIE System and vet against that list.

3.8.3.17 The System shall have the capability for all ACPs to be monitored and controlled at the central monitoring workstation on the Installation.

3.8.3.18 The System shall have the capability for the ACP Gate House, Guard Booth and central remote location to login to the System and use touch screen technology as needed to control/override ACP transactions.

3.8.3.19 The System shall provide the capability for all credential readers to be equipped with visual and audible feedback when credential is read.

3.8.3.20 The System should not register the same person more than once.

3.8.3.21 The System shall provide software installer packages.

3.8.3.22 The System shall provide the capability for the Guard Booth to monitor and control multiple (2) vehicle lanes using the AIE System.

3.8.3.23 The System shall provide the capability for platooning at the vehicle lane. Operations may consist of two guards with Handhelds controlling one lane or one guard with Handheld with the vehicle lane pedestal operational.

3.8.3.24 The System shall provide for a two-way intercom capability between the vehicle lane and Guard Booth at the ACP or the Gate House or central monitoring workstation. If the Guard Booth does not respond, the system shall rollover to the Gate House.

3.8.3.25 The System shall provide a Mobile Device Management (MDM) capability.

3.8.3.26 The Tier 2 sites/ACPs/lanes shall be able to be upgraded to AIE Tier 1 sites/ACPs.

3.8.3.27 The System shall implement version control for tracking changes to system components, source code, applications, to maintain site and system configuration.

3.8.3.28 The System shall automate unit tests, regression testing, functional tests, security scans, and deployment certification to the greatest extent possible.

3.8.3.29 The system shall be capable of bulk insertion of local debarment and Be On the Look Out (BOLO) lists.

3.8.4 Environmental

3.8.4.1 The System's exterior components shall be resistant to the effects of sand and be rated for continuous operation under harsh weather environments, chemicals and vapors sometimes present in the conduct of base operations and to the effects of chemicals used in winter road maintenance.

3.8.4.2 The System components, except the console equipment installed in interior locations having controlled environments, shall be rated for continuous operation under ambient environmental conditions of two to 50 degrees C (Celsius) dry bulb and 20 to 90 percent relative humidity and non-condensing.

3.8.4.3 The System console equipment, unless designated otherwise, shall be rated for continuous operation under ambient environmental conditions of two to 50 degrees C and a relative humidity of 20 to 80 percent.

3.8.4.4 The System components installed in interior locations having uncontrolled environments shall be rated for continuous operation under ambient environmental conditions of minus 18 to plus 50 degrees C dry bulb and 10 to 95 percent relative humidity and non-condensing.

3.8.4.5 The System components installed in exterior locations having uncontrolled environments shall be rated for continuous operation under ambient environmental conditions of minus 34 to plus 50 degrees C dry bulb and 10 to 95 percent relative humidity condensing.

3.8.4.6 The System components shall be rated for continuous operation when exposed to rain as specified in National Electrical Manufacturing Association (NEMA) 250, winds up to 137 km/hr and snow cover up to 610 mm measured vertically.

3.8.4.7 All exterior System components shall be operable in precipitation of up to two inches/hour.

3.8.4.8 All System components shall be operable in icing conditions.

3.8.4.9 All exterior components shall withstand exposure to solar ultraviolet radiation without performance degradation for a period of 10 years.

3.8.4.10 The System and equipment shall be sufficiently rugged to withstand handling in the field during operation, maintenance, supply and transport within the environmental limits specified for those conditions in the applicable hardware or system specification.

3.8.4.11 The System shall provide protective housing enclosures for interior electronics IAW NEMA 250 Type 12.

3.8.4.12 The System shall meet the requirements of the performance specification in all operational environments.

4 REQUIREMENTS VERIFICATION MATRIX

The requirements specified in Section 3 will be verified by the methods as listed in the following table, where D = Demonstration, I = Inspection, A = Analysis, and T = Test. Demonstration and test requirements shall be verified in a manner consistent with how the system will be used. (Reference AIE CONOPS and system architecture documents).

Section	Verification Method (D, I, A, T)
3.1.1.1	D
3.1.1.2	D
3.1.1.3	D
3.1.1.4	D
3.1.1.5	D
3.1.1.6	D
3.1.1.7	D
3.1.1.8	D
3.1.1.9	D
3.1.1.10	D
3.1.1.11	D
3.1.1.12	D
3.1.1.13	D
3.1.1.14	D
3.1.1.15	D
3.1.1.16	D
3.1.1.17	D
3.1.1.18	D
3.1.1.19	D

Section	Verification Method (D, I, A, T)
3.1.1.20	D
3.1.1.21	D
3.1.1.22	D
3.1.1.23	D
3.1.1.24	D
3.1.1.25	D
3.1.1.26	D
3.1.1.27	D
3.1.1.28	D
3.1.2.1	D
3.1.2.2	D
3.1.2.5	D
3.1.2.6	D
3.1.3.1	D
3.1.3.2	D
3.1.3.3	D
3.1.3.4	D
3.1.3.5	D
3.1.3.6	D
3.1.3.7	D
3.1.3.8	D
3.1.3.9	D
3.1.3.10	D
3.1.3.11	D
3.1.3.12	D
3.1.3.13	D
3.1.3.14	D
3.1.3.15	D
3.1.3.16	D
3.1.3.17	D

Section	Verification Method (D, I, A, T)
3.1.3.18	D
3.1.3.19	D
3.1.3.20	D
3.1.4.1	A/D
3.1.4.2	D
3.1.4.3	D
3.1.4.4	D
3.1.4.5	D
3.1.4.6	D
3.1.4.7	D
3.1.4.8	D
3.1.4.9	D
3.1.4.10	D
3.1.4.11	D
3.1.4.12	D
3.1.4.13	D
3.1.4.14	I
3.1.4.15	D
3.1.4.16	D
3.1.4.17	D
3.1.4.18	D
3.1.4.19	D
3.1.4.20	D
3.1.4.21	D
3.2.1.1	D
3.2.1.2	D
3.2.1.3	D
3.2.1.4	D
3.2.1.5	D
3.2.1.6	D
3.2.1.7	I
3.2.1.8	D
3.2.2.1	D

Section	Verification Method (D, I, A, T)
3.2.2.2	D
3.2.2.3	D
3.2.2.4	A/D
3.2.2.5	D
3.2.2.6	D
3.2.2.7	D
3.2.2.8	D
3.2.2.9	D
3.2.2.10	D
3.2.2.11	D
3.2.2.12	D
3.2.2.13	D
3.2.2.14	I
3.2.2.15	D
3.2.2.16	D
3.2.2.17	I/D
3.2.2.18	I
3.2.2.19	I
3.2.2.20	D
3.2.2.21	D
3.2.2.22	D
3.2.2.23	D
3.2.2.24	D
3.2.2.25	D
3.2.3.1	A
3.2.3.2	D
3.2.3.3	I
3.2.3.4	I/D
3.2.3.5	D
3.2.4.1	D
3.2.4.3	T
3.2.4.4	D

Section	Verification Method (D, I, A, T)
3.2.4.5	D
3.2.4.6	D
3.2.5.1	I/D
3.2.5.2	D
3.2.5.3	D
3.2.5.4	I
3.2.5.5	D
3.2.5.6	D
3.2.5.7	D
3.3.1.1.1	D
3.3.1.1.2	D
3.3.1.1.3	D
3.3.1.1.4	D
3.3.2.1.1	D
3.3.2.1.2	D
3.3.2.1.3	D
3.3.2.2.1	D
3.3.2.2.2	D
3.3.2.2.3	D
3.4.1.1	A/D
3.4.1.2	D
3.4.1.3	D
3.4.1.4	D
3.4.1.5	D
3.4.1.6	D
3.4.1.7	D
3.4.1.8	D
3.4.1.9	D
3.4.1.10	D
3.4.1.11	D
3.4.2.1	A/D
3.4.2.2	A/D
3.4.2.3	A/D

Section	Verification Method (D, I, A, T)
3.4.2.4	I
3.5.1	A/D
3.5.2	A/D
3.5.3	A/D
3.5.4	A/D
3.5.5	A/D
3.5.6	A/D
3.5.7	A/D
3.5.8	A/D
3.5.9	A/D
3.5.10	A/D
3.5.11	A/D
3.5.12	A/D
3.5.13	A/D
3.5.14	A/D
3.5.15	A/D
3.5.16	A/D
3.5.17	A/D
3.5.18	A/D
3.5.19	A/D
3.5.20	A/D
3.5.21	A/D
3.5.22	A/D
3.5.23	A/D
3.5.24	A/D
3.5.25	A/D
3.5.26	A/D
3.6.1.1	I
3.6.1.2	I/T
3.6.1.3	T
3.6.1.4	T
3.6.1.5	T
3.6.1.6	T

Section	Verification Method (D, I, A, T)
3.6.1.7	T
3.6.1.8	T
3.6.1.9	D
3.6.1.10	D
3.6.1.11	D
3.6.1.12	D
3.6.1.13	D
3.6.1.14	T
3.6.1.15	T
3.6.1.16	T
3.6.1.17	T
3.6.1.18	D
3.6.2.1	D
3.6.2.2	D
3.6.2.3	D
3.6.2.4	D
3.6.2.5	D
3.6.2.6	D
3.6.2.7	D
3.7.1.1	D
3.7.1.2	D
3.7.1.3	D
3.7.1.4	D
3.7.1.5	D
3.7.1.6	D
3.7.1.7	D
3.7.1.8	D
3.7.1.9	D
3.7.1.10	D
3.7.1.11	D
3.7.1.12	D
3.7.1.13	D
3.7.1.14	D

Section	Verification Method (D, I, A, T)
3.7.2.1	D
3.7.2.2	D
3.7.2.3	D
3.7.3.1	D
3.7.3.2	D
3.7.3.3	D
3.7.3.4	D/A
3.7.3.5	D
3.7.3.6	D
3.7.3.7	D
3.7.3.8	D
3.7.3.9	D
3.7.3.10	D
3.7.3.11	D
3.7.4.1	D
3.7.5.1	D
3.7.6.1	D
3.8.1.1	A/D
3.8.1.2	A
3.8.1.3	A
3.8.2.1	I
3.8.2.2	I
3.8.2.3	I
3.8.2.4	I
3.8.2.5	I
3.8.2.6	I
3.8.2.7	I
3.8.3.1	D
3.8.3.2	D
3.8.3.3	D
3.8.3.4	D
3.8.3.5	D
3.8.3.6	D

Section	Verification Method (D, I, A, T)
3.8.3.7	D
3.8.3.8	D
3.8.3.9	A/D
3.8.3.10	A
3.8.3.11	D
3.8.3.12	D
3.8.3.13	D
3.8.3.14	D
3.8.3.15	D
3.8.3.16	D
3.8.3.17	D
3.8.3.18	D
3.8.3.19	D
3.8.3.20	D
3.8.3.21	D
3.8.3.22	D
3.8.3.23	D
3.8.3.24	D
3.8.3.25	D
3.8.3.26	D
3.8.3.27	A
3.8.3.28	D
3.8.3.29	D
3.8.4.1	A
3.8.4.2	A
3.8.4.3	A
3.8.4.4	A
3.8.4.5	A
3.8.4.6	A
3.8.4.7	A
3.8.4.8	A
3.8.4.9	A
3.8.4.10	A

Section	Verification Method (D, I, A, T)
3.8.4.11	I
3.8.4.12I	D

5 DEFINITIONS

Access Control Point	Generally, a corridor at the Installation entrance through which all vehicles and pedestrians must pass when entering or exiting the Installation. For the purposes of this document, an ACP can be located within the Installation perimeter to provide access control to an area within the Installation. The perimeter of the ACP consists of both passive and active barriers arranged to form a contiguous barrier to pedestrians and vehicles.
Authentication (of credentials)	The process of ensuring that the presented credential exists in the registration database, generally performed when the user enters the lane.
Authoritative Source	A database or other information source that contains the definitive information of its kind and is maintained by an authorized Government entity. Examples include the DEERS database for DoD employee and CAC holders, and the NCIC for federal criminal information. A state database might be an authoritative source for state-level criminal information. An Installation can be an authoritative source for locally issued credentials.
Automated Lane	A lane at an Access Control Point that has the AIE System installed and operating.
Civilian	An individual not in the US Military.
Credentials	A form of identification used to uniquely identify an individual.
Credential Reader	A device used to read a presented credential.
Dependent	An individual who is supported by a person on active duty.
Enrollee	A user that is allowed access privileges onto an Installation.
Manual Lane	A lane at an Access Control point that does not have the AIE System operating. The lane could have the AIE system installed, but not in use.
Operator	A staff member who directly interfaces with the system to support users, such as a security guard or registration staff.
Wireless Handheld Configuration	A system configuration that provides the ability for the system to be deployed in an expedited schedule that has a set of capabilities that are less than the Fixed- Full system.

	Individual requirements annotated with "Handheld" are part of the minimum set of requirements for the Handheld configuration.
Installation	A Military base or other location.
Trusted Traveler	A program that allows Uniformed Service member, Government Civilian and designated personnel with a valid CAC, driver's license and clear NCIC check, to present their credential for automated authentication while simultaneously vouching for vehicle occupants.
User	A customer of the AIE System who uses the AIE System to gain access onto an Installation.
Vetting (of credentials)	The process of verifying that the presented credential is valid, usually against an authoritative source, and generally performed at time of registration.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

-A-

ACP	Access Control Point
ACPP	Access Control Point Program
ACS	Access Control System
ACWG	Access Control Working Group
AES	Advanced Encryption Standard
AIE	Automated Installation Entry
AIT	Automated Identification Technology
A_O	Operational Availability
AR	Army Regulation
ASIOE	Associated Support Items of Equipment

-B-

-C-

CAC	Common Access Card
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operating Picture
CPC	Corrosion Prevention and Control

-D-

DA	Department of the Army
DBIDS	Defense Biometric Identification System
DEERS	Defense Enrollment Eligibility Reporting System
DIAC	Defense Installation Access Control
DISA	Defense Information Systems Agency

DOB	Date of Birth
DoD	Department of Defense
DSS	Decision Support System
DVR	Digital Video Recorder

-E-

EOSH	Environmental Occupational Safety and Health
EM2P	Emergency Management and Monitoring Program

-F-

FITS PUB	Federal Information Processing Standard Publication
FOC	Full Operational Capability
FP	Force Protection
FPCON	Force Protection Condition

-G-

GIDEP	Government Industry Data Exchange Program

-H-

HSPD-2	Homeland Security Presidential Directive - 12

-I-

IAVM	Information Assurance Vulnerability Management
ICIDS	Integrated Commercial Intrusion Detection System
ID	Identification
IMESA	Identity Matching Engine for Security and Analysis
IoLS	Interoperability Layer Service
IPT	Integrated Product Team

-J-

JOpsC	Joint Operations Concepts

-K-

-L-

LAN	Local Area Network
LORA	Level of Repair Analysis
LRU	Line Replaceable Unit

-M-

MDT	Mean Down Time
MTA	Maintenance Task Analysis
MTBDE	Mean Time Between Downing Event

-N-

NCIC	National Crime Information Center
NET	New Equipment Training
NIPR Net	Non-secure Internet Protocol Router Network
NLETS	National Law Enforcement Telecommunications Network

-O-

OCONUS	Outside the Continental United States

-P-

PAC	Physical Access Control
PM FPS	Product Manager, Force Protection Services

PHS&T	Packaging, Handling, Storage, and Transportation
PII	Personal Identifiable Information
PIL	Preferred Items List
PIN	Personal Identification Number
PIR	Personal Information Record
PMCS	Preventive Maintenance Checks and Services
PSE	Physical Security Equipment

-Q-

-R-

-S-

S&I	Standardization and Interoperability
SCOM	System Center Operations Manager
SoS	System of Systems
SSA	Supply Support Activities
SSN	Social Security Number

-T-

TM	Technical Manual
TMDE	Test, Measurement, and Diagnostic Equipment
TPF	Total Package Fielding
TSDB	Terrorist Screening Database
TWIC	Transportation Workers Identification System

-U-

UPS	Uninterruptible Power Supply

-V-

VCC	Visitor Control Center
VHIC	Veteran Health Identification Card

-W-

WAP	Wireless Access Point

-X-

-Y-

-Z-

APPENDIX B – LIST OF AUTHORIZED CREDENTIALS

Credential Usage						
Authorized Credentials	**FIPS 201 Compliant**	**Use at Registration**	**Vetting**	**Auto Registration at Lane**	**Use at Lane**	**Vet to IoLS at the lane**
PIV	x	X	NCIC III Debarment List State & Local criminal justice agency DMV		x	
PIV-I	Not compliant	X	NCIC III Debarment List State & Local criminal justice agency DMV		x	
NFI PIV-I	Not compliant	X	NCIC III Debarment List State & Local criminal justice agency DMV		x	
CAC	x	x	IoLS Debarment List	x – authenticate & register if not in system	x	x
DD Form 2A (active duty)	Not compliant	x	IoLS Debarment List	x – authenticate & register if not in system	x	x
DD Form 2 (armed forces Geneva convention)	Not compliant	x	IoLS Debarment List	x – authenticate & register if not in system	x	x

Credential Usage

Authorized Credentials	**FIPS 201 Compliant**	**Use at Registration**	**Vetting**	**Auto Registration at Lane**	**Use at Lane**	**Vet to IoLS at the lane**
DD Form 2S	Not compliant	x	IoLS Debarment List	x – authenticate & register if not in system	x	x
DBIDS	Not compliant	x	IoLS Debarment List		x	
Passport	Not compliant	X (accepted at VCC)	NCIC III Debarment List State & Local criminal justice agency DMV			
State issued Driver's License	Not compliant	x	NCIC III Debarment List State & Local criminal justice agency DMV	x	x	
TWIC	Not compliant	x	NCIC III Debarment List State & Local criminal justice agency DMV		x	
State issued ID	Not compliant	x	NCIC III Debarment List State & Local criminal justice agency DMV			
Veteran Health Identification Card (VHIC)	Not compliant	x	NCIC III Debarment List State & Local criminal justice agency DMV		x	