AUTOMATED INSTALLATION ENTRY (AIE) NEXT

CONCEPT OF OPERATIONS (CONOPS)

2 March 2022

Version 1

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

THIS PAGE INTENTIONALLY LEFT BANK

TABLE OF CONTENTS

List of Figures

STATUS/REVISION HISTORY

Date of Issue	Version Description	Version Number
18 Jan 2022	Release for AIE Next Solicitation	1

THIS PAGE INTENTIONALLY LEFT BANK

1. INTRODUCTION

1.1 Purpose

This Concept of Operations (CONOPS) describes the Automated Installation Entry (AIE) capability for US Military Installations in meeting access control requirements. It defines AIE operational concepts that will enhance Installation security and Force Protection (FP) while reducing troop-to-task functions and streamlining authentication and verification of personnel entering US Army Installations.

1.2 Scope

The scope of this CONOPS is limited to Contractor and Government activities involved with development and implementation of AIE capabilities. This CONOPS provides guidance for all Army Major Commands, subordinate commands, defense agencies and contractor entities operating AIE.

1.3 Background

Homeland Security Presidential Directive - 12 (HSPD-12), signed by President George W. Bush on 27 August 2004, mandated implementation of a Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). In November 2005, the Access Control Working Group (ACWG), a standing sub-committee of The Department of the Army Physical Security Review Board, was convened to establish operational requirements for implementation of the AIE Program. As a direct result of this initial meeting, the Charter of the ACWG was changed to incorporate a reference to the Army Standard for Access Control Points (ACP) and Standard Definitive Design and to add the AIE Program to the Army Transforming Access Control Initiative. A special focus group was designated by the Chairman of the ACWG and an Integrated Process Team (IPT) was established to examine specific functional requirements and technical solutions to satisfy the Army access control initiative.

The Department of Defense (DoD) has an ongoing need to mitigate insider and external threats and reduce risks to institutional missions through the conduct of near-real time, continuous evaluation of personnel and vehicles against authoritative data sources during installation ACP operations. These operational requirements are a result of several high profile events such as the Fort Hood, Texas and Washington Navy Yard, District of Columbia incidents; multiple Congressional hearings; and Government Accountability Office (GAO) reports. Inherent in the needs and operational requirements is the necessary implementation of information technology (IT) solutions that provide the means for installation-based personnel to provide asset security management through personnel and vehicle screening at the installation perimeter. Specifically, the solution must provide physical security guards with the ability to validate and authenticate multiple types of identification credentials (to include those compliant with Homeland Security Presidential Directive - 12 requirements, state-issued driver licenses, etc.) using the DoD Identity Matching Engine for Security and Analysis (IMESA) architecture against dynamic Federal, state and local databases such as the following:

- Defense Enrollment Eligibility Reporting System (DEERS)
- National Crime Information Center (NCIC)
- Interstate Identification Index (III)
- Integrated Automated Fingerprint Identification System
- National Law Enforcement Telecommunications System (Nlets)
- Terrorist Screening Database (TSDB)

Program Executive Office (PEO) Intelligence, Electronic Warfare & Sensors (IEW&S) was designated as the Material Developer for the AIE Program. The AIE Program is being executed by the Product Manager, Force Protection Systems (PM-FPS), Fort Belvoir, Virginia.

1.4 Relation to Key Army Concepts

Secure Cloud Architecture: A well-defined and well-constructed cloud-based architecture is a critical mission enabler. The architecture must use a Cloud-Smart, data-smart approach. The architecture focuses on enabling mission criticality, data integrity, operational resilience and availability in a secure environment. By delivering centrally resourced and available Common Shared Services, Data Management Services, and Software Development Services we are able minimize long-term sustainment and duplication of effort.

Installation of the Future: The Army *Installation of the Future* is an ASA Installations, Energy and Environment (IE&E) initiative for incorporating "smart technology" to create installations that:

- support readiness;
- are resilient to disruptions;
- are sustainable;
- perform as strategic support areas; and
- coupled with analytics and artificial intelligence, provide faster awareness and decision options for Army leaders.

The initiative seeks to explore the possibilities of Army installations incorporating smart technologies available in cities located around them. The initiative also supports the Army's ability to remain a highly trained, effective, expeditionary and campaign-quality force today and in the future.

1.5 References

1.5.1 DOD

Department of Defense Instruction (DoDI) 5000.02, "Operation of the Adaptive Acquisition Framework (AAF)"

10 United Code (USC) 2222 DBS

Department of Defense Instruction (DoDI) 5000.75, "Business Systems Requirements and Acquisition," 24 January 2020

Department of Defense Instruction (DoDI) 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),” 15 October 2018

Department of Defense Instruction (DoDI) 5400.16, “DoD Privacy Impact Assessment Guidance”, 14 July 2015

Department of Defense Instruction (DoDI) 8500.01, “Cybersecurity,” 7 October 2019

Department of Defense Instruction (DoDI) 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” 28 July 2017

DOD Directive (DODD) 1000.25, Personal Identity Protection Program, 19 Jul 2004 (Certified current as of 23 Apr 2007)

1.5.2 Department of the Army

Army Pamphlet (DA PAM) 25-1-1, “Army Information Technology”, 15 July 2019

Army Pamphlet (DA PAM) 25-2-14, “Risk Management Framework for Army Information Technology”, 08 April 2019

Army Pamphlet (DA PAM) 25-2-16, “Communication Security (COMSEC)”, 08 April 2019

Army Regulation (AR) 25-1, “Army Information Technology”, 15 July 2019

Army Regulation (AR) 25-2, “Army Cybersecurity”, 4 April 2019

Army Regulation (AR) 25-22, “The Army Privacy Program”, 22 December 2016

Army Regulation (AR) 190-13, “The Army Physical Security Program”, 27 June 2019 Army Directive 2014-05, Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared contractors

Army Directive 2016-38Automated Installation Entry (AIE) Problem Statement (Part 1), HQDA, OPMG, 17 Aug 2016.

Army Standard for AIE (Part I) and Army AIE System Specifications (Part II), 19 Nov 2007

Capability Requirements Document (CRD) (Part 2), June 22, 2020, Department of the Army

1.5.3 Executive Branch

Executive Order 9397 (Social Security Number (SSN))

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, 27 Aug 2004

1.5.4 Federal Information Processing Standards Publications (FIPS PUB)

FIPS PUB 140 (2019) Security Requirements for Cryptographic Modules)

FIPS PUB 197 (2001) Advanced Encryption Standard

FIPS PUB 201-1 (2006) Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS PUB 201-2 (2011) DRAFT Personal Identity Verification (PIV) of Federal Employees and Contractors)

1.5.5 International Organization of Standardization (ISO)

ISO/International Electrotechnical Commission (IEC) 14443, Parts 1-4 (2018) Cards and security devices for personal identification—Proximity Objects

ISO/IEC 7810 (2019) Identification Cards—Physical Characteristics

ISO/IEC 7816 (2011, 2007, 2006, 2020, 2004, 2016) Identification Cards—Integrated Circuits with Contacts, Parts 1-6

1.5.6 National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018

American National Standards Institute (ANSI)/NIST-ITL 1-2011, NIST Special Publication 500-290, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, Nov 2011

NIST Special Publication 800-73-4 (May 2015 (Updated 2/8/2016)), Interfaces for Personal Identity Verification

NIST Special Publication 800-76-1 (2013), Biometric Specification for Personal Identity Verification

NIST Special Publication 800-78 (2010), Cryptographic Algorithms and Key Sizes for Personal Identity Verification

NIST Special Publication 800-116 (2018), Guidelines for the Use of PIV Credentials in Facility Access

1.5.7 Other Government

Office of Management and Budget (OMB) M-05-24, Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, 5 Aug 2005

Public Law 110-181, Section 1069, National Defense Authorization Act (FY2008 NDAA)

The Privacy Act of 1974, 5 USC. 552a

Title 10 US Code, Section 3013, Secretary of the Army

2. CONOPS

2.1 Operational Environment

The AIE System is installed at numerous US Military Installations (predominantly US Army Facilities) within the Continental United States (CONUS) and planned installation at Outside the Continental United States (OCONUS) locations. The AIE System is being installed, employed, maintained and supported at all locations by civilian contractors, military personnel and US Government Civilians. The AIE System is mission capable in environments that meet basic cold and hot weather criteria and be capable of continuous operation under harsh weather and environmental conditions. The AIE System operates using local commercial power and can be locally equipped with an Uninterruptible Power Supply (UPS). The System can be mutually compatible with other electronic equipment operating in its Area of Operations without system interference or degradation.

2.2 Threat Environment

The primary threats to be countered by AIE can be from physical or cyber actors. The former include terrorists, criminals, enemy infiltrators, insurgents and other belligerent parties.

Components of AIE may be vulnerable to physical destruction by small arms, grenade delivered fragments, blast effects, directed energy weapons, flame and incendiary weapons. Electronic Warfare Systems continue to pose a significant threat to US systems and are continuing to evolve and improve. Wireless communication links are susceptible to the effects of wireless attack from individuals using devices to overwhelm the wireless connections. If adversaries are able to disrupt wireless links, the wireless connections will be affected, rendering the data transmitted from Wireless Handheld devices useless. Other threats to AIE include theft, destruction and deception operations.

As with any Information Technology system, insiders present a real and persistent threat. Disgruntled operators, rogue insiders, or careless user activity could result in a loss of confidentiality, availability and/or integrity of the AIE system. Also, external threats exist that may seek to disrupt AIE operations through network attacks.

2.3 Program Interdependencies

AIE is part of a fused, automated, integrated and layered security plan, capable of interfacing with other FP systems to enhance the overall physical security posture of US Military Installations. The ability to share data across environments will greatly enhance Installation security.

2.3.1 External Interface Standards to Army Common Operating Environment (COE)

AIE conforms to the greater Army Common Operating Environment (COE) by ensuring that it integrates into other necessary systems and components. It will conform to the requirements of the appropriate Computing Environments (CE) such as the Data Center/Cloud CE.

2.3.2 Defense Installation Access Control (DIAC)

The DIAC Working Group's goal is to monitor compliance with Section 1069 of Public Law 110-181 for determining the fitness of personnel entering military Installations in the US. DIAC created IMESA to provide Military Commanders and Warfighters with improved Installation

security and enhanced situational awareness. IMESA provides accurate and actionable information to support real-time situational awareness from authoritative data bases to exercise access control and force protection responsibilities and assist force protection professionals to accurately execute access control policy.

The IMESA architecture is composed of three elements: 1) Interoperability Layer Service (IoLS), a system of software and services that provides linkage between the various Service PACS and authoritative data sources and provides the ability to share Installation access control information cross-service; 2) Continuous Information Management Engine (CIME), the engine that provides the analytical capability to continuously vet individual identities against authoritative data sources via deterministic and probabilistic methods; and 3) Local Population Database (LPDB), a consolidated DoD database, maintained by Defense Manpower Data Center (DMDC), containing individuals that require local Installation access but do not require or are not approved to receive a DoD Common Access Card (CAC).

2.4 Functional Capabilities

AIE has Fixed-Full (Tier 1) and Wireless Handheld configurations (Tier 2) as described in the AIE System Performance Specification. Fixed-Full AIE configuration is typically installed at large installations after the United States Army Corps of Engineers (USACE) Access Control Point Equipment Program (ACPEP) site preparation is complete. ACPEP design is described in the ACP Standard and Standard Design. The Wireless Handheld configuration provides AIE capabilities to installations that do not require the full System. Variations of the Fixed-Full and/or Wireless Handheld configurations may be necessary based on changes in policy, Installation and mission operations.

The system operates within an enterprise network that links all AIE sites. It reads, record and store credential and fingerprint information. The system is operational 24 hours a day, seven days a week. Security during increased levels of FPCON can be enhanced by the use of a second form of valid identification as stated in AD 2014-05.

Figure 2-1 provides a functional overview of a notional AIE architecture.

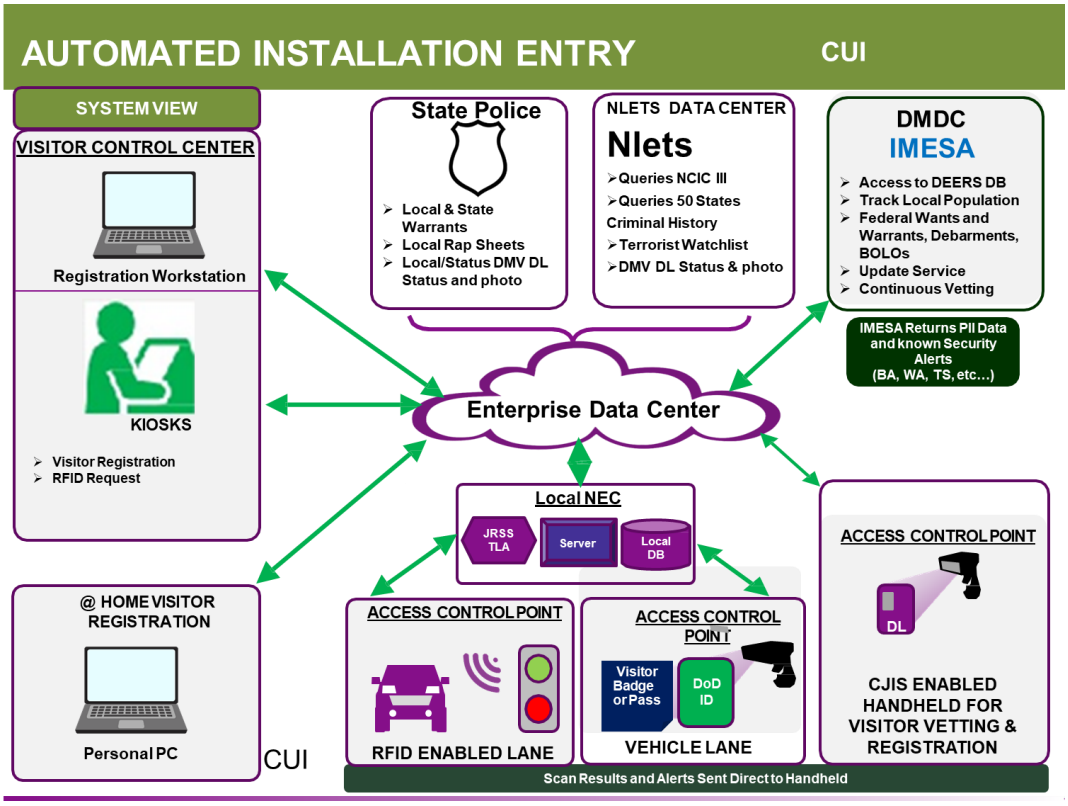

Figure 2-1: Notional AIE Functional Overview

2.4.1 Registration

To register users, each AIE installation will operate a Visitor Control Center (VCC) sized to handle local demand. Registration is conducted by VCC personnel, or by kiosk without assistance where installed. AIE also allow guards to register users in the lanes with assistance. Visitor passes are available online for a specific installation. These registration methods are detailed in the following sections.

During the registration process, AIE collects user information to include name, address, Date of Birth (DOB), SSN, signature, fingerprint, photo, expiration date of credential, user-specified PIN, class designation and unit of assignment. A valid credential is also necessary. (See Appendix B for a list of authorized credentials.) In accordance with Federal law, a notice addressing the Privacy Act and voluntary provision of personally identifiable information will be displayed at all registration locations. See Figure 2-2.

PRIVACY ACT STATEMENT, as required by 5 U.S.C. 552a (e) (3)
AUTHORITY: Executive Order 9397 (SSN); The Privacy Act of 1974, 5 U.S.C. 552a; Title 10 U.S.C. Section 3013; DoDD 8500.1
PRINCIPAL PURPOSE(S): To provide Installation Commanders and law enforcement officials with means by which information may be accurately identified to determine if applicant meets authorized access requirements. Use of SSN is required to make positive identification of an applicant. Records stored in the AIE System are maintained to support Department of the Army physical security and information assurance programs and are used for identity verification purposes, to record personal data and vehicle information registered with the Department of the Army, and for producing installation management reports. Employed by security officials to monitor individuals accessing Army installations. SSN, Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to Army installations.
ROUTINE USE(S): The "DOD Blanket Routine Uses" are set forth at the beginning of the Army compilation of systems of records notices.
DISCLOSURE: Voluntary; however, failure to provide the requested information will result in the denial of an authorized access pass (or equivalent) and denial of entry to Army installations.

Figure 2-2: AIE Privacy Act Statement

2.4.1.1 Visitor Control Center

Registration at each Installation is accomplished at the VCC using a Registration Workstation. The Workstation is a desktop computer with integrated personal data display and credential readers. It provides full registration and enrollment capabilities operated by Installation registration personnel. Registrants respond to system queries by entering registration information. The Registration Workstation receives personal information input by the registrar and user and supplies it for vetting against access denied lists and authoritative databases. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed on a placard at each Registration station.

The registrar is able to select the gate from a list of all ACPs and Pedestrian Gates at an Installation that a user will be allowed to enter. All visitors are vetted against the NCIC/Interstate Identification Index (III) database. Vetting through the Installation's Originating Agency Identifier (ORI) connection provides access to NCIC, Department of Motor Vehicles (DMV), in-state and out-of-state law enforcement sources. Vetting through IoLS provides access to Defense Enrollment Eligibility Reporting System (DEERS), authoritative databases and shared data from other Services.

Following Army guidance and Installation policy, the Trusted Traveler Program is implemented in the AIE System. This program allows a registered user designated as a Trusted Traveler to present their identification token for automated authentication while simultaneously vouching for other vehicle occupants. This reduces wait times during the identification process and increases traffic throughput. During Registration, the AIE System will identify individuals that are allowed Trusted Traveler privileges in accordance with applicable policies and regulations.

Upon positive feedback from debarment lists and authoritative databases, the Registrar completes enrollment. Depending upon local Installation policies, visitors may receive a temporary pass (paper), a long term pass (plastic), or may use their Driver's License as a registered credential. See Figure 2-3 for a sample description of a plastic AIE Visitor Badge which may be customized for an installation. The Registrar also links these credentials to the user's Personal Information Record (PIR). Data does not reside permanently on the Enrollment Workstation and all communication is encrypted using a network encryption method that is transparent to the system operator(s). Once registered, the user can immediately use the credential to enter the Installation via any AIE enabled ACP as designated during registration.

Back of card left blank to reduce life-cycle printing costs

1. Category. N/A
2. Base. The base to which the Registrar logs on.
3. Expiration Date. Expiration date is entered by the Registrar. Issue date is not displayed.
4. Name. Name can be updated at issuance as long as no other rule (like DEERS Authoritative Data Rule) prevents name edits.
5. Permission. N/A
6. Additional Permissions Indicator. N/A
7. Privileges. N/A
8. Remarks. N/A
9. Return to location. N/A
10. Other.
    a. Rank (free text field)
    b. ID number

Barcode format is Standard ID Format Code 39
Total characters is 9

| ① --- | ② -------- |----------③----------|

1. 888 (hardcoded value)
2. Credential Number (6 digit numeric sequence randomly generated)
3. Other - None

Figure 2-3: AIE Visitor Badge

2.4.1.2 Kiosk Registration

Kiosks are installed at selected Installations. Users can interact with the kiosk without needing help from VCC personnel. They must supply a valid identification such as a driver's license or passport and enter other information into the kiosk. The kiosk will take a photo of the registrant and compare it to the identification, send a request to initiate vetting as in the normal registration process, and if the visitor is granted access, print out a paper visitor pass that will be accepted at the local ACP. The visitor will show the pass and their driver's license to the guard. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed at each Kiosk.

2.4.1.3 Portable Registration

Portable Registration provides with an accompanying carrying case. This registration capability is used at pre-determined network accessible locations to register users holding valid CACs, Teslin cards and state drivers' licenses.

Portable Registration provides full registration capabilities and is operated by trained personnel. The portable Enrollment Workstation reads personal information input by the user and registrar to send a request to initiate vetting. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed on a placard at each portable Enrollment Workstation.

Upon positive vetting feedback, the Registrar completes enrollment. Data does not reside permanently on the Portable Registration Workstation and all communication is encrypted using a network encryption method that is transparent to the system operator(s). Once registered, the user can immediately enter the Installation via any AIE enabled ACP as designated during registration.

2.4.1.4 Automatic Registration at Vehicle Lane

AIE provides an automatic registration capability at the vehicle lanes for users holding valid CACs, Teslin or DBIDS cards. This selectable configuration is provided at each ACP and at each lane. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed at each vehicle lane.

The AIE System allows the vehicle operator to present an authorized credential at the lane and retrieve information from the card's memory (CAC), 1D and 2D bar codes and vet against debarment lists and authoritative databases.

AIE displays the retrieved image of the driver. This data is stored in the user PIR data file for future use. Once successfully vetted, Automatic Registration is complete and individuals are granted access to the Installation.

2.4.1.5 Visitor In Lane Registration

AIE provides a registration capability at the vehicle lanes for users holding valid state drivers' licenses. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed at each vehicle lane.

The AIE System will allow the vehicle operator to present a driver's license to the guard at the lane and will retrieve information from the 1D and 2D bar codes and vet against the access denied list, authoritative databases such as NCIC III, including in-state and out-of-state data sources. The system will only allow a CJIS certified guard to initiate visitor in lane registration. The system will query the driver for photo if not returned from DMV, capture and store as part of the PIR.

AIE will display the retrieved image of the driver. Access is not granted if photo is not displayed. This data is stored in the user PIR data file for future use. Once successfully vetted,

registration is complete, record pushed to IoLS for continuous vetting, and individuals are granted access to the Installation.

2.4.1.6 Online Visitor Registration

A link to the online registration website is found on each Installation Home Website. The visitor selects the desired Installation to visit, enters the requested information including email address and reason for visit and submits it. The system routes the request to the Installation's VCC to initiate vetting. If approved, a pass is emailed to the visitor that is printed/downloaded onto smartphone for display at the Installation ACP. If a pass is denied, the visitor will be informed by email to contact the VCC for questions. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed at the online registration website.

2.4.1.6.1 Sponsored Online Visitor Registration

To provide for sponsored Installation visitors, AIE has a registration capability that can be performed online for visitor convenience. A sponsor sends an invite with visit date and purpose to the visitor with a link to the online registration website which the visitor can access from off-site. There they enter the requested information including email address and submit it. The system routes their request to the sponsor for verification, and then to Installation's VCC for vetting. If approved, the visitor will be directed to pick up the pass at the VCC or receive it by email according to local Installation policy. If a pass is denied, the visitor will be informed by email. The pass is shown by the visitor at the Installation ACP along with their identification. Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement as illustrated in Figure 2-2 will be displayed at the online registration website.

2.4.2 Access Control Point Operations

An Access Control Point (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 validation and access challenges may vary significantly from one Installation to another, the AIE Program establishes access control and validation processes that facilitate standardization of ACP operations.

The AIE System allows the Installation Commander or authorized security official to electronically configure the system to support enhanced features such as automatic registration and visitor in-lane registration.**Error! Reference source not found.**

2.4.2.1 Vehicle Lane Operations

To accomplish ACP entry processing, vehicle lanes are equipped with several components to control credentials validation and vehicle movement. AIE is fielded in two versions: Tier 1 with pedestal credential scanners, gate arms, traffic lights, guard booths, and handheld scanners, and Tier 2 with only handheld scanners. The scanners are FIPS 201 compliant and read credentials identified in Appendix B. The device will have the ability to display user information, and photos. The device will not store user data and all data transmissions will be encrypted. The scanner will be configured such that the operator cannot modify configuration.

2.4.2.1.1 Tier 1 Lanes

Tier 1 ACPs have lanes with fixed components that enable entrance traffic flow with minimal supervision. The system will have 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 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 scans their credential at the pedestal and the driver camera records a live image of the driver's face.

The Tier 1 Guard Booth is equipped with a workstation, wireless handheld scanner with spare battery and docking station, display panel and intercom. Operators in each Guard Booth are able to monitor traffic in their respective and one adjacent lane, and also have the ability to override automatic gate functions if necessary.

Within the Guard Booth, a monitor displays information for determining access rights for each driver/vehicle or pedestrian. This information includes data from drivers and pedestrians, live video feeds of drivers and pedestrians and results from the vetting process. The monitor displays the user information and photo for comparison with real-time image of the user. The monitor displays when a user is denied access. The Guard Booth operator is able to grant/deny access, and/or perform a lane override and provide an integrated traffic hold.

The system retrieves the user's record from the site database and presents the information to the Guard Booth, Gate House and Central Remote Station. The system will also display whether the driver is allowed Trusted Traveler privileges. The Guard compares the user's photo with the video of the user at the lane to ensure they are the same individual. If there is a problem, the Guard will have the ability to override the system to prevent entry. All access control transactions are recorded for potential reporting.

A Gate Arm Assembly allows entry (arm goes up) upon successful user verification or denies entry (arm stays down) if access is denied. The Gate Arm will not rise automatically for drivers who are denied Trusted Traveler privileges. A traffic light (green, red) is integrated into the system to denote entry status.

Sequence of the Tier 1 Lanes follows:

1. As a vehicle enters the lane, fixed overwatch cameras constantly record and archive driver and vehicle images. All video is stored for forensic purposes using a Digital Video Recorder (DVR).

2. Signage and traffic lights are used to direct vehicles entering the automated lanes.

3. While the vehicle is at the vehicle pedestal, the pedestal camera captures the real time image of the driver for viewing by at the Gate House, Guard Booth and Central Remote Station.

4. The driver presents credentials.

5. The AIE System verifies credential and performs the following:

a. <u>If access is authorized:</u>

- "Access Granted" is displayed at the Pedestal and Guard Stations.
- The Gate Arm rises.
- The traffic signal switches from red to green.
- The information display on reader instructs the driver to proceed.
- The vehicle sensor determines that a vehicle has exited or cleared the lane and the Gate Arm lowers.

  NOTE: If the sensor on the Gate Arm Assembly detects the presence of a vehicle, the Gate Arm will not be lowered.

- The traffic signal returns to red and the entry lane is ready for the next vehicle.

b. <u>If access is denied:</u>

- "Access Denied" is displayed at the Pedestal and Guard Station.
- A description of the reason for denial is displayed at the Guard Station.
- The reader informs the driver that access is denied.
- The Gate Arm remains down and the Gate Arm traffic signal remains red.
- The vehicle driver is notified in person or by intercom to exit the vehicle lane using the turn-around after the Gate Arm is raised.
- The Lane Guard initiates an Integrated Traffic Hold and manually raises the Gate Arm to allow that vehicle to turn around.

The Lane Guard, Gate House Operator and Central Remote Station are all equipped with capability to perform these functions and to override automatic system functions as required to deny or allow access.

2.4.2.1.2 Tier 2 Lanes

Some installations will be wireless handheld lane operation only. Tier 2 Lanes only use wireless handheld credential scanners, provided at each vehicle lane's Guard Booth with a docking station and associated batteries. Tier 2 operates in the following sequence:

1. Signage and traffic lights are used to direct vehicles entering the automated lanes.
2. The driver presents credentials to the Guard.

3. The Guard reads the credential with the Wireless Handheld device and the system queries the database.
4. The Wireless Handheld device displays the user data and photo and the Guard compares the information and photo of the user.
5. If access granted is displayed, the Guard returns the credential and the vehicle is allowed to proceed.
6. If access is denied, the Guard will review the reason for denial and direct the vehicle accordingly.

2.4.2.2 Gate House Operations

The Gate House supports Tier 1 and is equipped with a workstation, Wireless Handheld battery charger, display panel and intercom. Operators in the Gate House are able to monitor all vehicle lanes and also have the ability to override automatic gate functions if necessary. The intercom provides two-way audio communication between the Gate House and the ACP lanes to assist and or interrogate users.

The Gate House monitor displays information from each of the ACP's lanes. This information includes data from drivers and pedestrians, live video feeds of drivers and pedestrians and results from the vetting process. The monitor displays the user record for comparison with real-time video recorded of the user from the vehicle lane and pedestrian portal. The monitor also alerts the Gate House operator when any user is to be denied access. Gate House Operators are able to grant/deny access, perform lane overrides and provide an integrated traffic hold.

2.4.2.3 Cellular Wireless Operations

Where Installation access is needed at a location without adequate communications infrastructure, a cellular access control point can be fielded consisting of a cellular wireless bridge, firewall, Wireless Access Point (WAP), uninterruptible power supply (UPS), and associated cables providing connectivity back to the local installation network.

It is capable of using multiple cellular providers, can maintain continuous connectivity, and is fully mobile and can be setup and operational within 15 minutes. A portable version can be deployed in a protected case. The system is able to support wireless scanning, remote registration and other emerging technologies.

2.4.3 Server Operations

The AIE system using a hybrid cloud scheme to store personal information records of all Installation users and is capable of storing at least 5,000,000 (scalable up to 50,000,000) personal records. It utilizes a web services open architecture interface to IoLS for vetting to DEERS and other authoritative databases. Server sites (large) only store records locally. Small sites with a Cache box store records in the cloud and partial records locally, and receive updates from IoLS via the Non-secure Internet Protocol Router Network (NIPRNet).

2.4.3.1 Enterprise Data Center Cloud Operations

The AIE System consists of primary and secondary servers that store AIE enrollment records. Small sites with a cache box utilize a hybrid cloud solution of local Network Enterprise Center (NEC) and enterprise cloud. This approach provides the ability for installations to continue to operate without the loss of external communications, as well as minimizing the total number and size of the servers on the Installation.

2.4.3.2 Large Site Server Operations

Larger Installations deploy more robust site or ACP servers with Database/Domain Controller for continuity of operations**.** A Witness/Splunk/WSUS server is added to enable automatic failover of the server cluster, and to manage software upgrades for that installation. The local NEC provides access to external communications.

2.4.3.3 Small Site Cache Box Operations

Smaller Installations are provided a cache box to store a minimal set of user data for access decisions. This helps to reduce the risk of communication outages but will operate directly to the cloud for transactions and registrations. External communications are provided via cloud operations.

2.4.4 Help Desk Operations

The AIE Help Desk is a centralized resource staffed to assist users in resolving problems. It operates under a three tiered structure to include Tier-1 (Quick Reference Guide assistance, Routing and Escalation engine), Tier-2 (break/fix) and Tier-3 (Complex technical support). Once a trouble ticket is submitted, it is evaluated and routed to the responsible organization for resolution. If not resolved, it is elevated to a Tier 2 subject matter expert who will respond within 24 hours. Root cause will be determined, and a course of action taken. If required, the issue is routed to a Tier 3 AIE engineer level for additional action.

2.4.5 Monitoring and Reporting

2.4.5.1 Dashboard

The System provides a Dashboard displaying Installation level reports from a central remote location. It also provides a public facing Dashboard that displays current totals of Registered Persons, DOD Credentials Registered, Visitor Credentials Registered, Visitor Credentials Registered, VHICs Registered, Survivor Access Cards, and Foreign Military Registered by Installation, updated monthly.

Additionally, the Dashboard provides an 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.

The Dashboard displays scan counts and total scan count by site, ACP, lane, and cumulative system total for Tier 1 and Tier 2, customizable by time and date ranges.

AIE system health and status shall be available to view with inputs from system and network tools such as Solarwinds and Splunk. This enables a view of the AIE network connectivity status with IMESA services and enterprise hosting in the cloud.

2.4.5.2 Video Management

AIE provides a video system to monitor and record activity at the lanes. The video has three views: overview, driver view, and the vehicle license plate. Guards have a real-time view of the driver during vehicle lane transaction. The system operates continuously 24 hours/day, 7 days/week and stores images for seven days with the ability to store 180 days of events requiring intervention. The video is viewable from the Central Monitoring Workstation with the ability to download or capture video and conduct quick search for Law Enforcement actions.

2.4.5.3 Transaction Reports

The System can generate an Installation Access Control Data Report which can be customized. It includes pass, debarment, access and denial history reports filterable by name, date, and time:

a. All Denied History Report (by name combination, DOB, SSN, EDIPI, date, category type, and time)
b. All Visitor Pass Report (by name combination, DOB, SSN, EDIPI, date, category type, and time)
c. Individual Scan History (by name combination, DOB, SSN, EDIPI, date, category type, and time)
d. Registered Persons Transaction Report (by name combination, DOB, SSN, EDIPI, date, category type, and time)
e. ACP Scan/Transaction Report (by name combination, DOB, SSN, EDIPI, date, category type, and 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 (by name combination, DOB, SSN, EDIPI, date, category type, and time)
i. Handheld Report
j. NCIC III transaction report including the FBI Number

2.4.5.4 Datamining and Analytics

As a part of the AIE reporting system, datamining is used to discover trends and relationships between system operation and sustainment parameters. This includes researching trouble tickets for root causes of issues, identifying trends and areas indicating improvement, and highlighting the longest open trouble tickets with their common characteristics. In order to understand demand at the vehicle lanes, we anticipate the following analysis:

- Daily lane throughput at each ACP and Installation and identify trends and changes in traffic volume
- Transaction times for registration, vetting, visitor center processing, handheld scanner and pedestals
- Vetting denials, TSDB hits, and active warrants and debarments
- NCIC vetting granted and denied by site and total
- Scans by site, ACP, lane and total

2.4.5.5 Artificial Intelligence

Artificial intelligence may be applied to reduce management burden by analyzing the system statuses and taking actions where appropriate:

- Analyze Network connectivity and identify trends, and alarm when parameters exceed normal values.
- Analyze Equipment breakage and replacement intervals and establish predictive maintenance intervals.
- Analyze ACP throughput and alarm when normal values are exceeded.

2.4.5.6 Reliability, Availability and Maintainability (RAM)

The AIE System is designed to deliver reliable entrance capability to the Installation and provide status reporting. It provides a non-integrated RAM tool that displays metrics such as help desk data, system availability and reliability, maintainability and cost. A Dashboard map is displayed for ease of understanding system health codes for identifying Full Mission Capable (FMC), Partially Mission Capable (PMC), and Not Mission Capable (NMC).

2.4.6 Network / Communications

AIE uses Army installation Network for transport purposes and to access AIE equipment on the local area Network. NETCOM provides an enterprise network infrastructure designed to integrate the AIE fiber/network architecture/topology infrastructure into each designated Army CONUS Installation site facility virtual local area network (VLAN). The AIE VLAN architecture will be used at each Installation, to include the AIE VLAN accreditation boundary in relation to the Installation facility boundary. All AIE installation network accesses are behind firewall and Army Security Router (ASR) under the management of 2nd Regional Cyber Center (2RCC), Joint Regional Security Stacks (JRSS), and Theater Network Operations and Security Center (TNOSC), which controls access to the NIPRNET. AIE enterprise network access to the NIPRNET will be available via the network Top-Level Architecture (TLA) or the Joint Regional Security Stack (JRSS) managed by 2nd Regional Cyber Center – Western Hemisphere (2RCC-WH) , to include CND protection, whereby the 2nd Signal Center/2RCC-WH will place its standard enterprise signature Network Intrusion Prevention System (NIPS)/Network Intrusion Detection System (NIDS) sensor detection templates on the TLA/JRSS sensors designed to protect the Army's Enterprise (to include AIE traffic) and to look for the common, current and most appropriate attack methods and vulnerabilities. The 2nd Signal Center/2RCC-WH will work with the Regional Computer Emergency Response Team – CONUS (RCERT-C) and the respective NECs/DOIMs when handling alerts from these sensors in accordance with current

computer network defense regulations and guidance (e.g., AR 25-2, Sections VII and VIII). AIE network protection below the 2nd Signal Center/2RCC-WH -managed TLA components will be provided by the Installation NECs, DOIMs and Information Assurance Managers (IAMs), such as local VLAN and Host Based Security System (HBSS) O&M requirements associated with the AIE network traffic.

The AIE network design will provide protected connectivity between the Army CONUS post/camp/station Installation AIE VLAN nodes and the Defense Information System Network (DISN) enterprise backbone Wide Area Network (WAN) via the Army LandWarNet NIPRNET.

Network security is engineered into the AIE System design by using firewalls, intrusion prevention systems, Host Based Security System (HBSS) and access control lists. HBSS services are provided by the Army Endpoint Security Solution (AESS) services and managed by the PM office and supported by the Prime Contractor. Communication between AIE servers will use Advanced Encryption Standard (AES) 256-bit encryption on top of any additional encryption offered by the Local Area Network (LAN), providing encryption of data in transit. The AIE System will also encrypt data at rest.

2.5 Information Assurance (IA)/Cybersecurity

2.5.1 IA/Cybersecurity Requirements

IA/Cybersecurity requirements are addressed throughout the AIE System life cycle in accordance with DoDI 8500.01, DoDI 8510.01, AR 25-2 and AR 190-13 and other DoD and Defense Information Systems Agency (DISA) requirements as they are added. The IA/Cybersecurity Strategy is an integral part of the program's overall acquisition strategy, identifying the technical, schedule, cost and funding issues associated with executing requirements for IA/Cybersecurity. The AIE System will also implement security controls from previously mandated DoDI 8500.2 or corresponding set of security controls from NIST SP 800-53R4 to comply with cybersecurity requirements specified in DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), whichever is mandated by the Army during the system authorization process.

A comprehensive authorization package is needed to obtain favorable 3 year accreditation approval. The Accreditation and Authorization (A&A) package will include system security maintenance and continuous monitoring activities to ensure the AIE System continues to operate within the designated categorization, security posture and stated parameters of the accreditation/authorization. A Working-level Integrated Product Team (WIPT) ensures that the AIE System complies with these requirements by reviewing the results of the AIE A&A system authorization effort. The AIE System will be subjected to Government Security Test and Evaluation (ST&E) for yearly cybersecurity risk assessments as a part of Federal Information Security Management Act (FISMA), and is subject to DISA managed Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) Command Cyber Readiness Inspection (CCRI) . The AIE Program Management Office (PMO) consents to any scheduled and unscheduled inspections by Army Cyber Command (ARCYBER). System and system accreditation artifacts shall be updated as part of FISMA and as well as any changes to the system that affects security posture of the system.

AIE System operators continuously assess and monitor security policies and procedures to incorporate an Information Assurance Vulnerability Management (IAVM) program, as referenced under DODI O-8530.2, Enclosure (6), Support to Computer Network Defense and CJCSI 6510.01F, IA and CND.

A continuous evaluation of IA/Cybersecurity implementation will be employed to maintain a Cybersecurity Risk Management (CRM) approach for mitigating the realization of system vulnerabilities. The CRM approach will be maintained by the AIE System owner as a part of the system RMF Documentation. Changes in the system necessary to strengthen the IA posture will be considered in a manner comparable to those satisfying any other functional requirement.

2.5.2 IA Technical Considerations

The AIE-3 cybersecurity strategy uses authorized ports and protocols and maximizes the use of Department of Defense Information Network Approved Products List (DODIN APL). AIE-3 integrates the identification, authentication, and authorization processes by relying on DoD Public Key Infrastructures (PKIs), the appropriate DISA Active Directory (AD) forests, and DoD identity management and standard connection methods. The plan for authorization creates a well-defined boundary, based on DoDAF drawings, that reduces integration risk by implementing management, operational, and technical information security controls to safeguard AIE-3 and data from unauthorized access and disclosure. AIE-3 system is designated as a Type accredited Information System Enclave. The Type authorization provides a set of installation, security control, and configuration requirements delineated between the program and multiple hosting Installations to provide a single and unified system

3. PRODUCT SUPPORT

The objective of the support strategy is to provide enduring support for AIE capabilities and identify opportunities for continuous process improvement in order to maintain the relevance of the AIE capabilities, the supporting hardware and software technologies, and infrastructure hosting solution.

A two level maintenance approach will be employed to sustain all generations of AIE System hardware and software and documentation. The two levels of maintenance are field support (also known as organizational support) and depot support. The AIE Contractor will provide one year of Contractor Logistics Support (CLS) after Government acceptance of installed systems. PM-FPS will establish agreements with Government sustainment support activities to continue AIE logistics support after the CLS period for the life of the system.

3.1 Contractor Logistics Support (CLS)

The AIE system uses a two level maintenance concept, Field and Depot.

Field Level consists of Basic Operator Maintenance, including replacement of expendable items such as straps, batteries, external screws, external cleaning, and toner cartridge replacement.

Depot Level is performed on newly fielded systems for one year under Contractor Logistics Support (CLS). AIE CLS includes warranty, licenses, service agreements, schedule and unscheduled field level maintenance above basic operator maintenance task and supply 10% of the consumables (such as printer supplies and identification card stock) for each AIE Installation. Additionally, the AIE contractor will establish and maintain a 24/7 Help Desk during the CLS period. After CLS, all warranties, licenses, service agreements, scheduled and unscheduled field level maintenance is transitioned to U.S. Army Communications-Electronics Command (CECOM) for continued logistics and sustainment support. One year of CLS will be provided upon Government acceptance of an installed AIE System. The CLS will include all warranty (to include IA); licenses; service agreements; scheduled and unscheduled field level maintenance above basic operator maintenance task and supply support, less consumables (such as printer supplies and identification card stock). Under CLS, the Contractor integrates and fields 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.

3.2 Organic Support

Following completion of the one year of CLS, sustainment of a fielded AIE System transitions to the Government. CECOM will provide organic AIE System sustainment support after the CLS period. CECOM will provide all required sustainment activities to include Hardware, Software, Cyber Security, and Information Assurance support to ensure maximum system Operational Availability (A_O). Arrangements are also made with other Army Support Commands as appropriate for the life cycle sustainment of the AIE System.

Post Deployment Software Support (PDSS) transitions AIE software to organic sustainment managed by CECOM Software Engineering Center (SEC) for software and CECOM Integrated Logistic Support Center (ILSC) for hardware. PM FPS provides the system, support equipment, OEM technical support and engineering environment for SEC and ILSC to perform the required PDSS at Government-Owned, Government-Operated (GOGO) facilities. PM FPS ensures resources are programmed and necessary Intellectual Property (IP) deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance.

THIS PAGE INTENTIONALLY LEFT BANK

APPENDIX A - ACRONYMS AND ABBREVIATIONS

2RCC-WH	2nd Regional Cyber Center – Western Hemisphere
7th SC(T)	7th Signal Command (Theater)
ACP	Access Control Point
ACPEP	Access Control Point Equipment Program
ACWG	Access Control Working Group
AEI	Army Enterprise Infrastructure
AES	Advanced Encryption Standard
AESS	Army Endpoint Security Solution
AIE	Automated Installation Entry
AIS	Automated Information Systems
ANSI	American National Standards Institute
APL	Approved Products List
AR	Army Regulation
ASR	Army Security Router
ATMIS	Advanced Traffic Management and Information System
C&A	Certification &Accreditation
CAC	Common Access Card
CIME	Continuous Information Management Engine
CECOM	Communications-Electronics Command
CLS	Contractor Logistics Support
CND	Computer Network Defense
COE	Common Operating Environment
CoN	Certificate of Networthiness
CONOPS	Concept of Operations
CONUS	Continental United States
CRM	Cybersecurity Risk Management
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
DISN	Defense Information System Network
DMDC	Defense Manpower Data Center
DMV	Department of Motor Vehicles
DOB	Date of Birth
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction

DoDIN	Department of Defense Information Network
DOIM	Directorate of Information Management
DVR	Digital Video Recorder
EDIPI	Electronic Data Interchange Personal Identifier
FHWA	Federal Highway Administration
FIPS PUB	Federal Information Processing Standard Publication
FOSS	Free Open-Source Software
FP	Force Protection
FPCON	Force Protection Condition
GOCO	Government Owned Contractor Operated
HBSS	Host Based Security System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAM	Information Assurance Manager
IAVM	Information Assurance Vulnerability Management
ICD	Interface Control Document
ICIDS	Integrated Commercial Intrusion Detection System
ID	Identification
IEW&S	Intelligence, Electronic Warfare & Sensors
IEC	International Electrotechnical Commission
III	Interstate Identification Index
ILSC	Integrated Logistics Support Center
IMESA	Identity Matching Engine for Security and Analysis
IoLS	Interoperability Layer Service
IPT	Integrated Product Team
ISO	International Organization of Standardization
IT	Information Technology
ITWA	Initial Threat Warning Assessment
JRSS	Joint Regional Security Stack
LAN	Local Area Network
LPDB	Local Population Database
MUTCD	Manual of Uniform Traffic Control Devices
NCIC	National Crime Information Center
NDAA	National Defense Authorization Act
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NIDS	Network Intrusion Detection System
NIPRNet	Non-secure Internet Protocol Router Network

NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy
O&M	Operations & Maintenance
OCONUS	Outside the Continental United States
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PACS	Physical Access Control Systems
PDSS	Post Deployment Software Support
PEO	Program Executive Office
PIN	Personal Identification Number
PIR	Personal Identity Record
PIV	Personal Identity Verification
PM-FPS	Product Manager, Force Protection Systems
PSE	Physical Security Equipment
PSEAG	Physical Security Enterprise & Analysis Group
RAR	Rapid Action Release
RAM	Reliability, Availability and Maintainability
RCERT-C	Regional Computer Emergency Response Team – CONUS
RMF	Risk Management Framework
SEC	Software Engineering Center
SEIWG	Security Equipment Integration Working Group
SSN	Social Security Number
ST&E	Security Test and Evaluation
TLA	Top-Level Architecture
TLCSM	Total Life Cycle System Management
TPF	Total Package Fielding
TSDB	Terrorist Screening Database
TYAD	Tobyhanna Army Depot
UPS	Uninterruptible Power Supply
USACE	US Army Corps of Engineers
USC	United States Code
VCC	Visitor Control Center
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WIPT	Working-level Integrated Product Team

THIS PAGE INTENTIONALLY LEFT BANK

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 DEERS at the lane
PIV	Compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases) NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	Yes	Yes	Yes
PIV-I	Not compliant	Yes	Access Denied List IoLS (NCIC Wants & Warrants, authoritative databases) NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	No	Yes	No
NFI PIV-I	Not compliant	Yes	Access Denied List IoLS (NCIC Wants & Warrants, authoritative databases) NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	No	Yes	No
CAC	Compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases) DMV In-state and out-of-state data sources	Yes – authenticate & register if not in system	Yes	Yes

Credential Usage						
Authorized Credentials	FIPS 201 Compliant	Use at Registration	Vetting	Auto Registration at Lane	Use at Lane	Vet to DEERS at the lane
CAC, Chipless (DoD Civilian Retiree)	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DA Form 1602 (DoD Civilian Retiree)	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 2 (armed forces Geneva convention)	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 2A (active duty)	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 2S	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 1173	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 1173-1	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DD Form 2765	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes – authenticate & register if not in system	Yes	Yes
DBIDS	Not compliant	Yes	Access Denied List IoLS (DEERS, NCIC Wants & Warrants, authoritative databases)	Yes	Yes	No

Credential Usage						
Authorized Credentials	FIPS 201 Compliant	Use at Registration	Vetting	Auto Registration at Lane	Use at Lane	Vet to DEERS at the lane
TWIC	Not compliant	Yes	Access Denied List NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	No	Yes	No
Passport	Not compliant	Yes	Access Denied List NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	No	No	No
State–issued Drivers License	Not compliant	Yes	Access Denied List NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	Yes	Yes	No
State issued ID	Not compliant	Yes	Access Denied List NCIC/III (via ORI connection) DMV In-state and out-of-state data sources	No	Yes	No