Product Manager,
Force Protection Systems (PM FPS)

Automated Installation Entry (AIE)-3.4

System Description and Architecture

01 April 2022

SYSTEM DESCRIPTION AND ARCHITECTURE
RECORD OF REVISION

Revision Number	Date	Description
Draft, Rev 0	17 October 2016	Initial Release for AIE-3
N/A	18 November 2016	Addressed comments by Government reviewers
N/A	22 November 2016	Additional details added regarding EntryPoint Datamodel (Appendix K) and Client-Server communication (Section 6.2)
Draft, Rev 1	31 January 2017	Added missing DODAF Views for: OV-6a, OV-6b, OV6c, SV-5b, SV-10a, SV-10b, SV-10c. Additionally, added Portable Registration System to SV-1 and SV-3.
Final	2 March 2017	Final submission
Final RCF	31 March 2017	Addressed comments by Government reviewers
Final, Rev 3	6 March 2020	Modifications to DODAF Views and Interfaces to account for Visitor Registration and RFID additions to the architecture. Depicts Pure Fleet design rather than AIE-3 baseline design.
Draft, Rev 4	14 February 2022	Modifications throughout to address AIE-3/4 capabilities and associated changes. Sections 3 and 8 have TBD's identified in content. Appendices B, I, J, W, X, Y, Z, EE are TBD
Draft, Rev 4.1	28 February 2022	Modifications to Sections 3 and 8, and Appendices B, I, J, W, X, Y, Z, EE Appendix J has TBDs for Event Trace: AutoRegistration, Event Trace: RFID Access Granted, and Event Trace: Handheld Operations.
Final, Rev 4.2	1 April 2022	Addressed comments by Government reviewers

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Title** **Page**

1. Scope

The original scope of this document was limited to the Automated Installation Entry, increment 3 (AIE-3) programs as detailed in the AIE-3 Statement of Work, AIE-3 System Performance Specification, and AIE-3 Concept of Operations (CONOPS).

Revision 4 of this document incorporates the evolution of AIE-3 to provide both Pure Fleet (PF) and AIE-4 functionality and capabilities and include:

- Includes fully internet protocol (IP) based lane operations through
  - the elimination of the Rhino Reader from the architecture replacement with an IP based Qscan reader device.
  - elimination of the AMAG door controller and DBU in favor of direct IP communication between the QScan Card Reader.
  - use of the Hawkeye Visual Verify software on the Guard Booth Workstation in support of RFID and Qscan processing; and
  - use of Hawkeye IMM software on the AIE Server or Cache Box
- In addition, the document details the integration of cellular wireless to provide alternate communications connectivity when warranted,
- replacement of existing handheld devices with upgraded Zebra handheld devices, upgrading to the enhanced visitor Kiosk 2.0,
- enhancements to the cloud enabled processing of the system, and
- enhancements to online vetting and registration.

1.1 Identification

This document describes the System Architecture (SA) for the AIE-3/4 program using the Department of Defense Architecture Framework (DoDAF) v2.02. This framework was developed to provide an accepted, consistent, integrated, and understandable means to express architectures of complex systems. In accordance with DoDAF v2.02 guidelines, the architecture will be depicted using prescribed diagrams and documents termed “viewpoints”. The format and content of the viewpoints are described in the DoDAF v2.02 documentation titled, “DoD Architecture Framework v2.0 Volumes 1, 2, and 3”. The list of viewpoints to be provided in this document is defined in Data Item Description (DID) DI-MGMT-81644A and is listed in Table 1 of the AIE-3 Systems Engineering Management Plan (SEMP) and in Section A.2.1 of the All Viewpoint 1 (AV-1) found at Appendix A.

1.2 System Overview

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 Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) was designated by the Principal Deputy Assistant Secretary of the Army (Acquisition, Logistics and Technology) on 12 August 2008 as the Material Developer for the AIE Program and has transitioned to Program Executive Office for Intelligence, Electronic Warfare, and Sensors (PEO-IEWS). The AIE Program is being executed by the office of the Product Manager, Force Protection Systems (PM FPS), Fort Belvoir, Virginia.

The AIE System provides timely, effective, and efficient threat detection necessary for Installation Commanders to assess and react in all threat environments. AIE automates access control processes for authorized and registered personnel entering an Installation. AIE improves access/denial accuracy and enables near real-time changes of authentication requirements in response to changes in force protection conditions. AIE enhances Installation security and improves both pedestrian and vehicle throughput at Access Control Points (ACPs).

The AIE System will be installed at 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 flexible and support future upgrades through incorporation of technical advancements. The AIE System will be used at US Military locations in the Continental United States (CONUS) and Installations Outside the Continental United States (OCONUS).

Two previous AIE Systems have been fielded. AIE-1 was fielded at three Installations. AIE-1 was designed as an interim step to meet the AIE specifications and standards and achieved the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) as a stand-alone system.

AIE-2 enhanced AIE-1 capabilities. AIE-2 has enterprise capability and achieved DIACAP accreditation. There are 32 AIE-2 Systems installed. A bridge contract issued to the AIE-2 contractor while waiting for the AIE-3 acquisition augmented the initial AIE-2 capabilities to include law enforcement (LE) vetting of non-DoD credentials and an interface to Interoperability Layer Services (IoLS) as a replacement for the Defense Enrollment Eligibility Reporting Service (DEERS) Interface Web Services (IWS). IoLS supports authoritative identity databases including DEERS as well as Continuous Information Management Engine (CIME) to provide security alerts from enterprise sources including the National Crime Information Center (NCIC) Wanted Persons File.

The AIE-3 System provides a cost-effective system that enhances security of Installation Access Control Points (ACPs), automates identity authentication and verification of authorized registered personnel entering the Installation, minimizes guard force requirement, 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 and wireless Handheld-only configurations. The Fixed-Full configuration includes the wireless handheld capability, but the handheld-only configuration provides AIE-3 capabilities to Installations that do not require the vehicle lane equipment. AIE-3 was also implemented at previously installed AIE-2 locations under the Pure Fleet fielding effort. This solution leverages existing AIE-2 lane equipment where possible to provide previously fielded AIE Installation with full AIE-3 capability.

AIE-4 related functionality and capabilities include elimination of the Rhino Reader from the architecture by replacement with an IP based Qscan reader device; elimination of the AMAG door controller and DBU in favor of direct IP communication between the QScan Card Reader; use of the Hawkeye Visual Verify software on the Guard Booth Workstation in support of RFID and Qscan processing; use of Hawkeye IMM software on the AIE Server or Cache Box. AIE-4 is also being implemented at previously installed AIE-2/3 locations under the Pure Fleet fielding effort. This solution leverages existing AIE-2/3 lane equipment where possible to provide previously fielded AIE Installation with full AIE-4 capability. AIE-4 also includes the integration of cellular wireless capabilities to provide alternate communications connectivity when warranted; replacement of existing handheld devices with upgraded Zebra handheld devices; upgrading to the enhanced visitor Kiosk 2.0; and enhancements to the cloud enabled processing of the system.

1.3 Document Overview

In accordance with DID DI-IPSC-81432A, the AIE-3/4 System-wide Design and Architecture Description is described in this document. The architecture is described through DID DI-MGMT-81644A designated DoDAF architecture views, and the document is further enhanced with DID DI-IPSC-81434A (Interface Requirements Specification), DID DI-IPSC-81435A (Software Design Description), DID DI-IPSC-81436A (Interface Design Description), and DID DI-IPSC-81437A (Database Design Description).

1.4 Component Definition

The following table identifies the components (with identifier prefix, CMP-) of the AIE-3/4 System.

Component ID	Component Name	Component Description	Component Type	Associations
CMP-001	Site Server Set	Runs applications at Installation level (Registration Server, Symmetry Server-Site, Identity Management Middleware (IMM) Client, and SQL Server). Supports database for PIR records, and Identity vetting.	Hardware	CMP-004, CMP-009, CMP-011, CMP-022, CMP-026, CMP-030
CMP-002	Removed			
CMP-003	Removed			
CMP-004	Symmetry Server-Site/Cloud	Services to support integration with Registration Server, SQL database, and manage PIR data.	Software	CMP-001, CMP-011
CMP-005	Removed			
CMP-006	Removed			
CMP-007	Registration Client	Application to collect PIR data, print temporary and permanent passes.	Software	CMP-009, CMP-022, CMP-026, CMP-039
CMP-008	Symmetry Client	Application to support various functions at Guard Booth, Gatehouse, and Central remote monitoring location.	Software	CMP-023, CMP-024, CMP-025
CMP-009	IMM Client	Identity Management Middleware to interface with vetting services (IoLS and LE Vetting service).	Software	CMP-001, CMP-007, CMP-015, CMP-016, CMP-017, CMP-022, CMP-026, CMP-032
CMP-010	Removed			
CMP-011	SQL Server-Site/Cloud	Database management at the Site/App/DB Servers	Software	CMP-001, CMP-004, CMP-030
CMP-012	Removed			

Component ID	Component Name	Component Description	Component Type	Associations
CMP-013	Symmetry Gate Controller	Access control, input and output interface and intelligence to control automated and manual operations at vehicle and pedestrian lanes. NOTE: comprised of the DCU and DBU.	Hardware	CMP-035
CMP-13a	Symmetry Door Control Unit (DCU)	Provides a conduit for barcode data exchanged between the Rhino Reader and DBU.	Hardware	CMP-013, CMP-042
CMP-13b	Symmetry Database Unit (DBU)	Provides a local database of trusted travelers for an installation.	Hardware	CMP-001, CMP-013, CMP-041, CMP
CMP-014	Lane Intercom Station	Intercom station that allows vehicle driver or pedestrian to initiate call to Guard for assistance.	Hardware	CMP-014, CMP-027, CMP-028, CMP-029
CMP-015	IoLS	Interoperability Layer Services is a government-managed cloud service that supports identity vetting through multiple authoritative sources and continuous information management engine (NCIC, TSDB, etc.)	External	CMP-009
CMP-016	LE Vetting Service	Law Enforcement vetting and adjudication service provides a response to an LE vetting request initiated by a CJIS trained operator	External	CMP-009
CMP-017	Hawkeye Mobile	Software solution that runs on the handheld for registration and validation at the ACP.	Software	CMP-009, CMP-018
CMP-018	Removed			
CMP-018(ALT1)	CrossMatch Verifier Sentry	Handheld for use at vehicle and pedestrian lanes.	Hardware	CMP-017
CMP-018(ALT2)	Zebra TC72	Handheld for use at vehicle and pedestrian lanes.	Hardware	CMP-017

Component ID	Component Name	Component Description	Component Type	Associations
CMP-019	Removed			
CMP-020	Removed			
CMP-021	Video Cameras	Cameras to capture front of vehicle, rear of vehicle (for vehicle lane), and person's face (vehicle and pedestrian gates).	Hardware	CMP-034
CMP-022	Registration Workstation	Workstation for use by the Registrar to register suitable personnel into the AIE-3 system. NOTE: aka Registration Workstation. (RGWS).	Hardware	CMP-001, CMP-007, CMP-009, CMP-039
CMP-023	Lane Control Workstation	Touch-enhanced workstation for use by Guard to monitor and control devices at the lane or multiple lanes. NOTE: aka Guard Booth Workstation. (GBWS).	Hardware	CMP-008
CMP-024	ACP Monitoring Workstation	Touch-enhanced workstation for use by Guard to monitor and control devices at one or more lanes. NOTE: aka Gatehouse Workstation (GHWS).	Hardware	CMP-008
CMP-025	Remote Monitoring Workstation	Touch-enhanced workstation for use by Guard to monitor and control devices at one or more lanes. NOTE: aka Central Monitoring Workstation (CMWS) or (Enhanced Monitoring Workstation) when configured with registration software to be used for dual purpose.	Hardware	CMP-008

Component ID	Component Name	Component Description	Component Type	Associations
CMP-026	Portable Registration System	Transportable system for use by the Registrar (or designee) to register suitable personnel into the AIE-3/4 system outside of the Visitor Center.	Hardware	CMP-001, CMP-007, CMP-009, CMP-039
CMP-027	Guard Booth Intercom Station	Intercom station that allows Guard to answer and initiate calls from/to the vehicle and pedestrian lanes.	Hardware	CMP-014, CMP-027, CMP-028, CMP-029
CMP-028	ACP Intercom Station	Intercom station that allows Guard to answer and initiate calls from/to the vehicle and pedestrian lanes.	Hardware	CMP-014, CMP-027, CMP-028, CMP-029
CMP-029	Remote Monitoring Intercom Station	Intercom station that allows Guard to answer and initiate calls from/to the vehicle and pedestrian lanes.	Hardware	CMP-014, CMP-027, CMP-028, CMP-029
CMP-030	Hawkeye Sync Services	Service that prepares PIR data at App/DB Servers for synchronization to Cache Box servers.	Software	CMP-001, CMP-011, CMP-038, CMP-51
CMP-031	Removed			
CMP-032	IMM-AutoReg	Service that manages the automatic registration process at the vehicle and pedestrian lanes.	Software	CMP-009, CMP-033
CMP-033	Rhino Reader	Multi-credential reader with display, biometric verification, and PIN pad. NOTE: Rhino Reader is being eliminated and replaced with Qscan device.	Hardware	CMP-032, CMP-013
CMP-034	Symmetry CompleteView	Video management subsystem	Software	CMP-021

Component ID	Component Name	Component Description	Component Type	Associations
CMP-035	RFID Reader	Antenna and reader to interact with Ultra-High Frequency (UHF) tags issued to trusted travelers for expedited passage through ACP. NOTE: operates with Symmetry Gate Controller or Adam Module.	Hardware	CMP-013, CMP-032
CMP-036	VCC Kiosk	Kiosk system accessible to visitors to the VCC for self-service registration.	Hardware	CMP-037
CMP-036 (ALT1)	VCC Kiosk 2.0	Iberon Kiosk system accessible to visitors to the VCC for self-service registration.	Hardware	CMP-037
CMP-037	AIE Visitor Registration Web Server	Hosted web site for visitor self-service input of registration information.	Software	CMP-036, CMP-039, CMP-040
CMP-038	SQL Server Enterprise	Enterprise cloud host of the SQL Database that houses PIR data store and Installation configuration DB	Software	CMP-030, CMP-039
CMP-039	Symmetry Server Enterprise	Enterprise cloud host of the Symmetry services that handle database management and the IMM Services that handle vetting and Web input.	Software	CMP-007, CMP-022, CMP-026, CMP-037, CMP-038
CMP-040	Visitor Home PC or another browser device	Visitor self-service portal (PC, tablet, or phone).	Hardware	CMP-037
CMP-041	Adam Module	IP enabled input/output device used to provide a method to monitor device status, provide status to Hawkeye IMM, receive commands from Hawkeye IMM, and control devices based on those commands.	Hardware	CMP-035, CMP-043, CMP-045

Component ID	Component Name	Component Description	Component Type	Associations
CMP-042	Exit Ground Loop with Loop Detector	Detects vehicles passing or arriving at a certain point and provides a response signal for processing.	Hardware	CMP-013
CMP-043	Gate Arm	Mechanical barrier used at the ACP to secure traffic.	Hardware	CMP-013, CMP-042
CMP-044	Traffic Light	Set of automatically operated lights for controlling traffic at the ACP.	Hardware	CMP-CMP057
CMP-045	Barcode Reader	Card credential reader that reads 1D and 2D barcodes. NOTE: Rhino Reader is being eliminated and replaced with Qscan barcode reader display device at installations.	Hardware	CMP-032, CMP-013
CMP-046	Mobile Device Management (MDM) Server	Enterprise cloud host of the SOTIMobiControl services that handle mobile device management of the handheld devices.	Hardware	CMP-018(ALT1), CMP-018(ALT2)
CMP-047	SOTIMobiControl	Enterprise cloud host for the SOTIMobiControl services that handle mobile device management of the handheld devices.	Software	CMP-018(ALT1), CMP-018(ALT2), CMP-048
CMP-048	SOTIMobiControl Client	Client for handheld devices to be managed by Enterprise cloud host SoTIMobiControl services.	Software	CMP-018(ALT1), CMP-018(ALT2), CMP-047
CMP-049	Cache Box	Runs applications and provides storage for local installation population as a backup to the App/DB Servers.	Hardware	CMP-050

Component ID	Component Name	Component Description	Component Type	Associations
CMP-050	Cloud Servers	Runs applications at Installation level from AIE Enterprise Data Center in the cloud (Registration Server, Symmetry Server-Site, Identity Management Middleware (IMM) Client, and SQL Server). Supports database for PIR records and Identity vetting.	Virtual Machine	CMP-004, CMP-009, CMP-011, CMP-022, CMP-026, CMP-030, CMP-38, CMP-39
CMP-051	Hawkeye Visual Verify	Application to support various functions at Guard Booth, Gatehouse, and Central remote monitoring location.	Software	CMP-23, CMP-24, CMP-25
CMP-052	Iberon Kiosk Software	Application to support the operations of the VCC Kiosk 2.0.	Software	CMP-036 (ALT1)
CMP-053	Cellular Wireless (Cradlepoint)	Provides a cellular wireless link into a connected device. Also used to provide a cellular point to multi-point link to provide IP connectivity without hard-wired infrastructure.	Hardware	CMP-001
CMP-054	Network Video Recorder	Records and stores video files from in lane cameras used to perform forensic analysis	Hardware	CMP-021, CMP-034
CMP-055	Cloud Server	Runs applications at Installation level (Registration Server, Symmetry Server-Site, Identity Management Middleware (IMM) Client, and SQL Server). Supports database for PIR records, and Identity vetting.	Virtual Machine	CMP-004, CMP-009, CMP-011, CMP-022, CMP-026, CMP-030

Component ID	Component Name	Component Description	Component Type	Associations
CMP-056	OPMG Enterprise Server	Provides repository to collect installation scan, registration, and denial data for generating OPMG Dashboard Reports.	Virtual Machine	CMP-052
CMP-057	24VDC Relay	Controls Traffic Light mechanical operations.	Hardware	CMP-041, CMP-044

09

Figure 1: System Component Definition

2. Reference Documents

2.1 Government Documents

The following documents contribute to this architecture to the extent that they reflect topics and content which relate to the AIE-3/4 requirements and architecture. Unless otherwise specified, the latest revision of the referenced document is in effect. Documents not specifically identified in the body of this architecture are for reference only.

2.1.1 DoD Documents (in alphabetical order)

a. Army Regulation (AR) 25-1, *Army Information Technology*, 15 July 2019.
b. AR 25-2, *Army Cybersecurity,4 April 2019*.
c. AR 70-1, *Army Acquisition Policy,* 10 August 2018.
d. AR 190-13, *Army Physical Security Program*, 27 June 2019.
e. AR 700-127, *Integrated Logistics Support*, 22 October 2018
f. Army Access Control Points Standard Definitive Design, 13 April 2019.
g. Chairman of the Joint Chief of Staff Instruction (CJCSI) 3170.01I *Joint Capabilities Integration and Development System (JCIDS)*, 23 January 2015.
h. CJCSI 5123.01G, *Charter of the Joint Requirements Oversight Council,* 30 October 2021
i. Department of the Army (DoA), Office of the Chief Information Officer, *Army Information Architecture (AIA) v4.1*, 5 June 2013.
j. *DoD Architecture Framework (DoDAF) v2.02*, Change 1, Volumes I, II, III, & IV, January 2015.
k. DoD Direction (DoDD) 5101.07, *DoD Executive Agent for Information Technology Standards*, 21 May 2004.
l. DoD, Office of the Chief Information Officer, *DoD Information Enterprise Architecture (IEA) v2.0*, Volume I, August 2012.

m. DoD, Office of the Chief Information Officer, *DoD Information Enterprise Architecture (IEA) v2.0*, Volume II, August 2012.

n. *DoD Information Technology Standards Repository (DISR),* (See DoDD 5101.07, May 2004).

o. DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, May 19, 2010, Incorporating Change 3, Effective: 20 November 2015.

p. DoD 5200.08R, *Physical Security Program*, April 9, 2007, Incorporating Change 2, 19 October 2020.

q. DoDI 8500.01, *Cybersecurity*, 14 March 2014, Incorporating Change 1, Effective: 7 October 2019.

r. DoDI 8510.01, *Risk Management Framework for DoD Information Technology*, 29 December 2020.

s. DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 July 2004.

t. Military Standard (MIL-STD) 810, *Environmental Engineering Considerations and Laboratory Tests*, latest revision (G or later). 810G with Change 1, Effective 15 April 2014

u. Security Equipment Integration Working Group (SEIWG) Interface Control Document (ICD) 0101B, *Force Protection Systems Sensor Information Interchange Information Interchange using XML,* June 2011.

v. Unified Capabilities Requirements (UCR) 2013, *Unified Capabilities Requirements 2013,* January 2013, Change 2, Effective 2 September 2017.

2.1.2 Other Government Documents

a. Criminal Justice Information Services, *Electronic Fingerprint Transmission Specification (EFTS)*, July 2013.

b. Criminal Justice Information Services, *Electronic Biometric Transmission Specification (EBTS)*, 14 December 2012.

c. Criminal Justice Information Services 6510.01F Information Assurance (IA) and Computer Network Defense (CND) 9 June 2015.

d. Department of Labor (DOL), *Americans with Disabilities Act: Accessibility Guidelines for Buildings and Facilities (ADAAG),* Latest Revision/Update.

e. Federal Highway Administration (FHWA), Installation of Traffic Control Devices, FHWA-SA-89-006, March 1988.

f. *FIPS 140-3: Security Requirements for Cryptographic Modules.* National Institute for Standards and Technology (NIST) Computer Security Resource Center (CSRC). 22 March 2019

g. *FIPS 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors.* NIST CSRC. January 2022

2.1.3 Code of Federal Regulations (CFR)

a. 36 CFR Part 1194, *Electronic and Information Technology Accessibility Standards.*

2.1.4. AIE-3/4 Program Documents

a. AIE Standards and Specifications November 19, 2007.

b. System Performance Specification for AIE-3, 22 October 2014.

c. AIE-3 Concept of Operations (CONOPS), 8 September 2014.

d. AIE-3 Statement of Work (SOW) 6 November 2014.

e. Additional clarifying requirements.

- Rhino Elimination, July 2021
- Kiosk 2.0, March 2020
- Dashboard, March 2022
- Network, January 2022

2.2 Non-Government Documents

a. American National Standards Institute/National Institute of Standards and Technology- ITL 1-2011, updated 2015

b. American National Standards Institute/National Institute of Standards and Technology- ITL 1-2011, updated 2013.

c. National Fire Protection Association (NFPA) 72, *National Fire Alarm Code®,* 2022 (or latest revision).

2.3 Order of Precedence: The contractor applies precedence in accordance with the post-award clarification, SOW, the System Architecture (this document), the System Performance Specification and the Concept of Operations, respectively. The various Specification documents detail the technical requirements of the system and/or component. However, nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. AIE-3/4 System-Wide Design Decisions

The AIE-3/4 System is an incremental improvement of the Army's fielded and operational AIE-2 system solution. Previous AIE increments were designed around a combination of COTS products and proprietary, non-COTS hardware and software. This posed significant challenges for transferring support and sustainment to the government beyond the contractor support period. The design of AIE-3/4 addresses this issue by being composed entirely of widely supportable, field-tested, and proven COTS hardware and software components. These design choices result in a significantly lower total cost of ownership (TCO) to the Government.

The AIE-3/4 System is designed to meet or exceed all required performance capabilities, including all key capabilities. Subsystems and components of the AIE-3/4 System have been selected for integrated system performance; relevant DoD physical security systems program experience; industry best practices; and long-term availability, supportability, and upgradability.

In addition, because the AIE-3/4 System is composed entirely of COTS products, the systems and equipment are constantly evolving to deliver new features, better performance, and supported integrations at no direct cost to the Government. The

primary AMAG Symmetry Access Control System (ACS), IoLS and LE Vetting Services include published application programming interfaces (APIs) and software development kits (SDKs) to facilitate integrations.

The AIE-3/4 System takes advantage of open architecture and cloud computing concepts to provide an on-premises and hybrid enterprise cloud solution. Cloud capabilities are procured and managed under the Infrastructure as a Service (IaaS) model, where all the environment is ‘rented’, and the program retains full control over the environment with respect to VM creation, network/firewall configuration, in addition to control over the Operating Systems and application on the VM servers. This approach allows Installation to share support Infrastructure, allowing for cost reduction and greater visibility into the Enterprise.

The AIE-3/4 network architecture leverages the existing Army network infrastructure backbone, in accordance with NETCOM guidance. Local networking is provided by the Installation over existing Non-secure Internet Protocol Router Network (NIPRnet) circuits, or by dedicated Fiber connecting AIE endpoints. External connections to both the cloud environment, and supporting external services is provided through the Installations connection to the Joint Regional Security Stack (JRSS) housed within the Network Enterprise Center (NEC). The IPSEC based site to site VPN connections are utilized between the cloud and the individual Installations, providing for continuous secure links, which enhances the capabilities provided by the IaaS cloud component.

4. System Architectural Design

In accordance with DID DI-MGMT-81644A, the AIE-3/4 architecture is described through DoDAF viewpoints (diagrams and documents) in the format prescribed by DoDAF v2.02. The following DoDAF artifacts are provided to describe the Systems description and architecture.

4.1 All Viewpoint 1 (AV-1): Overview and Summary Information

The AIE-3/4 AV-1 Overview and Summary document outlines the content, justification, and point of reference of the targeted architecture and encompasses the entire architecture. It lists the elements to be contained in the architecture, the organizational, programmatic and system documentation which provide the justification for creating the architecture and the enterprise points of reference which provide an anchor point for the development of the architecture artifacts. The AIE-3/4 AV-1 is provided as Appendix A.

4.2 All Viewpoint 2 (AV-2): Integrated Dictionary

The AIE-3/4 AV-2 Integrated Dictionary includes terms, abbreviations and acronyms that are system or topic unique found in the architecture. The AIE-3/4 AV-2 is provided as Appendix B.

4.3 Operational Viewpoint 1 (OV-1): High Level Operational Concept Graphic

The AIE-3/4 OV-1 provides a high-level graphical view of the system activities, elements, organizations, and external entities. The view includes system elements as well as external elements with which the AIE-3/4 will interface and support or which will provide support to AIE-3/4. The AIE-3 OV-1 is provided as Appendix C.

4.4 Operational Viewpoint 2 (OV-2): Operational Node Connectivity Description

The AIE-3/4 OV-2 provides a view depicting operational resource flows between the AIE-3/4 activities. The direction of resource flow and type of resource is identified. The AIE-3/4 OV-2 is provided as Appendix D.

4.5 Operational Viewpoint 3 (OV-3): Operational Information Exchange Matrix

The AIE-3/4 OV-3 is a matrix with the operational activities arrayed across the axes and the resource exchanges identified between the activities. The AIE-3/4 OV-3 is provided as Appendix E.

4.6 Operational Viewpoint 4 (OV-4): Organizational Relationships Chart

The AIE-3/4 OV-4 depicts the relationship between the various organizations which perform the activities depicted in the other operational views. It details the context, roles, and other relationships among the organizations. The AIE-3/4 OV-4 is provided as Appendix F.

4.7 Operational Viewpoint 5 (OV-5): Operational Activity Model

The AIE-3/4 OV-5 depicts the Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information organized hierarchically to provide a context for understanding their relationships. The AIE-3/4 OV-5 is provided as Appendix G.

4.8 Operational Viewpoint 6a (OV-6a): Operational Rules Model

The AIE-3/4 OV-6a depicts the operational rules that govern the activities and the organizations performing the activities. These are the “business” rules which constrain operations. The AIE-3/4 OV-6a is provided as Appendix H.

4.9 Operational Viewpoint 6b (OV-6b): Operational State Transition Description

The AIE-3/4 OV-6b depicts how the activities react to events and how they change or adjust their course as the operational flow of events unfolds. The AIE-3/4 OV-6b is provided as Appendix I.

4.10 Operational Viewpoint 6c (OV-6c): Operational Event Trace Description

The AIE-3/4 OV-6c depicts the sequential flow of events and how they may alter their course (branches) due to operational conditions. The AIE-3/4 OV-6c is provided as Appendix J.

4.11 Operational Viewpoint 7 (OV-7): Logical Data Model

The AIE-3/4 OV-7 depicts the system data requirements and structural business process rules of the Operational View. The AIE-3/4 OV-7 is provided as Appendix K.

4.12 Systems Viewpoint 1 (SV-1): Systems Interface Description

The AIE-3/4 SV-1 depicts the systems, system components and elements and their interconnections. The AIE-3/4 SV-1 is provided as Appendix L.

4.13 Systems Viewpoint 2 (SV-2): Systems Communications Description

The AIE-3/4 SV-2 depicts the systems, system components and their elements, and the system resource flows between the systems. The AIE-3/4 SV-2 is provided as Appendix M.

4.14 Systems Viewpoint 3 (SV-3): Systems-Systems Matrix

The AIE-3/4 SV-3 provides a tabular summary of the system interactions depicted in SV-1 & SV-2. The AIE-3/4 SV-3 is provided as Appendix N.

4.15 Systems Viewpoint 4 (SV-4): Systems Functionality Description

The AIE-3/4 SV-4 depicts the functions performed by the various parts of the system, their relationships, and the data/resources shared between the functions. The AIE-3/4 SV-4 is provided as Appendix O.

4.16 Systems Viewpoint 4a (SV-4a): Systems Functionality Description

The AIE-3/4 SV-4a depicts the system functional hierarchies and system functions, and the system data flows between them. The AIE-3/4 SV-4a is provided as Appendix P.

4.17 Systems Viewpoint 4b (SV-4b): Systems Functionality Description

The AIE-3/4 SV-4b depicts the service functionality that is exposed to the Net-Centric Environment, their respective grouping into service families, and their service specifications. The AIE-3/4 SV-4b is provided as Appendix Q.

4.18 Systems Viewpoint 5 (SV-5): Operational Activity to Systems Function Traceability Matrix

The AIE-3/4 SV-5 depicts the mapping of systems back to capabilities or of system functions back to operational activities. The AIE-3/4 SV-5 is provided as Appendix R.

4.19 Systems Viewpoint 5a (SV-5a): Operational Activity to Systems Function Traceability Matrix

The AIE-3/4 SV-5a depicts the mapping of operational activities to system functions and thus identifies the transformation of an operational need into a purposeful action performed by a system. The AIE-3/4 SV-5a is provided as Appendix S.

4.20 Systems Viewpoint 5b (SV-5b): Operational Activity to Systems Function Traceability Matrix

The AIE-3/4 SV-5b extends the SV-5a and depicts the mapping of capabilities to operational activities, operational activities to system functions, system functions to systems, and thus relates the capabilities to the systems that support them. The AIE-3/4 SV-5b is provided as Appendix T.

4.21 Systems Viewpoint 5c (SV-5c): Operational Activity to Systems Function Traceability Matrix

The AIE-3/4 SV-5c depicts the traceability and mapping of services to operational activities to assist in understanding which services support operational activities. The AIE-3/4 SV-5c is provided as Appendix U.

4.22 Systems Viewpoint 6 (SV-6): Systems Data Exchange Matrix

The AIE-3/4 SV-6 provides details of system data elements being exchanged between systems and the attributes of that exchange. The AIE-3/4 SV-6 is provided as Appendix V.

4.23 Systems Viewpoint 7 (SV-7): Systems Performance Parameters Matrix

The AIE-3/4 SV-7 provides performance characteristics of Systems View elements for the appropriate time frame(s). The AIE-3/4 SV-7 is provided as Appendix W.

4.24 Systems Viewpoint 8 (SV-8): Systems Evolution Description

The AIE-3/4 SV-8 provides planned incremental steps toward evolving the older AIE-1 and AIE-2 systems to the AIE-3/4 implementation. The AIE-3/4 SV-8 is provided as Appendix X.

4.25 Systems Viewpoint 9 (SV-9): Systems Technology Forecast

The AIE-3/4 SV-9 provides details of emerging technologies and software/hardware products that are expected to be available in each set of time frames and that will affect future development of the architecture. The AIE-3/4 SV-9 is provided as Appendix Y.

4.26 Systems Viewpoint 10a (SV-10a): Systems Rules Model

The AIE-3/4 SV-10a identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation. The AIE-3/4 SV-10a is provided as Appendix Z.

4.27 Systems Viewpoint 10b (SV-10b): Systems State Transition Description

The AIE-3/4 SV-10b identifies responses of a system to events. The AIE-3/4 SV-10b is provided as Appendix AA.

4.28 Systems Viewpoint 10c (SV-10c): Systems Event-Trace Description

The AIE-3/4 SV-10c identifies system-specific refinements of critical sequences of events described in the Operational View. The AIE-3/4 SV-10c is provided as Appendix BB.

4.29 Systems Viewpoint 11 (SV-11): Physical Schema

The AIE-3/4 SV-11 describes the physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema. The AIE-3/4 SV-11 is provided as Appendix CC.

4.30 Technical Viewpoint 1 (TV-1): Technical Standards Profile

The AIE-3/4 TV-1 provides a listing of standards that apply to Systems View elements in the given architecture. The AIE-3/4 TV-1 is provided as Appendix DD.

4.31 Technical Viewpoint 2 (TV-2): Technical Standards Forecast

The AIE-3/4 TV-2 provides a description of emerging standards and potential impact on current Systems View elements, within a set of time frames. The AIE-3/4 TV-2 is provided as Appendix EE.

5. Requirements Traceability Matrix

RTM ID	Requirement ID	Requirement Description	Source Document	Operational Area	AIE-3/4 Design Component	Comment
1	SS_100	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 registration.	AIE-3 System Performance Specification	Registration	Registration Client	
2	SS_101	The System shall vet credentials with authoritative databases through IoLS and populate registration fields without the operator having to re-key information. The System will connect to IoLS for access to DEERS, the local database, NCIC and out to the Federal Bridge. (Modification) The government waives this portion of the requirement: The System will connect to DEERS, independently of IoLS and be available in the event IoLS is unavailable.	AIE-3 System Performance Specification	Registration	[Multiple Requirements are delineated below]	
		The System shall vet credentials with authoritative databases through IoLS.	SS_101	Registration	IMM Client	
		The System shall populate registration fields without the operator having to re-key information.	SS_101	Registration	Registration Client	
		The System will connect to IoLS for access to DEERS.	SS_101	Registration	IMM Client	
		The System will connect to the local database.	SS_101	Registration	Registration Server	

		The System will connect to NCIC.	SS_101	Registration	IMM Client	Connects to LE vetting service, like IoLS but LE vetting service is at a fee.
		The System will connect out to the Federal Bridge.	SS_101	Registration	IMM Client	
		The System will connect to DEERS, independently of IoLS and be available in the event IoLS is unavailable.	SS_101	Registration	N/A	Direct connection to DEERS through IWS no longer viable.
3	SS_102	The System shall deny registration to personnel registering as permanent party who receive negative results from authoritative databases and shall proceed with the registration process for those receiving positive results.	AIE-3 System Performance Specification	Registration	Registration Client	
4	SS_103	The System shall provide Administrator override capabilities to register personnel who have negative results from authoritative databases.	AIE-3 System Performance Specification	Registration	Registration Client	
5	SS_104	The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication (PUB) 201-1 compliant credential for personnel access control during registration, vehicle lane operations, and pedestrian portal operations. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Registration	[Multiple Requirements are delineated below]	
		The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication	SS_104	Registration	Registration Client	

		(PUB) 201-1 compliant credential for personnel access control during registration.			
		The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication (PUB) 201-1 compliant credential for personnel access control during vehicle lane operations.	SS_104	Process Personnel at Vehicles Lanes	Rhino Reader Qscan Reader
		The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication (PUB) 201-1 compliant credential for personnel access control during pedestrian portal operations.	SS_104	Process Personnel at Vehicles Lanes	Rhino Reader Qscan Reader
6	SS_105	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) and verifying credentials with DEERS.	AIE-3 System Performance Specification	Registration	Registration Client
7	SS_106	The System shall be capable of reading 1-D and 2-D bar-coded information issued by local Installations.	AIE-3 System Performance Specification	Registration	Registration Client
8	SS_107	The System shall display information obtained from credentials along with a captured digital image of the credential holder to the enrollment operator.	AIE-3 System Performance Specification	Registration	Registration Client
9	SS_108	The System shall have the capability to limit locally issued credentials to access only	AIE-3 System Performance Specification	Registration	Registration Client

		Installations from which the credential was issued.				
10	SS_109	The System shall be capable of reading fingerprints, recalling templates for everyone enrolled in the database and authenticating the individual's identity by their fingerprint with the registration database.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Rhino Reader Qscan Reader	Requirement for reading fingerprints at the pedestal removed by Government 17 Aug 2021
11	SS_110	The System shall have the capability to accept no fingerprints and continue the enrollment process.	AIE-3 System Performance Specification	Registration	Registration Client	
12	SS_111	DEFERRED - 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.	AIE-3 System Performance Specification	Registration	Registration Client	There is no need to store FP images in EFTS format. FPs captured are converted to ANSI/INCITS 378 templates and image is not stored.
13	SS_112	The System shall store an enrollee Personal Identification Number (PIN) of up to ten digits with the registration record. (Modification) The Government will accept a fixed eight-digit PIN.	AIE-3 System Performance Specification	Registration	Site Server App/DB Servers Cache Box Symmetry Gate Controller	
14	SS_113	The System shall allow input at the time of registration the Force Protection Condition (FPCON) levels at which the individual is authorized to enter the facility.	AIE-3 System Performance Specification	Registration	Registration Client	
15	SS_114	The System shall be capable of identifying if individuals are allowed Trusted Traveler (TT) privileges IAW Army Regulation (AR) 190-13 ~~and~~	AIE-3 System Performance Specification	Registration	Registration Client	

		~~applicable Installation policies and regulations~~. (Deferred until IoLS v2.2 is implemented). (Modification) Remove "... and applicable Installation policies and regulations".			
16	SS_115	The Registrar shall be capable of designating a user's TT privileges based on applicable Installation policies and regulations.	AIE-3 System Performance Specification	Registration	Registration Client
17	SS_116	The System shall be capable of linking multiple approved credentials to an individual user Personal Information Record (PIR).	AIE-3 System Performance Specification	Registration	Registration Client
18	SS_117	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 and Non-Resident and Retiree (Military and Government Civilian).	AIE-3 System Performance Specification	Registration	Registration Client
19	SS_118	The System shall allow individuals to belong to more than one class of users.	AIE-3 System Performance Specification	Registration	Registration Client
20	SS_119	The System shall be capable of querying user for input, allowing user to enter information and collecting credential information, PIN, digital photo, signature, and fingerprint data for all registrants. The System shall store all valid forms of identification for users.	AIE-3 System Performance Specification	Registration	Registration Client
21	SS_120	The System shall be able to electronically read an individual's driver's license or state issued identification card	AIE-3 System Performance Specification	Registration	Registration Client

		and display information embedded on the credential for the enrollment operator to visually compare and confirm against the data printed on the card.			
22	SS_121	The System shall provide a fully integrated capability for single sign-on for the registration station for registration activities.	AIE-3 System Performance Specification	Registration	Registration Client
23	SS_122	The System shall have a portable registration station capability.	AIE-3 System Performance Specification	Registration	Registration Client
24	SS_123	The System shall provide the capability for the registrar to select from a list of all Installation ACPs and Pedestrian Gates, the ACP(s) that a user will be allowed to enter. Default configuration is access to all ACPs.	AIE-3 System Performance Specification	Registration	Registration Client
25	SS_124	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.	AIE-3 System Performance Specification	Registration	Registration Client
26	SS_125	The System shall electronically read and record information from an individual's driver's license or state issued identification card into the System database and issue a visitor pass.	AIE-3 System Performance Specification	Registration	Registration Client
27	SS_126	The System shall display captured information and populate fields in the visitor pass.	AIE-3 System Performance Specification	Registration	Registration Client

28	SS_127	The System shall allow the Registrar to manually enter and update user personal information into the Registration System including access denied and debarments.	AIE-3 System Performance Specification	Registration	Registration Client
29	SS_128	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's driver's license and store the signature and photo in the System database.	AIE-3 System Performance Specification	Registration	Registration Client
30	SS_129	The System shall generate long-term badges (plastic) and short-term visitor passes (paper) and allow Registrar to assign expiration date and time. Badge formats shall be IAW with AIE Concept of Operations.	AIE-3 System Performance Specification	Registration	Registration Client
31	SS_130	The System shall enable the unique enrollment of at least 2,000,000 (scalable up to 20,000,000) personal information records.	AIE-3 System Performance Specification	Registration	Site Server Cloud Server
32	SS_131	The System shall have the capability to allow CAC, Teslin card and Driver's License holders to use their authorized credential to automatically register at ~~both Fixed Full and Handheld~~ vehicle lanes with a Handheld. (Modification) Remove …both Fixed Full and …)	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	IMM AutoReg Rhino Reader Qscan Reader Handheld
33	SS_132	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	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	[Multiple Requirements are delineated below]

		memory, 1D ~~or 2D~~ barcode and vet against authoritative databases. (Modification) Remove …or 2D …)			
		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 barcode~~. (Modification) This does not include the 2D barcode on a CAC.	SS_132	Automatic Registration at Vehicle Lane	Rhino Reader Qscan Reader
		The System shall have the capability to allow the vehicle operator to present an authorized credential and vet against authoritative databases.	SS_132	Automatic Registration at Vehicle Lane	IMM AutoReg
34	SS_133	The System shall provide the capability, upon positive vetting response, to query vehicle operator for fingerprint via selectable menu. This data will be stored with the user PIR data file.	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	IMM AutoReg
35	SS_134	(Deleted by the Government on 10/12/2017).	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	IMM AutoReg
36	SS_135	The System shall display the retrieved image of the driver from the DEERS database, DMV (if available) or other authoritative databases.	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	IMM AutoReg GBWS
37	SS_136	The System shall provide a selectable menu to allow state driver's license card holders to use their authorized credential to automatically register at ~~both Fixed Full and Handheld~~ vehicle lanes with a Handheld	AIE-3 System Performance Specification	Automatic Registration at Vehicle Lane	IMM AutoReg

		(Modification) remove …both Fixed Full and..			
38	SS_200	The System shall perform a Wants and Warrant checks through IoLS using data from National Crime Information Center (NCIC) during registration of permanent parties and at automatic registration.	AIE-3 System Performance Specification	Vet Personnel	[Multiple Requirements are delineated below]
		The System shall perform a Wants and Warrant checks through IoLS using data from National Crime Information Center (NCIC) during registration of permanent parties.	SS_200	Vet Personnel	Registration Client
		The System shall perform a Wants and Warrant checks through IoLS using data from National Crime Information Center (NCIC) during registration of permanent parties at automatic registration.	SS_200	Vet Personnel	IMM AutoReg
39	SS_201	The System shall perform a check of in-state and out-of-state law enforcement and DMV data sources using data from a driver's license captured and decoded during registration at a registration station~~, vehicle lane~~ or Handheld. (Modification) The Government does NOT want the ability to register Driver's Licenses at the Vehicle Pedestal; however, the Government wants the ability to register Driver's Licenses at a selectable HH.	AIE-3 System Performance Specification	Vet Personnel	IMM Client

40	SS_202	The System shall establish a local database of personnel information.	AIE-3 System Performance Specification	Vet Personnel	Site Server Cloud Server Cache Box
41	SS_203	The System shall maintain a list of personnel that are denied access onto the Installation. (Modification) The types of denials include Debarment, Post Driving Privileges Revoked, Duty Hours Only, and Restricted to Post. In addition, the following list of IoLS Alerts must be included in the denial type in the all denied History report: Debarment, Revocation, Suspended, Wants and Warrants, and Be On The Lookout.	AIE-3 System Performance Specification	Vet Personnel	Registration Server
42	SS_204	The System shall update user records through IoLS every 15 minutes.	AIE-3 System Performance Specification	Vet Personnel	IMM Client
43	SS_205	The System shall perform recurring Wants and Warrant checks through IoLS of enrolled personnel using data from NCIC every 15 minutes.	AIE-3 System Performance Specification	Vet Personnel	IMM Client
44	SS_206	The System shall perform verification of state issued credentials with DMV databases via the Installation's Originating Agency Identifier (ORI) connection in real-time independent of IoLS.	AIE-3 System Performance Specification	Vet Personnel	IMM Client
45	SS_207	The System shall perform initial vetting of visitors via the Installation's ORI connection to the NCIC (Interstate Identification Index (III) files), DMV, and in-state or out-of-state law enforcement sources in real-time independent of IoLS.	AIE-3 System Performance Specification	Vet Personnel	IMM Client

46	SS_208	The System shall perform re-vetting at selectable time intervals via the Installation ORI connection of enrolled personnel using data from NCIC (Interstate Identification Index (III) files), DMV, and in-state or out-of-state law enforcement sources. (Modification) The System shall perform re-vetting of visitors and guests when a new pass is generated via the Installation ORI connection of enrolled personnel using data from NCIC (Interstate Identification Index (III) files), DMV, and in-state or out-of-state law enforcement sources.	AIE-3 System Performance Specification	Vet Personnel	IMM Client
47	SS_209	The System shall deny access at the lanes and pedestrian portal to individuals who fail periodic vetting. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Vet Personnel	Symmetry Gate Controller
48	SS_210	The System shall log and produce reports of all vetting transactions including date, time, record number, and status.	AIE-3 System Performance Specification	Vet Personnel	[Multiple Requirements are delineated below]
		The System shall log all vetting transactions including date, time, record number, and status.	SS_210	Vet Personnel	SQL Server
		The System shall produce reports of all vetting transactions including date, time, record number, and status.	SS_210	Vet Personnel	Symmetry Advanced Reporting OPMG Dashboard Reports

49	SS_300	The System shall be capable of using fixed lane equipment and wireless Handheld readers to perform credential and fingerprint verification functions at ACPs.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Hawkeye Mobile CrossMatch Handheld Zebra TC72 Handheld	The Government waived the fingerprint requirement ACP operations.
50	SS_301	The System shall allow the operator from the Guard Booth or Gatehouse to switch to manual control of pedestrian and vehicular lane operations.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Visual Verify	
51	SS_302	The System shall provide continuous digital video surveillance of pedestrian portal and vehicle lanes. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry CompleteView Axis Cameras Pelco Cameras	
52	SS_303	The System shall record digital video of all access control transactions that occur in each pedestrian lane for seven days and the ability to store 180 days of events requiring intervention.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry CompleteView	
53	SS_304	The System shall provide simultaneous operation of pedestrian portal and vehicle lanes. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Symmetry Gate Controller	
54	SS_305	The System shall compare applicant information against the access denied list and alert gate guard staff when a denied individual attempts to gain access. The access denied list	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Hawkeye Visual Verify DBU Site Server	Sites not using DBU are controlled by Site Server.

		shall be automatically updated to each ACP upon status change.				
55	SS_306	The System shall read Federal PIV credentials during vehicle lane and pedestrian portal operations.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Rhino Reader Qscan Reader	
56	SS_307	The System shall provide the capability for archived video to be viewed at the Gatehouse and central remote location.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client	
57	SS_308	The System shall provide the System Administrator the capability to select the FPCON level. The System shall provide the Operators the capability to configure each lane using a selectable menu to increase the following access criteria for the FPCON requirements: automatic registration, personal credentials plus PIN, personal credentials plus fingerprint, personal credentials plus PIN and fingerprint, at any FPCON Level.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client	
58	SS_309	The System shall provide fiber optic cable from the ACP to the point of debarkation of Installation's fiber optic cable which is approximately 500 feet.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	N/A	Assigned to the physical installation process, not any component.
59	SS_310	The System shall provide the capability to produce and display reports at ACPs and central remote location.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Advanced Reporting	

60	SS_311	The System shall generate the following filterable reports: • All Denied History Report by range (name, date and time) • All Visitor Pass Report by range (name, date and time) • Individual Scan History Report by range (name, date and time) • Registered Persons Transaction Report by range (name, date and time) • ACP access/transaction Reports by range (name, date and time) • Escort Visitor Pass Report by range (name, date and time) • Personnel entered into debarment list by range (name, date and time) • Handheld report by range (name, date and time) • NCIC III transaction report by range (name, date, time and FBI Number) (Modification) The NCIC III transaction report portion of this requirement is differed.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Advanced Reporting
61	SS_312	The System shall have the capability to login and display ACP transactions at the Gatehouse.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Visual Verify
62	SS_313	The System shall have the capability for ACP, lane and Pedestrian Portal monitoring and control at the Guard Booth.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Visual Verify
63	SS_314	The System shall have the capability at the Guard Booth and Gatehouse for selectable override control of all lanes and Pedestrian Portal per ACP.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Visual Verify

64	SS_315	The System shall have the capability for selectable override control of each ACP on the Installation at the central remote location.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry Client Visual Verify	
65	SS_316	The System shall provide the capability for a FIPS 201-1 compliant wireless Handheld capable of reading PIV, PIV-I, CAC, DD Form 2, ~~DA Form 1602,~~ Defense Biometric Identification System (DBIDS), state driver's license, Transportation Worker Identification Card (TWIC) and displaying user data and image. (Modification) The portion of the requirement for a FIPS 201-1 compliant wireless Handheld is deferred until a FIPS 201-1 compliant wireless Handheld is added to the APL. DA 1602 has been removed from the System Performance Specification.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Hawkeye Mobile CrossMatch handheld Zebra TC72 Handheld	DA Form 1602 is not machine-readable and should be removed from this list.
66	SS_317	The System shall provide the capability for the wireless Handheld to operate continuously for 12 hours.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	CrossMatch Handheld Zebra TC72 Handheld	
67	SS_318	The Handheld device shall have a removable pistol grip attachment.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	CrossMatch Handheld Zebra TC72 Handheld	
68	SS_319	The System shall provide the capability for digital video storage that allows transfer to removable media.	AIE-3 System Performance Specification	Access Control Point (ACP) Processing	Symmetry CompleteView	
69	SS_320	The System shall provide a minimum lane throughput of six authorized vehicles per minute.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Gate Controller Site Server Adam Module App/DB Servers Cache Box	Sites using Qscan do not use Symmetry Gate Controller.

70	SS_321	The System shall read, capture, and decode data encoded on a driver's license or state issued identification card at the vehicle lane and with the handheld.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	[Multiple Requirements are delineated below]	
		The System shall read, capture, and decode data encoded on a driver's license or state issued identification card at the vehicle lane.	SS_321	Process Personnel at Vehicles Lanes	Rhino Reader Qscan Reader	
		The System shall read, capture, and decode data encoded on a driver's license or state issued identification card with the handheld.	SS_321	Process Personnel at Vehicles Lanes	Hawkeye Mobile CrossMatch Handheld Zebra TC72 Handheld	
71	SS_322	The System shall enable permanent party and visitors to enter through the lanes using permanent party credentials or temporary visitor passes issued or accepted at the time of registration.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Rhino Reader Qscan Reader	
72	SS_323	The System shall grant access at the ACP according to the highest level of access permitted by any of the classes to which the user belongs.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Site Server Cloud Server	
73	SS_324	The System shall read and display to the lane control guard a real-time image of the driver's face as the credential is presented.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Hawkeye Visual Verify	
74	SS_325	The System shall display a stored image of the driver from the local database to the lane control guard and deny automated access when not available.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Symmetry Gate Controller Hawkeye Visual Verify Hawkeye IMM Adam Module	Qscan uses Hawkeye VV, IMM and ADAM Module
75	SS_326	The System vehicle lane digital video surveillance subsystem shall record the vehicle driver's face, during vehicle lane transaction, ranging from a	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry CompleteView Stentofon TCIV-3+	

		height of 3ft. to 7ft. from the ground and 30 inches from the face plate of the camera. (Modification) The Government clarifies that the length from the pedestal is 30 inches from the face plate of the camera.			
76	SS_327	The System shall display a real time video or image to the lane control guard of the vehicle rear license plate.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client
77	SS_328	The lane digital 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.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry CompleteView NVR
78	SS_329	The System shall enable authorized personnel to access enrollment records and electronic entry control equipment.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Visual Verify Site Server App/DB Servers Hawkeye IMM
79	SS_330	The System shall prominently identify to the lane control guard whether the driver is allowed Trusted Traveler privileges.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Hawkeye Visual Verify GBWS
80	SS_331	The System shall prominently display information to the Gatehouse and Guard Booth for all events where vehicle operators do not match with registered information or are invalid and the guard is prompted to manually check or stop the vehicle.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Hawkeye Visual Verify
81	SS_332	The System shall display description information to the Guard Booth, Gatehouse, and central remote location for all access denial events.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Hawkeye Visual Verify

82	SS_333	The System shall provide an integrated traffic light (green, red).	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Traffic Light	
83	SS_334	The System shall provide a traffic hold capability that allows the Lane Guard to hold all traffic and allow a vehicle to turn around.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Client Visual Verify ADAM Module Symmetry Gate Controller	
84	SS_335	The System gate arm shall not rise automatically, and traffic light remains red for drivers who are denied Trusted Traveler privileges.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry Gate Controller Hawkeye IMM	Sites using Qscan using Hawkeye IMM
85	SS_336	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.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm Visual Verify Symmetry Client ADAM Module	
86	SS_337	The System shall generate a signal capable of indicating alarm conditions to remote workstations and Installation's Intrusion Detection System if a vehicle crashes into the traffic arm when it is in the down position.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm Symmetry Gate Controller	
87	SS_338	The traffic arm controller shall have a ~~waterproof~~ resistant housing. (Modification) The Government will accept "water resistant housing" vice "waterproof housing."	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	
88	SS_339	The traffic arm assembly shall be capable of manual override operation in the event of a malfunction due to mechanical failure, main power outage	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	

		and/or backup power supply failure.				
89	SS_340	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.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	
90	SS_341	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.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	
91	SS_342	Each traffic arm shall be equipped with an obstruction detector that will automatically reverse the traffic arm motor when an obstruction is detected.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	An optical sensor is part of the Gate Arm assembly
92	SS_343	The traffic arm shall be covered with retro reflective red and white sheeting. See FHWA SA-89-006 for proper orientation of sheeting.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Gate Arm	
93	SS_344	The System shall have the capability to scan and compare fingerprint and display results at the vehicle lane.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Rhino Reader CrossMatch Handheld	Qscan does not have a keypad for PIN or bio-scanner for fingerprint. Per the Government, pin and fingerprint no longer applicable to ACP operations.
94	SS_345	The System shall provide for connectivity of the portable registration station via a hardwired data connection to	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Portable Reg System	

		the Installation registration database for vetting.				
95	SS_346	The System shall digitally capture the front, driver, and license tag of the vehicle.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	Symmetry CompleteView Cameras	
96	SS_347	The System shall provide the capability for the license plate camera to read and store the license plate information. (Modification) The requirement to read and store the alpha numeric characters is deferred to an undetermined future release.	AIE-3 System Performance Specification	Process Personnel at Vehicles Lanes	ALPR	ALPR capability available but not in use
97	SS_348	The System shall provide a minimum ACP pedestrian throughput rate of three authorized personnel per minute per lane. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Symmetry Gate Controller Hawkeye IMM ADAM Module	Hawkeye IMM and ADAM Module used with Qscan.
98	SS_349	The System pedestrian portal digital video surveillance subsystem shall record each pedestrian's face. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Symmetry CompleteView Stentofon TCIV-3+	
99	SS_350	The System shall provide for a two-way intercom capability from the pedestrian portal with a selected Guard Booth at the ACP or the Gatehouse or the Central Remote Location. If	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Stentofon AlphaCom	

		the selected communication point does not respond, the system shall rollover from the selected communication point to the Gatehouse and then to Central Remote Location. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.				
100	SS_351	The System shall be able to read approved credentials and display the credential information to the gate control guards during pedestrian processing. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Rhino Reader Qscan Reader	
101	SS_352	The System shall require an approved credential and successful input of a PIN to allow pedestrian entrance to the portal/turnstile at lower FPCON levels. At higher FPCON levels, the System shall require a fingerprint feature. (Modification) The Government defers the Pedestrian Portal portion of the requirement until such time as an Installation requires implementation of the solution.	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Rhino Reader Qscan Reader Symmetry Gate Controller	Qscan does not have a keypad for PIN or bio-scanner for fingerprint. Per the Government, pin and fingerprint are no longer applicable to ACP operations.
102	SS_353	The system shall provide the capability for the system administrator to download and save filterable reports in Excel and Word format to CD drive.	AIE-3 System Performance Specification	Process Personnel at Pedestrians Gates	Symmetry Advanced Reporting	

103	SS_400	The System shall provide alarm notification to the central remote station when non-routine conditions such as tampering, equipment failures, or electrical power failures occur. Tamper notifications are not required on equipment housed in secure server facilities.	AIE-3 System Performance Specification	Physical Security	Symmetry Client	
104	SS_401	The System shall employ tamper switches that are inaccessible until the switch is activated; have mounting hardware concealed so that the location of the switch cannot be observed from the exterior of the enclosure; and be connected to circuits which are always under electrical supervision.	AIE-3 System Performance Specification	Physical Security	Enclosures	
105	SS_402	The System shall provide secure switches and control features.	AIE-3 System Performance Specification	Physical Security	Enclosures	
106	SS_403	The ACP local processor shall be capable of automatically restoring communication within 10 seconds after an interruption with the field device network that is internal to AIE.	AIE-3 System Performance Specification	Physical Security	Symmetry Gate Controller DBU	ACP Local processor is the DBU which is not used with AIE-4 deployments.
107	SS_404	The local processor shall store a minimum of 10,000 transactions during periods of communication loss between the ACP server and site server.	AIE-3 System Performance Specification	Physical Security	Symmetry Gate Controller DBU	ACP Local processor is the DBU which is not used with AIE-4 deployments.
108	SS_405	The ACP local processor shall be able to support the number of alarm inputs needed by the System for all lanes at the ACP, with a maximum of eight alarm inputs.	AIE-3 System Performance Specification	Physical Security	Symmetry Gate Controller DBU ADAM Module	ACP Local processor is the DBU which is not used with AIE-4 deployments.

109	SS_406	The System shall be capable of reporting alarm conditions that remain off normal for periods exceeding 500 milliseconds.	AIE-3 System Performance Specification	Physical Security	Symmetry Gate Controller	
110	SS_407	The System shall provide an alarm notification within three seconds of unauthorized attempts to access the Installation or System component failure (tamper, power failure, or System failure).	AIE-3 System Performance Specification	Physical Security	Symmetry Gate Controller	
111	SS_408	The System shall integrate with the Installation's Intrusion Detection System for notification and reporting alarms.	AIE-3 System Performance Specification	Physical Security	Site Server	
112	SS_409	The System shall implement the security controls of DoD Instruction (DoDI) ~~8500.2~~ 8510.01 (IA Implementation) commensurate with a Mission Assurance Category (MAC) II sensitive level System and AR 25-2, (IA) and display a privacy act statement at appropriate user interfaces. (Modification) DODI 8500.2 is obsolete and has been replaced by DODI 8510.01. This change also supports The DoD Information Assurance Certification and Accreditation Process (DIACAP) to RMF change noted at SS 410.	AIE-3 System Performance Specification	Information Security	All servers and network devices	
113	SS_410	The System shall implement System security measures sufficient to attain an Authorization to Operate (ATO) IAW DoD Information Assurance Certification and Accreditation Process (DIACAP) per the DoDI	AIE-3 System Performance Specification	Information Security	All servers and network devices	This requirement should be updated to reflect Risk Management Framework (RMF) process.

		8510.01 (DIACAP), AR 25-2 and the Chief Information Officer (CIO)/G6 Office of Information Assurance and Compliance, Certification and Accreditation (C&A) Best Business Practice dated March 2012.			
114	SS_411	~~The System shall implement System security measures sufficient to attain a Certificate to Operate through the Network Command (NETCOM) Certificate of Net worthiness (CoN) process.~~ (Modification) Remove: CoN process absorbed by RMF process for DoD IT systems.	AIE-3 System Performance Specification	Information Security	All servers and network devices
115	SS_412	The System shall use secure encrypted communications over the network of at least AES-256.	AIE-3 System Performance Specification	Information Security	All servers and network devices
116	SS_413	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, ~~DoD 8500.2 "Information Assurance (IA) Implementation," dated February 6, 2003,~~ DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," dated April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, dated June 2, 2006, DoD Policy Memorandum, "Department of Defense	AIE-3 System Performance Specification	Information Security	SQL Server

		Guidance on Protecting Personally Identifiable Information (PII)," dated August 18, 2006 and DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," dated April 18, 2006. (Modification) Deleted reference to DoD 8500.2 "Information Assurance (IA) Implementation," dated February 6, 2003,				
117	SS_414	The System shall ensure data concurrency of all System components among physical installations with secure network connectivity and be able to store encrypted data or eliminate duplicate information.	AIE-3 System Performance Specification	Information Security	SQL Server	
118	SS_415	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).	AIE-3 System Performance Specification	Information Security	WSUS DoD Patch Repository	External System Accessible to AIE via the LANDWARNET
119	SS_416	The System shall provide Host Based Security System (HBSS), per JTF-GNO CTO 07-12.	AIE-3 System Performance Specification	Information Security	HBSS ePO	External System Accessible to AIE via the LANDWARNET
120	SS_417	The System shall provide a hierarchical Organizational Unit (OU) structure that is adaptable and sustainable.	AIE-3 System Performance Specification	Information Security	AD Domain Controller	
121	SS_418	The system shall provide the capability that is enabled to use PKI certificates (CAC logon) on workstations, servers, and tools for managing, renewing, and revoking certificates and	AIE-3 System Performance Specification	Information Security	Windows 10 OS DoD CAC Validation	External System Accessible to AIE via the LANDWARNET

		related services and support IAW DoD Policy for Public Key Infrastructure (PKI) and Public Key (PK) Enabling.			
122	SS_500	The System shall provide Uninterruptible Power Supply (UPS) to supply power to the AIE System in the event of power loss. The 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. The 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. (Modification) The Government does not require nor desire an UPS for the Portable Registration Workstation.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	UPS
123	SS_501	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.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	ACP and Lane equipment
124	SS_502	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	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	ACP and Lane equipment

		hours. A critical failure is defined as a failure that renders a System unusable. The System becomes unusable when the System cannot automatically validate or verify the credentials presented at the ACP.			
125	SS_503	The System (one ACP with two vehicle lanes) shall be configured and installed to operate continuously and yield an Operational Availability (Ao) of 97%. Ao 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).	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	ACP and Lane equipment
126	SS_504	The System shall have an Ao of 97% per pedestrian portal.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	ACP and Lane equipment
127	SS_505	The probability of the System granting entry to an unauthorized individual (false acceptance rate) shall be less than 0.1 percent.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Symmetry Gate Controller ADAM Module Hawkeye IMM

128	SS_506	The probability of the System denying entry to an authorized individual (false rejection rate) shall be less than 1.0 percent.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Symmetry Gate Controller ADAM Module Hawkeye IMM	
129	SS_507	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.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Symmetry Gate Controller ADAM Module Hawkeye IMM Gate Arm	
130	SS_508	The System shall allow for upgrades of hardware and software with minimal System disruption and cost.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Applies to all	Applies to all.
131	SS_509	The System shall maintain spares for all mission critical components that are readily available to field users.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Applies to all	Applies to all.
132	SS_510	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 to perform operator level maintenance.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Applies to all	Applies to all.
133	SS_511	The System shall be designed so that personnel can operate the System with no more than eight hours of initial or refresher training.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Symmetry Client	
134	SS_512	The Registration System shall have an Ao of 97% (the Registration System as defined for RAM shall be two Registration Workstations).	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Registration Client Registration Server	

135	SS_513	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.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Registration Client Registration Server
136	SS_514	The Site Server System shall have an Ao of 97% (the Site Server System as defined for RAM shall consist of the Primary and Secondary Site Servers).	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Site Server Cloud Server
137	SS_515	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.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Site Server Cloud Server
138	SS_516	The System shall conduct a graceful shutdown in the event of power loss and automatically restart upon restoration of power. (Modification) This requirement does not pertain to Primary and Secondary Site Servers when UPS power is required to be provided (and is provided) via Installation UPSs.	AIE-3 System Performance Specification	Reliability, Availability and Maintainability (RAM)	Site Server
139	SS_600	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.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures

140	SS_601	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.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures
141	SS_602	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.	AIE-3 System Performance Specification	Environmental Conditions	Cache Box Workstations Stentofon Alphacom
142	SS_603	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.	AIE-3 System Performance Specification	Environmental Conditions	Guard Booth Workstation Stentofon Dual Disp Mstr
143	SS_604	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.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures
144	SS_605	The System components shall be rated for continuous operation when exposed to rain as specified in National Electrical Manufacturing	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures

		Association (NEMA) 250, winds up to 137 km/hr and snow cover up to 610 mm measured vertically.				
145	SS_606	All exterior System components shall be operable in precipitation of up to two inches/hour.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures	
146	SS_607	All System components shall be operable in icing conditions.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis CameraEnclosures Pelco Camera Enclosures	
147	SS_608	All exterior components shall withstand exposure to solar ultraviolet radiation without performance degradation for a period of 10 years.	AIE-3 System Performance Specification	Environmental Conditions	Rhino Reader Qscan Reader Stentofon TCIV-3+ Axis Camera Enclosures Pelco Camera Enclosures	
148	SS_609	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.	AIE-3 System Performance Specification	Environmental Conditions	Applies to all	Applies to all.
149	SS_610	The System shall provide protective housing enclosures for interior electronics IAW NEMA 250 Type 12.	AIE-3 System Performance Specification	Environmental Conditions	Applies to all	Applies to all.
150	SS_700	The System shall be safe to operate and maintain.	AIE-3 System Performance Specification	Safety	Applies to all	Applies to all.
151	SS_701	All System components shall be protected against the effects of lightning, power surges and stray electrical charges or emissions.	AIE-3 System Performance Specification	Safety	Applies to all	Applies to all.

152	SS_702	The System shall protect personnel against electrical shock.	AIE-3 System Performance Specification	Safety	Applies to all	Applies to all.
153	SS_703	The System shall operate using local commercial power.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
154	SS_704	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.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
155	SS_705	The System shall have non-proprietary interfaces.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
156	SS_706	The System components shall be interoperable, modular, and scalable products that can be tailored to accommodate future hardware and software upgrades.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
157	SS_707	The System shall consist of commercial components.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
158	SS_708	System computers shall be state-of-the-market.	AIE-3 System Performance Specification	Physical Characteristics	Site Server AIE Enterprise Data Center Cache Box All workstations	
159	SS_709	The System shall provide nameplates for major components of the System. Nameplates shall have the manufacturer's name, address, type or style, model or serial number identified on the equipment.	AIE-3 System Performance Specification	Physical Characteristics	Applies to all	Applies to all.
160	SS_710	The System shall have the capability for the Installation Commander or authorized security official to electronically configure the System to require varying combinations of	AIE-3 System Performance Specification	System Design	Symmetry Client	

		identification for each threat condition or FPCON level.				
161	SS_711	The System shall be able to quickly change from one FPCON level to another and apply the corresponding required combination of forms of identification for controlling vehicle and pedestrian access.	AIE-3 System Performance Specification	System Design	Symmetry Client	
162	SS_712	The System shall have the capability to process an approved credential and successful input of a PIN; approved credential and fingerprint to allow vehicle entrance at higher FPCON levels.	AIE-3 System Performance Specification	System Design	Rhino Reader Qscan Reader (not FP or PIN) Site Server App/DB Servers Symmetry Gate Controller	Qscan does not have a keypad for PIN or bio-scanner for fingerprint. Per the Government, pin and fingerprint no longer applicable to ACP operations.
163	SS_713	The System shall be able to securely create, store, update, and delete PIR data for all registrants.	AIE-3 System Performance Specification	System Design	Symmetry Client Hawkeye IMM	
164	SS_714	The System shall be capable of identifying and removing duplicate PIR data for registrants.	AIE-3 System Performance Specification	System Design	Symmetry Client Hawkeye IMM	
165	SS_715	The System shall be able to immediately communicate PIR data to each ACP, each automated entrance lane to include Handhelds and the Visitor Control Center (VCC).	AIE-3 System Performance Specification	System Design	Symmetry Server Sync Hawkeye IMM	
166	SS_716	The System shall provide uninterrupted entry control processing despite loss of data connectivity from the network or site server.	AIE-3 System Performance Specification	System Design	Cache Box	
167	SS_717	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.	AIE-3 System Performance Specification	System Design	Symmetry Client	

168	SS_718	The System shall provide pre-established reports and user-defined and user- configurable formatting for all reports.	AIE-3 System Performance Specification	System Design	Symmetry Client Symmetry Advanced Reporting	
169	SS_719	The System shall record date, time, location, and identity of all personnel granted access in the access control events records.	AIE-3 System Performance Specification	System Design	Symmetry Gate Controller	
170	SS_720	The System shall store access control event records for 30 days. NCIC III transaction records shall be stored for three years. (Modification) This requirement is deferred until a decision is made by the Government on NCIC III reports and transactions.	AIE-3 System Performance Specification	System Design	SQL Server	NCIC III transactions are stored at LE Vetting Service.
171	SS_721	The System shall conform to National Fire Protection Association (NFPA) 70 standards.	AIE-3 System Performance Specification	System Design	Applies to all	Applies to all.
172	SS_722	The System shall be able to discriminate between individual switches, sensors, entry control devices, and report status to the Network Management Workstation, Central Remote Station and Registration Station.	AIE-3 System Performance Specification	System Design	Symmetry Gate Controller Site Server	
173	SS_723	The System will utilize a maximum of 65% of the provided computer memory, storage, and computing speed.	AIE-3 System Performance Specification	System Design	Site Server AIE Enterprise Data Center Cache Box All workstations	
174	SS_724	The System shall be able to access the registration data of all other facilities within the AIE network. (Modification) These requirements are deferred until an Enterprises solution exists.	AIE-3 System Performance Specification	System Design	Enterprise servers Symmetry Server Sync	

175	SS_725	The System shall provide remote monitoring and control of all ACPs from the central remote on the Installation ~~location~~ (Modification, “on the Installation”).	AIE-3 System Performance Specification	System Design	Symmetry Client Visual Verify	Duplicate of SS_729.
176	SS_726	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, Credential Only, Credential and fingerprint, Credential and PIN.	AIE-3 System Performance Specification	System Design	Site Server Symmetry Gate Controller	
177	SS_727	The System shall provide the capability to count and tally vehicle entry per ACP per vehicle lane.	AIE-3 System Performance Specification	System Design	SQL Server	
178	SS_728	The System shall provide the capability to import an access denied list from a text file, Excel spreadsheet, or document format into the AIE System and vet against that list.	AIE-3 System Performance Specification	System Design	Registration Client	
179	SS_729	(Deleted by Government as duplicate of SS_725 on 10/27/2017)	AIE-3 System Performance Specification	System Design	Symmetry Client	Duplicate of SS_725.
180	SS_730	The System shall have the capability for the ACP Gatehouse, Guard Booth, and central remote location to login to the System and use touch screen technology to control/override ACP transactions.	AIE-3 System Performance Specification	System Design	Symmetry Client Visual Verify	
181	SS_731	The System shall provide the capability for all credential readers to be equipped with visual and audible feedback when credential is read.	AIE-3 System Performance Specification	System Design	Rhino Reader Qscan Visual Verify Symmetry Client	

182	SS_732	The System should not register the same person more than once.	AIE-3 System Performance Specification	System Design	Registration Server	
183	SS_733	The System shall provide software installer packages.	AIE-3 System Performance Specification	System Design	Symmetry Hawkeye	
184	SS_734	The System shall provide the capability for the Guard Booth to monitor and control multiple vehicle lanes using the AIE System.	AIE-3 System Performance Specification	System Design	Symmetry Client Visual Verify	
185	SS_735	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. Gate crash and tail gate alarms are inactive.	AIE-3 System Performance Specification	System Design	Symmetry Gate Controller Symmetry Client Hawkeye Mobile	
186	SS_736	The System shall provide for a two-way intercom capability between the vehicle lane and Guard Booth at the ACP or the Gatehouse or the Central Remote Location. If the Guard Booth does not respond, the system shall rollover to the Gatehouse. If the Gatehouse does not respond, the system shall rollover to the Central Remote Location.	AIE-3 System Performance Specification	System Design	Stentofon AlphaCom	
187	SS_800	The System shall be designed to integrate with existing infrastructure and networks.	AIE-3 System Performance Specification	External Interfaces	Applies to all	Applies to all.
188	SS_801	The System shall use standard communication protocols and communication links of CONUS Installations.	AIE-3 System Performance Specification	External Interfaces	Applies to all	Applies to all.
189	SS_802	The System shall verify the fingerprint read at the pedestrian lane with that in the registration database and	AIE-3 System Performance Specification	External Interfaces	Rhino Reader	Qscan does not have a keypad for PIN or bio-scanner for fingerprint. Per the

		provide the match result within 5.0 seconds.				Government, pin and fingerprint no longer applicable to ACP operations.
190	SS_803	The System shall verify the fingerprint read at the vehicle lane and wireless Handheld device against registration database and provide results within 5.0 seconds.	AIE-3 System Performance Specification	External Interfaces	Rhino Reader Hawkeye Mobile CrossMatch Handheld Zebra CT72 Handheld	Per the Government, pin and fingerprint no longer applicable to ACP operations.
191	SS_804	(Deleted by Government as duplicate of SS_811 on 10/27/2017).	AIE-3 System Performance Specification	External Interfaces	IMM Client	Duplicate of SS_811.
192	SS_805	The System shall provide CAC enabled server computers and all workstations except at the Guard Booth and Gatehouse.	AIE-3 System Performance Specification	External Interfaces	Site Server Selected workstations	
193	SS_806	The System program software shall electronically connect to the enterprise servers to transmit and receive user data (Modification) This requirement is deferred until an Enterprises solution exists.	AIE-3 System Performance Specification	External Interfaces	Hawkeye Synchronization Service Cloud Server Cache Box	An Enterprise solution currently exists.
194	SS_807	The System program software shall electronically connect to IoLS for access to authoritative databases.	AIE-3 System Performance Specification	External Interfaces	IMM Client	
195	SS_808	The System shall provide the capability to selectively share access denied list/debarment lists with IoLS.	AIE-3 System Performance Specification	External Interfaces	IMM Client	

196	SS_809	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 the following three categories: 1. Does not have a digital identity in DoD-wide DEERS 2. Does not have a DoD ID card 3. 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.	AIE-3 System Performance Specification	External Interfaces	IMM Client	
197	SS_810	The System shall provide the capability to electronically share local population information with other DoD and federal Systems.	AIE-3 System Performance Specification	External Interfaces	IMM Client	
198	SS_811	The System program software shall electronically connect to in-state and out-of-state law enforcement and (Modification, “in-state and out-of-state”) DMV data sources.	AIE-3 System Performance Specification	External Interfaces	IMM Client	
199	SS_812	The System shall be capable of providing a standard interface for data interchange that complies with the Security Equipment Integration Working Group (SEIWG) 0101 series Interface Control Document.	AIE-3 System Performance Specification	External Interfaces	JIGSAW for Symmetry	JIGSAW is a Government-owned SEIWG 0101 compliant tool.

		(Modification) add "…be capable of providing".				
200	SS_813	The contractor shall implement Internet Protocol version 6 (IPv6) on public-facing servers and services providing for dual stack operations of IPv4 and IPv6 in parallel.	AIE-3 System Performance Specification	External Interfaces	Does Not Apply to AIE-3/4 Servers	Applies only to Visitor Web Registration Server.
201	SS_814	The System shall be capable of providing an external interface via an Ozone Widget Framework-compatible widget. This widget web app shall serve as an interface with Command Nodes to provide FPCON level and operational status of data elements for access control point lanes at Army Installations. It shall provide for both query and update. The address portion of the widget shall be configurable to enter the external system information. (Modification) add "…be capable of providing".	AIE-3 System Performance Specification	External Interfaces	Ozone for Symmetry	Contractor to develop an Ozone Widget Framework compatible widget.

Figure 2: Requirements Traceability Matrix

6. Software Design Description

In accordance with DID DI-IPSC-81435A, the AIE-3/4 Software Design Description (SDD) is described in this section. Typically, the SDD is a highly detailed document that describes a software development project down to the subroutine. However, since AIE-3/4 is not a software development program, but a system of systems that makes use of commercial-off-the-shelf products that are completely owned and copyright protected by the respective manufacturers, this SDD will instead describe the software components of the solution, the interaction with other software and hardware elements and the interfaces defined between them.

6.1. COTS Software Component Identification

As described in the DODAF operational and system viewpoints (Appendices A through EE) the AIE-3/4 system is made up of key operational building blocks: Installation-wide PIR data store, registration function, system monitoring, and one or more ACPs. The ACPs also support a registration capability. Cloud-based sites generally add a local Cache Box to allow continued processing of previously registered users in the event of a loss of cloud communications or capabilities. These building blocks are each implemented through one or more COTS software and hardware products. The following paragraphs describe the software components that make up the AIE-3/4 solution in the context of the top-level operational function they perform.

6.2. Registration

The registration function is accomplished through the Hawkeye Registration software from Hawkeye Technologies. Hawkeye software allows multiple clients to connect to the Site Server/Cloud Server and the Hawkeye IMM Client to support the Registration function. The Hawkeye Registration software uses a combination of web services published by the Site Server/Cloud Server and direct database reads and writes. The details of the communication between client and server are not published by Hawkeye and are not included in this document; however, it can be stated that the Registration client software serves to collect the PIR data from the user, package the information in a format utilized by the Symmetry Data Connect module and passed to the Site

Server/Cloud Server over the network. The data model that represents the collected PIR data is included in Appendix K, Data Information Viewpoint DIV-2. The server component is installed on the Site Server/Cloud Server cluster as a SQL database server. The Hawkeye IMM Client imports the PIR data into the Symmetry Installation-wide PIR data store (see section 6.3 below).

Another component available to AIE-3/4 Installations is the use of a Visitor Registration Web Site. This web site interfaces to the Hawkeye IMM Client running on the Site Server to collect initial biographical information from the registrant that is used to speed the process of operator-assisted registration.

During the registration process, three (3) types of data sets are collected and sent to the server. The information is stored in different tables in the PIR database.

- Person and Vetting Information
- Credential Information
- Access Information

The data relationships are such that each person may have one or more credentials (for example, a Retiree card and a Contractor CAC), one or more accesses (for example, to ACP 1 and ACP 2), and one or more vetting results.

Person Information

Person information consists of the biographic and biometric data associated with the identity. Common biographic elements are items such as name, date of birth, contact information, etc. Common biometric elements are picture, fingerprint templates, and signature image. Vetting information typically includes the vetting source checked, the time of the check, and the result of the check.

PIR and Credential Information

The Credential is the object that will be presented by the user at the ACP to request access. The AIE-3/4 PIR Database supports multiple credential types, such as CAC cards, Teslin/Retiree cards, Local Badges, Drivers Licenses, DBIDS visitor cards, and RFID tokens.

The Personal Information Record (PIR) passed to the server includes a unique credential identifier, a Begin and End date, and other details as defined in DODAF Viewpoint DIV-2 (see Appendix K).

Access Information

The access represents the instance of privilege for AIE. It combines the Person information, the credential information, and a privilege level for that person at that facility. Each person can only have one set of access rights per Installation at the same time. Each access will have a start/end date, a credential, and a set of privileges for the local AIE-3/4 System. Only after registration and vetting is the access information sent to the Symmetry PIR data store.

To collect the PIR data, the registration software interfaces with various peripheral devices such as barcode scanners, fingerprint scanners, signature pads, PIN pads, and webcams. The interfaces to these devices are published by the respective device manufacturers but are not duplicated here.

6.2.1 Portable Registration

A portable registration workstation works the exact same way as a standard registration workstation.

6.2.2 Kiosk

Two types of Kiosks are provided. The original Kiosk is an all-in-one computer and monitor combination that allows users who have lost or forgot their CAC or previously

issued passes to obtain a one-day pass. In addition, this Kiosk is used to register RFID cards for sites where they are used but is no longer being deployed.

Kiosk 2.0 is an all-in-one free-standing unit manufactured by Iberon. These units allow applicants to use a driver's license or passport to register for passes of up to eight days (based on reason for visit). Applicants are vetted through Iberon's NCITE vetting service and if they pass the vetting process are issued passes at the kiosk. These passes are registered into the AIE system when they are scanned in lane.

6.2.3 Online Vetting and Registration

Online Vetting and Registration is a vital element of the Army's Visitor Control Program. It provides seamless processing of visit requests to Army Installations while minimizing the need for visitors to enter the Visitor Control Center (VCC). Applicants are vetted through Iberon's NCITE vetting service, IoLS, and the Installation's Local Debarment List to complete the access determination process. Having a single AIE enterprise Visitor Portal allows visitors to an Army Installation a single location to begin the visitor request process.

6.3. Installation-wide Data Store

The Symmetry Security Management Software from AMAG Technology is used to manage the Installation-wide Data Store. Symmetry creates multiple databases in the SQL Server including one specifically for transaction storage and another that includes the PIR data in several tables. AMAG publishes the interface, known as Data Connect, and this document is referenced. Data from Hawkeye Registration software and IMM Client and other such external sources are imported into a specialized Import database where data undergoes an integrity and validation check. The data is moved to the PIR data store if authorized.

The Hawkeye Synchronization Services identifies new or modified PIR records as they are queued for storage in the database. For small sites with a Cache Box, this information is moved to the appropriate Cache Box. A field in the PIR record called the

"ACP Mask" indicates to the Synchronization service which ACPs should receive the new data. This process works on an on-demand basis.

6.4. Identity Management Middleware (IMM)

The Identity Management Middleware is from Hawkeye Technologies and is designed to connect to external vetting sources such as IoLS and LE Vetting sources for credential validation and identity vetting. The response is logged and returned to the requestor. The Registration software and the IMM Automatic Registration at the vehicle lane or pedestrian turnstile each interface with the IMM Client to route requests for vetting and validation. IMM logs all transactions, and imports alarm information into the Installation-wide data store.

The structure of IMM is such that adding new vetting sources is relatively easy to do and does not cause disruption to the existing architecture. For instance, to validate legacy AIE-2 credentials, IMM was updated to allow the legacy database to be utilized as a new authoritative vetting source.

6.5. Removed

6.6. ACP Physical Access

For Tier 1 sites the Site Server primarily runs the Symmetry Security Management System software. This software utilizes client-server architecture to provide scalability – multiple Symmetry clients can be connected to the same server. Equivalently, multiple local processors can be connected to the same server. The local processor works in conjunction with the Symmetry Gate Controllers to receive signals from the lane equipment such as vehicle detection, tamper or crash detection for sites that are not using Qscan. The Symmetry Gate Controller also controls the gate arm going up or down and the traffic light changing from red to green. For sites with Qscan, an ADAM module and relay control these functions.

For Tier 2 Sites a cloud-based configuration is used to provide the needed computing resources. The AIE Enterprise Data Center is a collection of virtual machines that provide server computing for the AIE-3/4 system in the cloud. The Domain Controllers provide security authentication and verify user access into the AIE Enterprise Data Center. The App/DB Servers provide analogous server computing as the Tier 1 onsite Site Server and are referred to in this document as the Cloud Server.

The Support Servers are virtual machine servers that provide a variety of capabilities that support and span the AIE-3/4 enterprise:

- Assured Compliance Assessment Solution (ACAS) - Vulnerability scanning mandated for DoD
- System Center Configuration Manager (SCCM) – System updates and patches
- Splunk – System Monitoring and Reporting
- SolarWinds – Network Monitoring and Reporting
- SOTI – Mobile Device Management
- OPMG – Installation scan, registration, and denials reporting

Note: There are some AIE 58 large sites that are considered Tier 2 sites, however they use on-premises Site Servers instead of the Cloud Servers.

6.6.1. Lane Control Client

The Symmetry Lane Control Client software provides the graphical user interface for the guards using AIE-3/4. The client is tailored to present a view that is familiar and informational to the guard. The same client is used for the Remote Central Monitoring function and the Gatehouse guard functions. The client either requires the guard to log into the application, or the application is automatically launched into Kiosk mode for administration.

The common operating picture (COP) presented by the Symmetry Lane Control Client shows one or more lanes being managed by the guard, live video stream from available cameras (for vehicle lane this is front of vehicle, rear of vehicle, and driver face; but for a pedestrian lane it would be face and overview camera), the user's photo from the PIR record stored in the database, the credential information and additional pertinent

information about the user prominently displayed such as Trusted Traveler status, valid or invalid credential, etc. In addition to the COP the Lane Control Client provides interactive icons for the guard to use in the normal course of their duties. Icons include the ability to raise or lower the gate arm, and ability to command a traffic hold to allow a denied vehicle the opportunity to turn around.

The COP on the Handheld is defined based on Tier 2 architecture (no lane control equipment, no traffic light, gate arm, pedestal reader, cameras, or intercom). Therefore, the HH COP shows the PIR data record information – a picture of the credential owner from the PIR database, name, expiration date of the token, and where appropriate, service and rank.

The Symmetry Client ascertains operator privileges from the Site/Cloud server. If the login credentials used are for an individual of higher administrative level, then this operator may have the ability to change threat condition (FPCON) for the system. They may have the ability to configure the rules that are applied to the hardware components of the gate operations system.

6.6.2. IMM AutoReg

The Automatic Registration function is another piece of software that runs at the Site/Cloud Server. This software can control several Rhino Readers and Qscan Readers simultaneously. As a reader notifies the AutoReg software of a credential, the software simply provides the reader with the next step in the process. The AutoReg software works with the Rhino Readers and Qscan Readers as well as with the Handhelds to perform the automatic registration function.

IMM AutoReg works with all AIE-3/4 supported credentials. If a DoD credential is submitted, AutoReg sends this to IMM Client for vetting against IoLS. If a driver's license is submitted, AutoReg sends this to IMM Client for vetting against LE and DMV sources. Note: AIE-3/4 supports the ability to automatically register driver's licenses in

lane, however, based on U.S. Army or base commander policy this feature may be disabled.

6.6.3. Handheld

Handheld functionality is offered through a variety of Android compatible devices (i.e., CrossMatch Verifier Sentry and Zebra CT72). The software that runs on the handheld devices is Hawkeye Mobile from Hawkeye Technologies (same manufacturer that supplies the IMM Client software). Hawkeye Mobile performs lane functions such as credential validation without storing PIR data at the device. The device is in wireless communication with the Site/Cloud Server or Cache Box to access the PIR Data Store and gather the data from there for display to the handheld operator. In this manner, the handheld operates independently of the vehicle lane hardware allowing operational modes such as using the handheld in addition to the lane hardware.

6.6.4. Visual Verify

Hawkeye Visual Verify is an application that provides viewing of the access determination resulting from card reads from IP based card readers (e.g., Qscan and RFID) on the GBWS, GHWS and CMWS. Color coded visual queuing is provided to guard personnel to facilitate rapid acknowledgement of access determination outcomes. Green backgrounds indicate a trusted traveler, red backgrounds indicate security alert, and blue backgrounds indicate a non-trusted traveler. In addition to the access determination, Visual Verify provides interactive icons for the guard to use in the normal course of their duties. Icons include the ability to raise or lower the gate arm, and ability to command a traffic hold to allow a denied vehicle the opportunity to turn around.

6.6.5 Symmetry CompleteView

Symmetry CompleteView provides a video display capability from multiple in lane cameras to the GBWS, GHWS, and CMWS. Video from in lane cameras is displayed through the identity verification panel in Symmetry Complete View. Symmetry Complete View presents each camera’s video in a separate window

6.6.6 Mobile Device Management (MDM)

MDM solutions provide several key features to ensure centralized proper control and management of the mobile devices in the enterprise to include tracking of physical assets, managing and upgrading applications, applying necessary access controls and security policies, and locking down devices to keep data and devices safe and secure.

The SOTI MobiControl software suite provides the MDM capability for AIE-3/4. The suite consists of a centralized server application that is hosted in the cloud with a Web Service console that provides an enterprise view of all mobile devices that have the SOTI MobiControl agents resident on them.

6.6.7 Iberon Kiosk Software

Iberon Kiosk Software supports operations of VCC Kiosk 2.0. It manages input of user information, control of built-in Kiosk devices (camera for biometric capture, credential and passport reader, and external communications with vetting services.

7. Interface Requirements Specification

In accordance with DID DI-IPSC-81434A, the AIE-3/4 Interface Requirements Specification (IRS) is described in this section.

7.1. Interface Identification

The AIE-3/4 System components are identified in section 1.4. The associations among different components indicate interfaces. The following table identifies the interfaces including in place site existing/provided components (e.g., Gate Arm, Entry Loop, Exit Loop, Traffic Light, Rear Camera, Front Camera, Driver Camera, and Intercom Station) and section 7.2 describes the requirements for the LE Vetting Interface.

Interface ID	Interface Description	Fixed/Dev	Type	Physical	Source	Destination
INT-001	IP network interface	Fixed	Data Transfer	Ethernet	Various	Various
INT-002	Wiegand	Fixed	Data Transfer	Wiegand	Rhino Reader RFID Reader	Symmetry Gate Controller
INT-003	RS-485	Fixed	Data Transfer	RS-485	Symmetry Gate Controller	Symmetry Local Control Panel
INT-004	Handheld	Fixed	Data Transfer	IEEE 802.11 Wi-Fi	Handheld	IMM Client
INT-005	Dry Contact	Fixed	Signaling	Dry Contact	Various	Symmetry Gate Controller
INT-006	Removed					
INT-007	Vehicle exiting lane	Fixed	Signaling	Dry Contact	Exit Loop Controller	Symmetry Gate Controller ADAM Module
INT-008	Gate Arm Up Command	Fixed	Signaling	Dry Contact	Symmetry Gate Controller ADAM Module	Gate Arm
INT-009	Gate Arm Down Command	Fixed	Signaling	Dry Contact	Symmetry Gate Controller ADAM Module	Gate Arm
INT-010	Gate Crash Alarm	Fixed	Signaling	Dry Contact	Gate Arm	Symmetry Gate Controller ADAM Module
INT-011	Red Light Control	Fixed	Signaling	Dry Contact	Symmetry Gate Controller 24DC Relay	Traffic Light
INT-012	Green Light Control	Fixed	Signaling	Dry Contact	Symmetry Gate Controller 24DC Relay	Traffic Light

Interface ID	Interface Description	Fixed/Dev	Type	Physical	Source	Destination
INT-013	Rhino Reader Comms	Fixed	Data Transfer	Ethernet	IMM AutoReg	Rhino Reader
INT-014	Traffic Light	Fixed	Signaling	HMI	Traffic Light	Driver
INT-015	Rhino Reader Display	Fixed	Signaling	HMI	Rhino Reader	Driver or Pedestrian
INT-016	Intercom Data	Fixed	Data Transfer	Ethernet	Lane Intercom Ped Intercom Guard Intercom ACP Intercom	Intercom Station (various)
INT-017	Intercom Station	Fixed	Signaling	HMI	Driver Pedestrian Guard ACP Operator Remote Op	Intercom Station (various)
INT-018	Rhino Reader Credential Data	Fixed	Data Transfer	HMI	Driver Pedestrian	Rhino Reader
INT-019	Rhino Reader Fingerprint Capture	Fixed	Data Transfer	HMI	Driver Pedestrian	Rhino Reader
INT-020	Video	Fixed	Data Storage	Ethernet	Rear Camera Front Camera Driver Camera	Symmetry CompleteView Visual Verify
INT-021	Lane Control Client Ops	Fixed	Data Transfer	HMI	Symmetry Client	Guard ACP Operator Remote Op
INT-022	Registration Operations	Fixed	Data Transfer	HMI	Registration Client	Registrar
INT-023	Registration Data Collection	Fixed	Data Transfer	HMI	Registrant	Registration Client
INT-024	Removed	Fixed				
INT-025	PIR Import	Fixed	Data Storage	N/A	Registration Client	SQL Server-Site

Interface ID	Interface Description	Fixed/Dev	Type	Physical	Source	Destination
INT-026	Cache Box Synchronization	Fixed	Data Storage	N/A	Hawkeye Sync Services	SQL Server-Site
INT-027	Removed	Fixed				
INT-028	Registration Vetting	Fixed	Data Transfer	Ethernet	Registration Client	IMM Client-Site
INT-029	In-Lane Auto Registration Vetting	Fixed	Data Transfer	N/A	IMM AutoReg	IMM Client-ACP
INT-030	IoLS Vetting Request	Fixed	Data Transfer	Ethernet	IMM Client	IoLS
INT-031	LE Vetting Request	Fixed	Data Transfer	Ethernet	IMM Client	LE Vetting Service
INT-032	Qscan Reader Comms	Fixed	Data Transfer	Ethernet	IMM Client Visual Verify	Qscan
INT-033	Qscan Reader Display	Fixed	Signaling	Ethernet	Qscan	Driver or Pedestrian
INT-034	Qscan Reader Credential Data	Fixed	Signaling	Ethernet	Qscan	Driver or Pedestrian
INT-035	Cache Box Updates	Fixed	Data Transfer	Ethernet	Cache Box	App/DB Servers
INT-036	App/DB Servers Updates	Fixed	Data Transfer	Ethernet	App/DB Servers	Cache Box
INT-037	Mobile Device Management	Fixed	Data Transfer	Ethernet	SOTI MobiControl Client	SOTI MobiControl Server
INT-038	Cellular Wireless	Fixed	Data Transfer	Cellular	Handheld Cellular Wireless Spoke	Cellular Wireless Hub Site Server
INT-039	Input Status	Fixed	Data Transfer	Ethernet	ADAM Module	IMM (Server)
INT-040	Relay Control	Fixed	Data Transfer	Ethernet	IMM (Server)	ADAM Module
INT-041	Contact Open/Close	Fixed	Data Transfer	Ethernet	ADAM Module	Qscan Reader

Figure 3: Interface Identification Matrix

7.2. LE Vetting Interface Requirements

The Law Enforcement Vetting Interface is utilized to request adjudication of driver's licenses and state-issued identification cards against NCIC III and in-state and out-of-state law enforcement including department of motor vehicles (DMV) checks. The adjudication component is configured uniquely for each Installation and includes at a minimum DoD adjudication requirements and Army adjudication requirements – local Installation adjudication requirements can also be included. The requirements for the LE Vetting request are as follows:

Parameter	Description	I/O	M/O	Restrictions
First Name	Individual's given first name	In	Mandatory	English alphabet
Last Name	Individual's sur name	In	Mandatory	English alphabet
Middle Names	Individual's other given names	In	Optional	English alphabet
SSN	Individual's Social Security Number	In	Optional	
DOB	Date of Birth	In	Mandatory	
DLN	Driver's License (or State-issued ID) number	In	Mandatory	Alphanumeric
DL State	State that issued the DL or ID	In	Mandatory	
Validity	Result of Adjudication	Out	Mandatory	Granted, Denied
Warrant	Result of LE data collection	Out	Mandatory	True or False

Figure 4: Law Enforcement Vetting Interface Requirements

The response from the automated adjudication process includes one of three options.

- If the individual is determined fit for access, then a response of Pass will be returned and the AIE-3/4 system can proceed with normal functions, or
- If the vetting indicates that the individual does not meet fitness for access, but there were no pending warrants for arrest or other grave indications, then a response of Fail will be returned and the individual is asked to go to the Visitor Control Center for further processing, or
- If the vetting indicates that the individual does not meet fitness for access due to outstanding warrant for arrest or other grave indication as determined by Army and Installation command, then a response of Deny and Detain is returned and the Guard is to detain the individual and notify appropriate authorities as defined by local Installation command.

8. Interface Design Description

In accordance with DID DI-IPSC-81436A, the AIE-3/4 Interface Design Description (IDD) is described in this section. Section 7.1 identifies the various interfaces. Each interface is further explained in this section.

8.1. INT-001 IP network interface

The IP Network Interface represents the physical Ethernet infrastructure developed for AIE-3/4. This is made up of copper and fiber connections to various layer 2 and layer 3 switches that support connectivity for network devices utilizing TCP/IP.

8.2. INT-002 Wiegand

Wiegand defines both the protocol and the physical interface between an access control card reader and the PACS that controls the gate arm and coordinates other activities such as situational awareness, common operating picture, and services management. The Wiegand interface is limited to transmission of a credential ID number from credential reader to the PACS. The PACS responds with two signal lines generally intended to light a red (access denied) or green (access granted) indicator that are presented to the user (driver or pedestrian).

8.3 INT-003 RS-485

RS-485 is an ANSI/IEC standard communication interface used for point to point and multipoint bidirectional communications. The Symmetry ACP Local Processor uses RS-485 to communicate to a Symmetry Gate Controller at each vehicle lane and pedestrian gate. The use of RS-485 is restricted to communications between Symmetry controllers. The protocols are proprietary as they are not intended for integration. Integration is performed at the software level over the IP network.

RS-485 communications include passing credential identifier information, notification of status changes for inputs, and control signals to set the state of relay outputs.

8.4 INT-004 Handheld

The Handheld communications utilize IEEE 802.11 standard communications interface. Commonly known as Wi-Fi, this interface provides the handheld operator with the freedom to move within a defined space that supports sufficient signal strength to provide connectivity. The handheld device runs the Hawkeye Mobile application that retrieves all data in real time from the Site/Cloud Server or Cache Box and presents it to the operator for situational awareness. The handheld communications include credential identifier information and PIR information presented to the operator.

8.5 INT-005 Dry Contact

The Dry Contact interface is a two-conductor interface that indicates to the receiving component that the transmitting component is either in normal or off-normal condition. Such signals are used to transmit that a vehicle has entered or exited the lane or that the gate arm should raise or lower.

8.6 INT-006 Removed

8.7 INT-007 Vehicle Exiting Lane

The Vehicle Exiting Lane interface notifies the PACS through the Symmetry Gate Controller that a vehicle has been detected on the Vehicle Exit Loop Detector. This causes several other actions to initiate or complete.

8.8 INT-008 Gate Arm Up Command

The Gate Arm Up Command interface allows the PACS through the Symmetry Gate Controller to set the Gate Arm in the Up position. The Gate Arm motor is controlled by a controller in the gate arm assembly.

8.9 INT-009 Gate Arm Down Command

The Gate Arm Down Command interface allows the PACS through the Symmetry Gate Controller to set the Gate Arm in the Down position. The Gate Arm motor is controlled by a controller in the gate arm assembly.

8.10 INT-010 Gate Crash Alarm

The Gate Crash Alarm interface notifies the PACS through the Symmetry Gate Controller that the gate arm boom has been disengaged from its normal position. Typically, this indicates that a vehicle or other has attempted to run through the gate arm before the arm was raised sufficiently.

8.11 INT-011 Red Light Control

The Red-Light Control interface allows the PACS through the Symmetry Gate Controller or 24VDC Relay to illuminate the Red-light in the Traffic light assembly. The Red light indicates to the vehicle driver that they should not proceed.

8.12 INT-012 Green Light Control

The Green Light Control interface allows the PACS through the Symmetry Gate Controller or 24VDC Relay to illuminate the Green-light in the Traffic light assembly. The Green-light indicates to the vehicle driver that they should proceed when safe to do so.

8.13 INT-013 Rhino Reader Communications

Rhino Reader Communications utilize the IP network. Communications are always initiated by the IMM AutoReg component, and the Rhino Reader responds to the requests. Rhino Reader communications include reading a credential, displaying a message on the screen, or sending Wiegand data to the Symmetry Gate Controller.

8.14 INT-014 Traffic Light

The Traffic Light interface is the Human-Machine Interface (HMI) that informs the vehicle driver to proceed (green light) or not proceed (red light).

8.15 INT-015 Rhino Reader Display

The Rhino Reader Display provides an HMI that a scanned credential has been accepted and access has been granted, or that an issue was encountered and that the

access request has been denied. The guard will interface with the credential holder if an access denial is displayed.

8.16 INT-016 Intercom Data

The Intercom Data interface utilizes the IP network infrastructure to provide critical voice communications over IP. The Intercom Server acts as a central hub for all Intercom communications. Voice is digitized, sent over IP to the Intercom server and then out to the destination intercom station. The Intercom data interface also supports control functions such as a pushbutton on Intercom Station at the vehicle lane or at the pedestrian gate. Pressing the button initiates the Intercom server programming that will be configured to ring at the appropriate Guard Booth or Gatehouse.

8.17 INT-017 Intercom Station

The Intercom Station interface is the HMI that allows the driver or pedestrian to press a button to initiate communications with a guard or allows the driver or pedestrian to hear and speak to the guard.

8.18 INT-018 Rhino Reader Credential Data

The Rhino Reader Credential Data interface is the HMI that allows the driver or pedestrian to present their credential (CAC, other military ID, driver's license, or locally provisioned credential) to be scanned by a laser scanner.

8.19 INT-019 Rhino Reader Fingerprint Capture

The Rhino Reader Fingerprint Capture interface is the HMI that allows the driver or pedestrian to present their finger to be scanned by a special-purpose fingerprint scanner.

8.20 INT-020 Video

The Video interface utilizes the IP communications network to stream live video from various cameras such as the front-facing camera, the driver-facing camera, the rear-

facing camera, or other overview camera to the Symmetry CompleteView network video recorder (NVR) for storage.

8.21 INT-021 Lane Control Client Operations

The Lane Control Client Operations interface is the HMI that displays for the guard the common operating picture including credential information, live video feeds, and PIR information such as stored picture and Trusted Traveler status. The guard interacts with the Lane Control Client through the touch screen monitor or keyboard and mouse to raise and lower the gate arm. Operators with sufficient privilege can change FPCON and mode of operation (Card/PIN/Biometric).

8.22 INT-022 Registration Operations

Registration Operations interface is the HMI that displays registration information for the registrar as it is collected. The registrar interacts with the Hawkeye registration software on the registration workstation with keyboard and mouse to assist the registrant in presenting appropriate information in expected order.

8.23 INT-023 Registration Data Collection

Registration Data Collection interface is the HMI that allows the registrant to provide the data needed to vet the individual for potential registration in the AIE-3/4 System. The data collection includes driver’s license and passport scanner, fingerprint scanner, signature capture, and PIN entry pad.

8.24 INT-024 Removed

8.25 INT-025 PIR Import

PIR Import interface utilizes the published Symmetry Data Import API to import the collected PIR package into the Symmetry PIR database. The Hawkeye Registration software utilizes the IP network to send the collected PIR data to the Site/Cloud Server or Cache Box.

8.26 INT-026 Cache Box Synchronization

The Hawkeye Synchronization Services interface utilizes the IP network to send the PIR records for new and modified records to appropriate Cache Box. The synchronization writes the PIR data into the Symmetry Import database.

8.27 INT-027 Removed

8.28 INT-028 Registration Vetting

The Registration Vetting interface is used to communicate credential and identity data from the Hawkeye Registration Client software on the Registration Workstation to the IMM Client. The IMM Client simply parses this information and passes it on to appropriate external interface such as IoLS (section 8.30) and LE Vetting services (section 8.31). The IMM Client uses the Registration Vetting interface to provide the Registration Client with the response from the external system.

8.29 INT-029 In-Lane Auto Registration Vetting

The In-Lane Auto-Registration Vetting interface is internal to the IMM services running on the Site/Cloud Server so there is no physical interface. The Auto-Registration service controls the Rhino Reader to collect credential and Identity information (fingerprints) or the QScan IP Reader to collect credential only information to submit information for vetting and to create a PIR for import into the PIR database. The Qscan does not have a fingerprint capability.

8.30 INT-030 IoLS Vetting Request

The IoLS Vetting Request interface utilizes the Installation IP infrastructure and network routing gateway to send vetting requests for appropriate credentials to the IoLS web services hosted by the Defense Manpower Data Center (DMDC). Vetting requests include personally identifiable information such as name and DoD EDIPI. Responses to the vetting request include validity of the submitted credential as well as any security alerts reported for the requested identity.

8.31 INT-031 LE Vetting Request

The LE Vetting Request interface utilizes the Installation IP infrastructure and network routing gateway to send vetting requests for appropriate credentials to the LE Vetting service. Vetting requests include personally identifiable information such as name, driver's license number (and state of issue), and Date of Birth. Responses to the vetting request include validity of the submitted credential as well as an indication of the suitability for access for the individual.

8.32 INT-032 Qscan Reader Communications

Qscan Reader Communications utilize the IP network. Communications are always initiated by the IMM AutoReg component, and the Qscan Reader responds to the requests. Qscan Reader communications include sending Credential data to IMM and receiving commands to display messages on the Reader Display from IMM or Visual Verify.

8.33 INT-033 Qscan Reader Display

The Qscan Reader Display provides an HMI that a scanned credential has been accepted and access has been granted, or that an issue was encountered, and the access request has been denied. The guard will interface with the credential holder if an access denial is displayed.

8.34 INT-034 Qscan Reader Credential Data

The Qscan Reader Credential Data interface is the HMI that allows a credential holder to present their credential (CAC, other military ID, driver's license, or locally provisioned credential) to be scanned by a laser scanner.

8.35 INT-035 Cache Box Updates

The Cache Box interface allows continued processing of previously registered users in the event of a loss of communications with the cloud based AIE Enterprise Data Center App/DB Server. Data is kept in sync between the Cache Box and App/DB Servers by the Cache Box Synchronization interface.

8.36 INT-036 App/DB Servers Updates

The App/DB servers interface allows user registration data to be sent from the cloud to the Cache Box and transaction data to be sent from the Cache Box to the cloud.

8.37 INT-037 Mobile Device Management

The Mobile Device Management interface allows Handhelds to be viewed, secured, and updated remotely from the cloud. SOTIMobiControl agents are installed on the handhelds which enable the SOTIMobIControl server to communicate with and manage these devices.

8.38 INT-038 Cellular Wireless

The Cellular Wireless interface extends the communications network without the need for additional network communications infrastructure to connect endpoints. The Cellular Wireless interface provides a communications path for endpoints by having a cellular wireless “Hub” connected to the NEC at the Installation and one or more cellular wireless “Spokes” connected at the destination(s) to create a reliable network communications path.

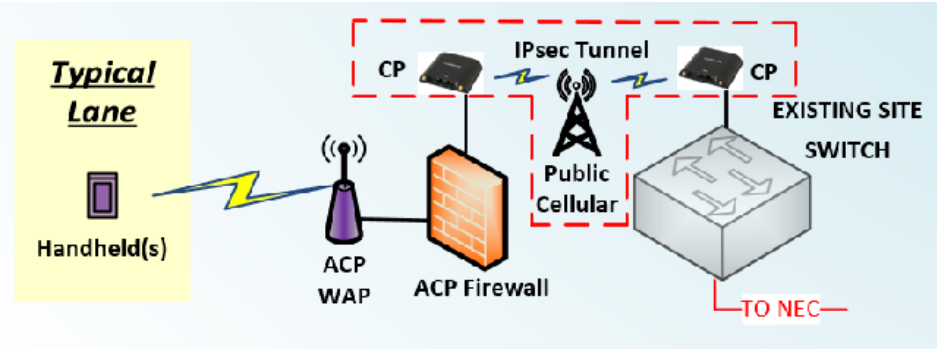

Figure 5: Cellular Wireless Configuration

- CP replaces the function of the site switch at an existing ACP
- An additional CP is located on an available existing site switch on the Installation
- Secure tunnel is setup between CPs for encrypted communications via public cellular infrastructure
- Requires cellular service at both CP locations (preferred networks AT&T, Verizon, or T-Mobile)

8.39 INT-039 Input Status

The ADAM Module transmits status of all inputs to the IMM Server. 1) on any input status change, the status is immediately sent and identifies the input that has changed and 2) status is provided on a defined interval.

8.40 INT-040 Relay Control

The IMM server sends a command to the ADAM Module to set a relay to an open or close status to control a device.

8.41 INT-041 Contact Open/Close

The ADAM Module provides a contact open/close to an input of the Qscan Reader which is used for card reader lock out and turn around lockout.

9. Database Design Description

In accordance with DID DI-IPSC-81437A, the AIE-3/4 Database Design Description (DBDD) is described in this section. Typically, the DBDD is a highly detailed document that describes the design of the database being used. However, since AIE-3/4 is not a software development program, but a system of systems that makes use of commercial-off-the-shelf products that are completely owned and copyright protected by the respective manufacturers, this DBDD will instead describe the use of databases in the solution, the interaction with software elements and the use of the databases as it pertains to supported interfaces for data sharing among the commercial systems.

This document does not describe the databases to the level of detail of the elements of each table or the specifics of the stored procedures that make up the database automation. Those elements are proprietary to the respective manufacturers.

9.1. Database Overview

The AIE-3/4 System makes use of several databases that are described below. The databases are all managed by Microsoft (MS) SQL Server, Enterprise Edition. The choice of Microsoft SQL Server was made by the manufacturers of the COTS software – this is the only database management system (DBMS) that is supported by all

software component manufacturers. The selection of the Enterprise Edition was made by the contractor for the “Transparent Data Encryption (TDE)” feature that is offered in this edition of the software. TDE supports the requirement for encryption of data at rest in the solution and supports the contractor’s efforts to achieve Authorization to Operate (ATO) and the US Army’s Certificate of Networthiness (CoN).

MS SQL Server is installed at the Site Server cluster, Cloud Database Cluster and Cache Box. Symmetry installs several databases in the SQL Server database at the Site Server and App/DB Servers. These are discussed in sections below.

As described in Section 8 above, Interface Design Description, the interface to the Symmetry PACS (as implemented in AIE-3/4) is through the database using the AMAG Technology published API called “Data Connect”. Various software components of the AIE-3/4 System import data into the Symmetry multiMAXImport database and read data from the various tables of the Symmetry multiMAX database.

9.2. Removed

9.3. Symmetry Database Design

Symmetry creates several databases in the DBMS:

- multiMAX
- multiMAXExport
- multiMAXImport
- multiMAXTxn
- multiMAXTxnArchive
- multiMAXTxnOps
- multiMAXTxnRestore
- multiMAXVideo
- OPMG

9.3.1. multiMAX

The multiMAX database is the location of most of the PIR data and the operational configuration data for the Symmetry application. The specifics of the tables, the table design, and the stored procedures that make up this database are proprietary to AMAG Technology.

9.3.2. multiMAXExport

This database includes tables that support the exporting of PIR and transactional data out of the Symmetry multiMAX database to other systems. The multiMAXExport database is not used in the AIE-3/4 architecture.

9.3.3. multiMAXImport

This database is used as a landing point for imported PIR data from other systems. Those systems write data to the DataImport table which triggers a stored procedure to validate the datatypes, format of data, existence of mandatory data, and other aspects of the imported data. If the “ImportNow” flag is set, then the validated data will be written to the multiMAX database. If the flag is not set, then Data Import can be triggered from the GUI. Once the import process has completed, the RecordStatus field is updated with a value to indicate success or failure code. The RecordStatus field is the feedback to the external system that imported the data. Therefore, it is the responsibility of the external system to check for that feedback and remove the table entries once the feedback is received. If this table management process is not followed, the DataImport table can grow to unexpected size unnecessarily.

9.3.4. multiMAXTxn

This database is used to store the audit transactions. It is kept in a separate database to not impact the normal operations from the multiMAX database with such a large table. Reporting on such a large table can sometimes be taxing on the system. The other Archive databases are also used in support of the Audit data storage functions. For instance, the multiMAXTxnArchive database is used to move transactions of a certain date range out of the multiMAXTxn database. Often this database is stored on

separate storage than the multiMAXTxn or multiMAX databases. The multiMAXTxnRestore, and Ops databases are used in a similar fashion.

9.3.5. multiMAXVideo

This database is used to store information about video clip files when Symmetry is additionally used as a Network Video Recorder (NVR). This feature is not used in the AIE-3/4 System. The AIE-3/4 System uses a more robust video subsystem that AMAG Technology provides under an OEM reseller agreement with Salient Systems called Symmetry CompleteView.

9.3.4. OPMG

This database is used to store information collected from each Installation on scans, registrations and denials and is used as a central repository that facilitates the OPMG Dashboard Reports. Local instances of the OPMG database, co-located with the Symmetry database on the installation servers, have stored procedures that query the local instance of the Symmetry database to produce the summary data. The OPMG central repository collects summary data from the OPMG instances on the installation servers and makes it available for viewing via web-based reports. The OPMG central repository does not query the Symmetry database.

9.4. Symmetry CompleteView Database Design

The AIE-3/4 System uses a video subsystem from Salient Systems called Symmetry CompleteView. This system does not use MS SQL Server as the DBMS. To provide better performance without the overhead of the DBMS, Symmetry CompleteView uses a proprietary database solution. Video is stored from each camera in files on the NVR Server. A database of the camera index, the location of the file, and the time/date range captured in the file is maintained. Symmetry CompleteView is solely responsible for maintaining and managing the database and the video files.

10. Notes

This section left blank.

APPENDIX A

AV-1 System Overview and Summary

APPENDIX A
AV-1 System Overview and Summary

A.1 IDENTIFICATION

A.1.1 Name

Automated Installation Entry, Increment 3/4 (AIE-3/4) System Architecture; hereafter, identified as: AIE-3/4 System Architecture.

A.1.2 Architect

Product Manager, Force Protection Systems (PM FPS) AIE-3/4, and Prime Contractor.

A.1.3 Organization

The AIE program is a program of record for PM FPS. AIE-3/4 is a system to be deployed to approximately 98 Installations.

A.1.4 Description

This AV-1 identifies, describes, and provides a purpose, scope, plan, and architecture product status for developing architecture products required to support AIE-3/4 capabilities.

A.1.5 Assumptions and Constraints

A.1.5.1 Assumptions

The following are assumptions made in the development of the architecture.

A.1.5.1.1 Capability

The AIE-3/4 System capabilities are defined in reference documents AIE-3 System Performance Specification and AIE-3 CONOPS. The AIE-3/4 System design assumes

that the System requirements are sufficient to describe a system that will meet the expectations of Installation

A.1.5.1.2 Availability

The AIE-3/4 System design includes the need to connect to external resources such as IoLS and LE Vetting sources. Therefore, the design assumes availability of the network connection from the Installation out to the public Internet. Furthermore, the design includes the assumption that IoLS and the LE vetting service is available to perform the Registration vetting processes.

A.1.5.1.3 Physical Plant

The AIE-3/4 System design assumes the existence of network infrastructure between each ACP and the Installation NEC/DOIM. The system design further assumes that the US Army Corps of Engineers has provided the Access Control Point (ACP) preparation.

The AIE-3/4 System design assumes the existence of sufficient power for servers at the NEC and at the ACP and at each vehicle lane and pedestrian portal.

A.1.5.2 Constraints

The AIE-3/4 System design is constrained by the removal of the Enterprise servers that were installed during AIE-2. Without an Enterprise architecture AIE-3/4 cannot share data from one facility with other AIE-2 and AIE-3/4 facilities.

A.1.6 Approving Authority

Product Manager, Force Protection Systems (PM FPS).

A.1.7 Completion Date

Work is assigned in individual delivery orders (DOs). The completion date of each DO will be determined in the contract award for the specific DO.

A.1.8 Level of Effort

The contractor has defined the Level of Effort per individual Contract Line-Item Numbers (CLIN). The Government orders the implementation of AIE-3/4 at a particular Installation by purchasing the necessary CLINs.

A.2. SCOPE

A.2.1 Viewpoints

The following Department of Defense Architecture Framework Version (DoDAF) 2.02 viewpoints are included as part of the System Architecture document.

Applicable View	Framework Product	Framework Product Name	General Description
All Views	AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
All Views	AV-2	Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Operational	OV-1	High-Level Operational Concept Graphic	High-level graphical/textual description of operational concept
Operational	OV-2	Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange need lines between nodes
Operational	OV-3	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
Operational	OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
Operational	OV-5	Operational Activity Model	Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
Operational	OV-6a	Operational Rules Model	One of three products used to describe operational activity— identifies business rules that constrain operation
Operational	OV-6b	Operational State Transition Description	One of three products used to describe operational activity— identifies business process responses to events
Operational	OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity— traces actions in a scenario or sequence of events
Operational	OV-7	Logical Data Model	Documentation of the system data requirements and structural business process rules of the Operational View
Systems	SV-1	Systems Interface Description	Identification of systems, systems components and elements and their interconnections
Systems	SV-2	Systems Communications Description	Systems, system components and their elements, and the system resource flows between the systems
Systems	SV-3	Systems-Systems Matrix	Provides a tabular summary of the system interactions depicted in V-1 & SV-2
Systems	SV-4	Systems Functionality Description	Functions performed by systems and the system data flows among system functions
Systems	SV-4a	Systems Functionality Description	Documents system functional hierarchies and system functions, and the system data flows between them
Systems	SV-4b	Services Functionality Description	Documents service functionality that is exposed to the Net-Centric Environment, their respective grouping into service families, and their service specifications
Systems	SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to capabilities or of system functions back to operational activities
Systems	SV-5a	Operational Activity to Systems Function Traceability Matrix	Depicts the mapping of operational activities to system functions and thus identifies the transformation of an operational need into a purposeful action performed by a system
Systems	SV-5b	Operational Activity to Systems Function Traceability Matrix	Extends the SV-5a and depicts the mapping of capabilities to operational activities, operational activities to system functions, system functions to systems, and thus relates the capabilities to the systems that support them
Systems	SV-5c	Operational Activity to Service Traceability Matrix	Depicts the traceability and mapping of services to operational activities to assist in understanding which services support operational activities

Systems	SV-6	Systems Data Exchange Matrix	Provides details of system data elements being exchanged between systems and the attributes of that exchange
Systems	SV-7	Systems Performance Parameters Matrix	Performance characteristics of Systems View elements for the appropriate time frame(s)
Systems	SV-8	Systems Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
Systems	SV-9	Systems Technology Forecast	Emerging technologies and software/hardware products that are expected to be available in each set of time frames and that will affect future development of the architecture
Systems	SV-10a	Systems Rules Model	One of three products used to describe system functionality— identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation
Systems	SV-10b	Systems State Transition Description	One of three products used to describe system functionality— identifies responses of a system to events
Systems	SV-10c	Systems Event-Trace Description	One of three products used to describe system functionality— identifies system-specific refinements of critical sequences of events described in the Operational View
Systems	SV-11	Physical Schema	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Technical	TV-1	Technical Standards Profile	Listing of standards that apply to Systems View elements in each architecture
Technical	TV-2	Technical Standards Forecast	Description of emerging standards and potential impact on current Systems View elements, within a set of time frames

Figure 6: DODAF Viewpoints Required by DI-MGMT-81644A

A.2.2 DoDAF-Described Models

This architecture, conforming to DoDAF 2.02 guidelines, serves to assist DoD acquisition decision-makers and provide an enhanced understanding of the desired system capabilities and the linkages between capabilities and systems (both internal and external).

A.2.3 Organizational Entities

The following high-level organizations provide Points of Contact (POCs), Subject Matter Experts (SMEs), and information to facilitate data collection, analysis, and developmental documentation review.

A.2.3.1 U.S. Department of Army

A.2.3.2 Sponsor

Product Manager, Force Protection Systems (PM FPS)

A.2.3.3 AIE-3/4 POC

Michael V. Doney, Program Officer, Installation Physical Security Systems (IPSS) PM, FPS
George W. Smith, Deputy AIE Contracting Officer's Representative (COR)

A.2.3.4 Operational Architecture POC

Alonzo Wilson, PM FPS, AIE-3/4 Systems Engineer Lead, Contractor in Support

A.3. PURPOSE AND PERSPECTIVE

A.3.1 Architectural Analysis

The AIE-3/4 System is required to be made up of commercial components (SS_707). The contractor has designed a solution from COTS products that interoperate and combine to meet the requirements specified. The use of COTS products in a modular architecture supports maintainability, supportability, system growth, and evolution.

A.3.1.1 Approach

Requirements are decomposed and allocated to systems elements included in AIE-3/4. Architecture products are developed as necessary for program presentation, design, and documentation, in accordance with DoDAF 2.02. Based on the approved architecture, a System Level Specification is developed that includes the key elements of the system and high-level requirements allocated at the system level to include the System Performance Specifications. Upon completion of the System Specification, the Component Specifications are developed for each of the main AIE-3/4 components: Registration, Lane Operations, Gatehouse Operations, and Central Remote Management Operations. From these component specifications, site specific and enterprise designs are developed based on component product and locality characteristics.

A.4. CONTEXT

A.4.1 Security Classification

Unclassified

A.4.2 Data Management Access Level

Protected access enabled through approval organization.

A.4.3 Mission

A.4.3.1 Operational Environment

The AIE-3/4 System will be installed at US Military Installations (predominantly US Army Facilities) within the CONUS and may also be installed OCONUS. The AIE-3/4 System will be installed, employed, maintained, and supported at all locations by civilian contractors, military personnel, and US Government Civilians. The AIE-3/4 System will be mission capable in environments that meet basic cold and hot weather criteria and be capable of continuous operation under harsh weather and environmental conditions. It will be employed across the full spectrum of CONUS and perhaps OCONUS Installation operations.

The AIE-3/4 System will operate using local commercial power and be equipped with an Uninterruptible Power Source (UPS). The System will be mutually compatible with other electronic equipment operating in its Area of Operations without system interference or degradation.

A.4.3.2 Threat Environment

The primary threats to be countered by AIE-3/4 will include enemy infiltrators, insurgents, and other belligerent parties - virtually any person, element, or hostile group, including irregulars, criminals, terrorists, and looters. Components of AIE-3/4 will 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 can disrupt wireless links, the wireless connections will be affected, rendering the data transmitted from Wireless Handheld devices useless. Other threats to AIE-3/4 include theft, destruction, and deception operations.

A.4.4 CONCEPT OF OPERATIONS

See reference document, *AUTOMATED INSTALLATION ENTRY (AIE) – 3, CONCEPT OF OPERATIONS (CONOPS),* Dated 8 September 2014.

A.4.5 System Deployment Concept

The AIE-3/4 system is comprised of cloud support architecture, on premise server and network equipment, and COTS products that interoperate to provide an architecture solution that can be tailored for site specific conditions. The concept of deployment begins with certain minimum Installation infrastructure elements to be in place (structures, power, underground conduits, network connectivity). These infrastructure elements are analyzed during a site survey and a design is developed based upon those results. Each varying architecture has certain design elements that are critical to deployment and are considered as part of the design. Specifically, the Pure Fleet architecture is dependent upon existing AIE equipment being in place for integration.

The AIE-3/4 system is deployed at an Installation following equipment procurement and system build within the AIE Laboratory. The laboratory builds and equipment configurations are dependent upon the AIE-3/4 design documentation that was developed based upon results of the site survey. All systems are pre-built and tested within the laboratory environment prior to shipment to the Installation for deployment. This approach permits troubleshooting of any issues discovered during the build process within a controlled environment prior to deployment. Following delivery to the Installation, the pre-configured AIE-3/4 system is deployed per the approved design documentation.

A.5. STATUS

A.5.1 Architecture Status

The AIE-3/4 System Architecture is defined in this document, the System Description and Architecture. The System Architecture represents the baseline system as of the date of acceptance of this document by the Government. Changes to the System Description and Architecture document are made through requests to the CCB as defined in the System Engineering Management Plan (SEMP).

A.6. ASSURANCE AND VALIDATION

A.6.1 Approval Status

This document, Rev 4, is presently in DRAFT status, awaiting commentary or approval from the Government.

A.6.2 Directed Requirements Documents

The AIE-3 System Performance Specification, dated October 2014, is the definitive requirements document. Other requirements are found in the AIE-3 Statement of Work and AIE-3 CONOPS.

A.6.3 DoD Architecture Framework

The AIE-3/4 System Architecture is intended to conform to DoD Architecture Framework (DoDAF) v2.02.

A.6.4 Configuration management (CM)

Configuration management (CM) of artifacts and documents will be performed in accordance with the AIE-3/4 CM Plan and as outlined in the AIE-3/4 System Engineering Plan (SEP).

A.7 TOOLS AND FILE FORMATS USED

The following were used to develop and maintain the AIE-3/4 System Architecture, as well as the files and formats for the Architectural Models/Diagrams.

A.7.1 Microsoft Office Suite®

This includes:

a. Microsoft Visio
b. Microsoft Word
c. Microsoft Excel

A.7.2 Architectural Data Storage

The AIE-3/4 System Architecture will be stored in the AIE-3/4 CM and Document Repository.

A.8. ARCHITECTURE DEVELOPMENT SCHEDULE

A.8.1 Start Date

16 September 2016 (DO-1 Contract Issued)

A.8.2 Milestone Dates

A.8.2.1 Initial Draft Architecture, Completed: 17 October 2016

A.8.2.2 Draft Architecture Review and Comments, Comments were scheduled and/or provided on the following dates: 4 November 2016

A.8.2.3 Comments scheduled and/or Addressed and Additional Revisions
19 November 2016

A.8.2.4 Updated Architecture and System Design for Pure Fleet , 6 March 2020

A.8.2.5 Updated Architecture and System Design for AIE-3/4 enhancements
14 February 2022

A.8.2.5 Updated Architecture and System Design for AIE-3/4 enhancements
28 February 2022

APPENDIX B

AV-2 Integrated Dictionary

APPENDIX B

AV-2 Integrated Dictionary

B.1. ACRONYMS

ACRONYM	DEFINITION
ACP	Access Control Point
ACS	Access Control System
ACWG	Access Control Working Group
AES	Advanced Encryption Standard
AIE	Automated Installation Entry
ANSI	American National Standards Institute
A_o	Operational Availability
API	Application Programming Interface
AR	Army Regulation
ATO	Authority to Operate
AV	All Viewpoint
C&A	Certification and Accreditation
CAC	Common Access Card
CCB	Configuration Control Board
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
CIME	Continuous Information Management Engine
CIO	Chief Information Officer
CJCSI	Chairman Joint Chiefs of Staff Instruction
CJIS	Criminal Justice Information System
CLIN	Contract Line-Item Number
CLS	Contractor Logistics Support
CM	Configuration Management
CMP-	Component identifier prefix
CND	Computer Network Defense
CoN	Certificate of Net worthiness
CONOPS	Concept of Operations
CONUS	Continental United States
COR	Contracting Officer's Representative
COTS	Commercial-off-the-Shelf
CRM	Cybersecurity Risk Management
DA	Department of the Army
DBDD	Database Design Description
DBIDS	Defense Biometrics Identification System
DD	Department of Defense
DEERS	Defense Enrollment Eligibility Reporting System
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DID	Data Item Description

ACRONYM	DEFINITION
DMDC	Defense Manpower Data Center
DMV	Division of Motor Vehicles
DO	Delivery Order
DOB	Date of Birth
DoD	Department of Defense
DoD UC APL	DoD Unified Capabilities Approved Products List
DODAF	Department of Defense Architecture Framework
DOIM	Director of Information Management
EDIPI	Electronic Data Interchange Personal Identifier
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FHWA	Federal Highway Administration
FHWA SA	Federal Highway Administration Safety Audit
FIPS	Federal Information Processing Standard
FP	Force Protection
FPCON	Force Protection Condition
HBSS	Host Based Security System
HSPD	Homeland Security Presidential Directive
HTML	Hyper Text Markup Language
IA	Information Assurance
IaaS	Infrastructure as a Service
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Information Assurance Manager
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
ICD	Interface Control Document
ICIDS	Integrated Commercial Intrusion Detection System
IDD	Interface Design Description
IEA	Information Enterprise Architecture
IEC	International Electro-technical Commission
ILS	Integrated Logistics Support
IMM	Identity Management Middleware
IoLS	Interoperability Layer Service
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPT	Integrated Process Team
IRS	Interface Requirements Specification
IT	Information Technology
ITL	Institute of Standards and Technology
IWS	Interface Web Services
JPEO-CBD	Joint Program Executive Office for Chemical and Biological Defense

ACRONYM	DEFINITION
JPM IS	Joint Project Manager, Information Systems
LAN	Local Area Network
LE	Law Enforcement
LPDB	Local Population Database
MDT	Mean Down Time
MIL-STD	Military Standard
MTBCF	Mean Time Between Critical Failure
MTBDE	Mean Time Between Downing Events
MTBF	Mean Time Between Failure
NAC	National Agency Check
NCIC	National Crime Information Center
NEC/DOIM	Network Enterprise Center/Director of Information Management
NEMA	National Electrical Manufacturers Association
NETCOM	Network Command
NFPA	National Fire Protection Association
NIPRNET	Non-secure Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NVR	Network Video Recorder
OCONUS	Outside Continental United States
OPSEC	Operations Security
ORI	Originating Agency Identifier
OV	Operational Viewpoint
PACS	Physical Access Control System
PC	Personal Computer
PDF	Portable Document Format
PM FPS	Product Manager, Force Protection Systems
PEO-IEWS	Program Executive Office for Intelligence, Electronic Warfare, and Sensors
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Personnel Identity Protection
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
POC	Point of Contact
PSRB	Physical Security Review Board
PUB	Publication
Pure Fleet	Applying AIE-3/4 software to AIE-2 and AIE-2+ sites reusing equipment as appropriate
RFID	Radio Frequency Identification
RMF	Risk Management Framework

ACRONYM	DEFINITION
SCAP	Security Content Automation Protocol
SDD	Software Design Description
SDK	Software Development Kit
SEIWG	Security Equipment Integration Working Group
SEMP	Systems Engineering Management Plan
SME	Subject Matter Expert
SOW	Statement of Work
SQL	Structured Query Language
SSN	Social Security Number
ST&E	Security Test and Evaluation
ST&Es	Security Test and Evaluations
StdV	Standards Viewpoint
SV	System Viewpoint
T& E	Test and Evaluation
TCO	Total Cost of Ownership
TDE	Transparent Data Encryption
TLA	Top Level Architecture
TPF	Total Package Fielding
TSDB	Terrorist Screening Data Base
TT	Trusted Traveler
TV	Technology Viewpoint
TWIC	Transportation Workers Identification Credential
TYAD	Tobyhanna Army Depot
UHF	Ultra-High Frequency
UPS	Uninterruptible Power Supply
VCC	Visitor Control Center
XML	eXtensible Markup Language

Figure 7: AIE-3/4 Acronym Definitions

B.2. TERMS

Does not apply

APPENDIX C

OV-1 High Level Operational Concept Graphic

APPENDIX C

OV-1 High Level Operational Concept Graphic

The Operational Concept Graphic portrays how AIE supports the Installation's mission to provide Installation access for personnel and other members of the community as qualified by Federal Government, U.S. Army, and Installation Commander. The intent of AIE-3/4 is to provide high throughput of registered personnel, and to properly vet and adjudicate those wishing to register in the AIE-3/4 System.

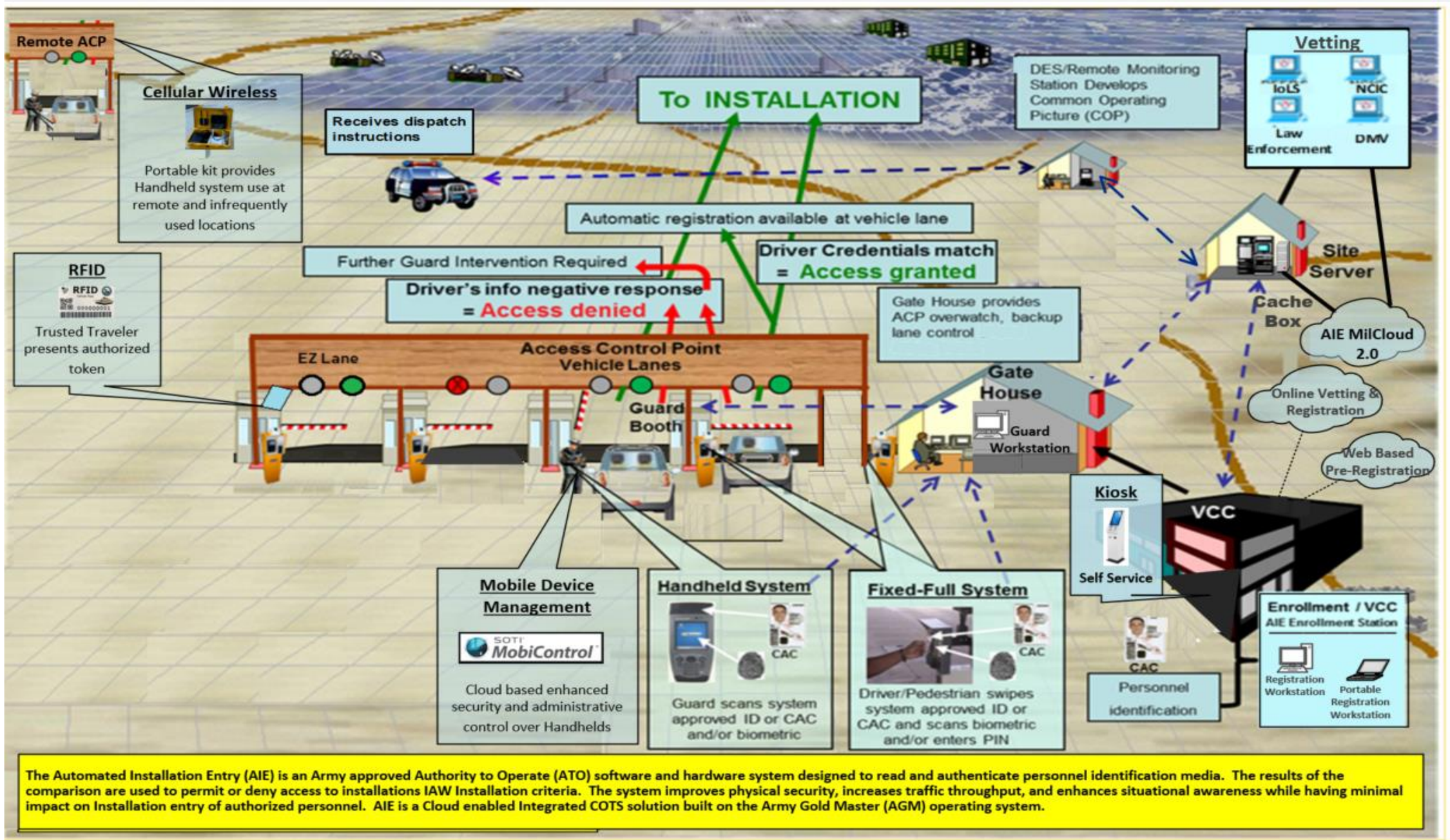

Figure 8: OV-1, High Level Operational Concept

APPENDIX D

OV-2 Operational Resource Flow Description

APPENDIX D

OV-2 Operational Resource Flow Description

The Operational Resource Flow Graphic depicts the flow of information, instructions, and materials for the various performers to support the Installation's gate access needs. The Resource Flow lines are labeled and are described in OV-3, Appendix E.

The Installation Command includes Installation leadership as well as the guard force that is used to operate the AIE-3/4 System. Therefore, need lines, or resources, necessarily extend from the Installation Command out to where human resources are required. The AIE-3/4 System enables the Installation Command to reduce human resource needs by allowing the guards to monitor and control multiple lanes from a single workstation at either the Guard Booth, Gatehouse, or Central Monitoring location.

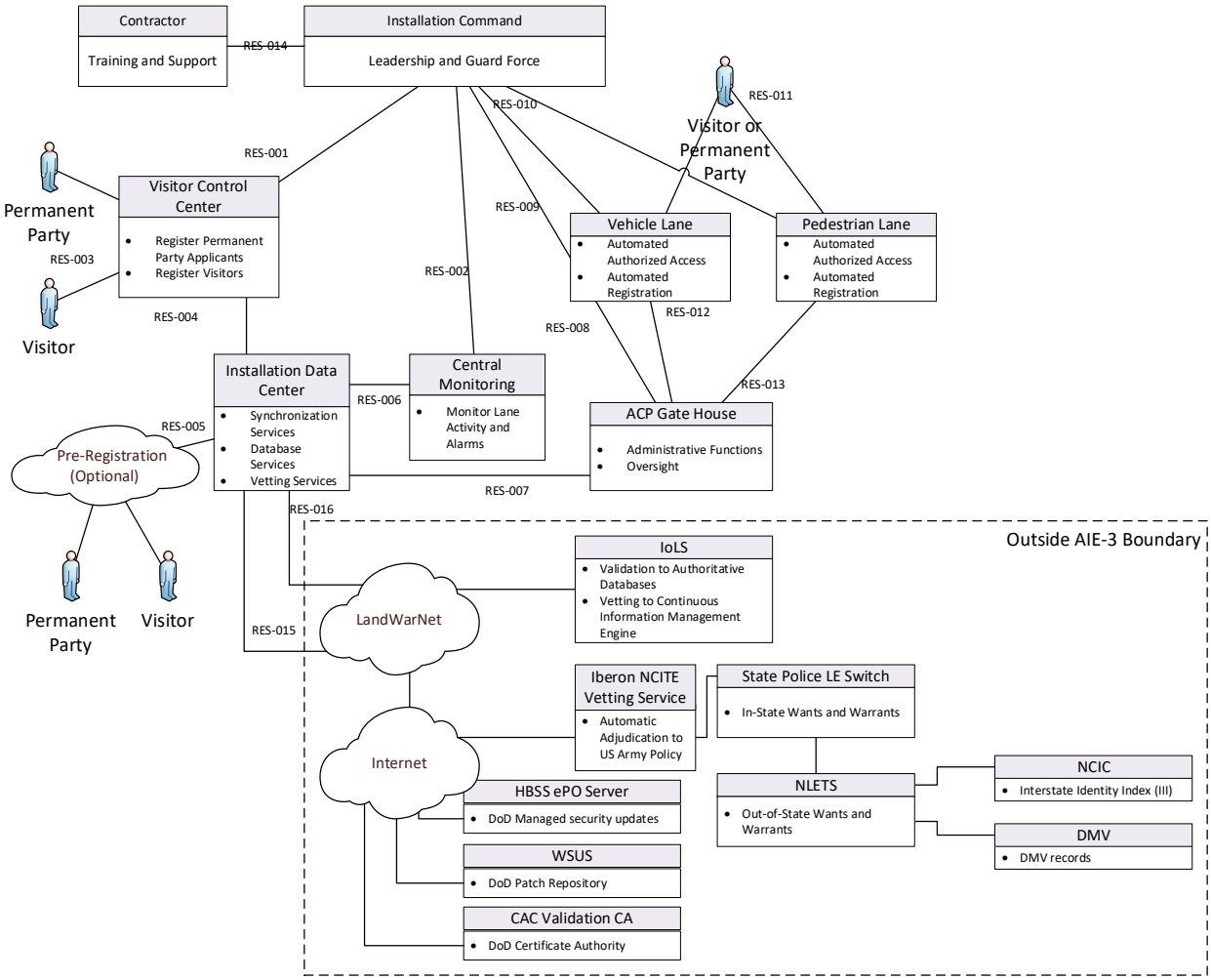

Figure 9: OV-2, Operational Resource Flow Description

APPENDIX E

OV-3 Operational Information Exchange Matrix

APPENDIX E

OV-3 Operational Resource Flow Matrix

The Operational Resource Flow Matrix details information exchanges between elements of the AIE-3/4 Architecture. The flow of information, instructions, and materials between the various elements is broken down and the attributes of the exchanges are laid out. Some of the attributes include:

- Information exchange identifiers
- Nature of the transaction
- Source
- Destination
- Allocation to systems
- Gov. Actions

In the following table, each unique resource (indicated by RES-) is associated with an Operational Activity, and the characteristics of this resource allocation are described.

Resource Identifier (From OV-2)	Operational Activity	Resources Exchanged	Source	Destination	Purpose	Key Attributes
RES-001	Registration	Personnel Policy	Installation Command	Visitor Control Center (VCC)	Staff the Visitor Control Center to support in-person registration of permanent party (U.S. DoD ID Card Holders) and visitor enrollees	Personnel trained on AIE-3/4 Registration Personnel trained on collection of PII
RES-002	Monitoring and Control	Personnel Policy	Installation Command	Central Remote Monitoring	Optionally staff a remote monitoring location	Personnel trained on AIE-3/4 and incident response
RES-003	Registration	Personal Information and credentials	Registrants	Site/Cloud Server	Capture PII and credential data to vet registrant for Installation access suitability	Supply approved documents and PII data
RES-004	Registration	PIR data	IMM Registration Client	Site/Cloud Server Cache Box	Store PIR data for dissemination to ACPs	Encrypted PII data
RES-005	Pre-Registration	Personal Information and credentials	Registrants	Site/Cloud Server	Capture PII and credential data in advance of on-site registration	Supply approved documents and PII data
RES-005a	Online Vetting and Registration	Personal Information and credentials	Registrants	Site/Cloud Server	Capture PII and credential data in lieu of on-site registration	Supply approved documents and PII data
RES-006	Monitoring and Control	Voice, Video, and control data	Central Remote Monitoring	Site Server	Control equipment at vehicle and pedestrian lanes when not staffed locally	Trusted Traveler Not on barred list No re-vetting security alerts
RES-007	Access, Monitoring and Control	Personnel Policy	Site/Cloud Server	GBWS GHWS CMWS	Staff the ACP Gatehouse	Personnel trained on AIE-3/4 and incident response
RES-008	Access, Monitoring and Control	Personnel Policy	Installation Command	GBWS GHWS CMWS	Staff the ACP Guard Booth	Personnel trained on AIE-3/4 and incident response
RES-009	Access, Monitoring and Control	Personnel	Installation Command	GBWS GHWS CMWS	Optionally staff a Vehicle Lane Guard Booth	Personnel trained on AIE-3/4
RES-010	Access, Monitoring and Control	Personnel	Installation Command	GBWS GHWS CMWS	Optionally staff a Pedestrian Guard Booth	Personnel trained on AIE-3/4

Resource Identifier (From OV-2)	Operational Activity	Resources Exchanged	Source	Destination	Purpose	Key Attributes
RES-011	Registration	Personal Information and credentials	Registrants	Registration Client RGWS Site/Cloud Server Pedestrian Lane	Capture PII and credential data to vet registrant for Installation access suitability	Supply approved documents and PII data
RES-011a	Access	Credentials	AIE-3/4 registered party	Rhino Reader Qscan Reader Handheld RFID Site/Cloud Server Symmetry Gate Controller ADAM Module	Automatically grant Installation access if criteria are met	Trusted Traveler Not on barred list No re-vetting security alerts
RES-012	Access	PIR data Voice, Video, and control data	ACP Gatehouse	Rhino Reader Qscan Reader RFID Site Server Symmetry Gate Controller ADAM Module 24VDC Relay Intercom Camera NVR	Control traffic light, gate arm, credential reader, intercom, and video cameras	Credential number, biometric templates, access decision
RES-013	Access	PIR data Voice, Video, and control data	ACP Gatehouse	Rhino Reader Qscan Reader RFID Site Server Symmetry Gate Controller ADAM Module Intercom Camera NVR	Control turnstile, credential reader, intercom, and video cameras	Credential number, biometric templates, access decision
RES-014	Training, Support, Maintenance	Staffing to provide Training, Support and Maintenance	Contractor location	As defined by Installation	Provide Training and Support Services	AIE-3/4 Operational Manuals and information, Support
RES-015	Vetting	PIR data, Fitness for access	Site/Cloud Server	NLETS Data Center	Determine Fitness for Access against US Army adjudication policy. Validation of Driver's License	Name, DOB, Driver's License Number, Adjudication response

Resource Identifier (From OV-2)	Operational Activity	Resources Exchanged	Source	Destination	Purpose	Key Attributes
RES-016	Vetting	PIR data, Fitness for access	Site/Cloud server	IoLS Data Center	Validation of DOD Credentials Identify changes in fitness for access	EDI-PI, Adjudication Updates

Figure 10: OV-3, Operational Resource Flow Matrix

APPENDIX F

OV-4 Organizational Relationships Chart

APPENDIX F

OV-4 Organizational Relationships Chart

The Organization Relationship Chart depicts the organizational elements that utilize and support AIE-3/4 together with their interrelationships.

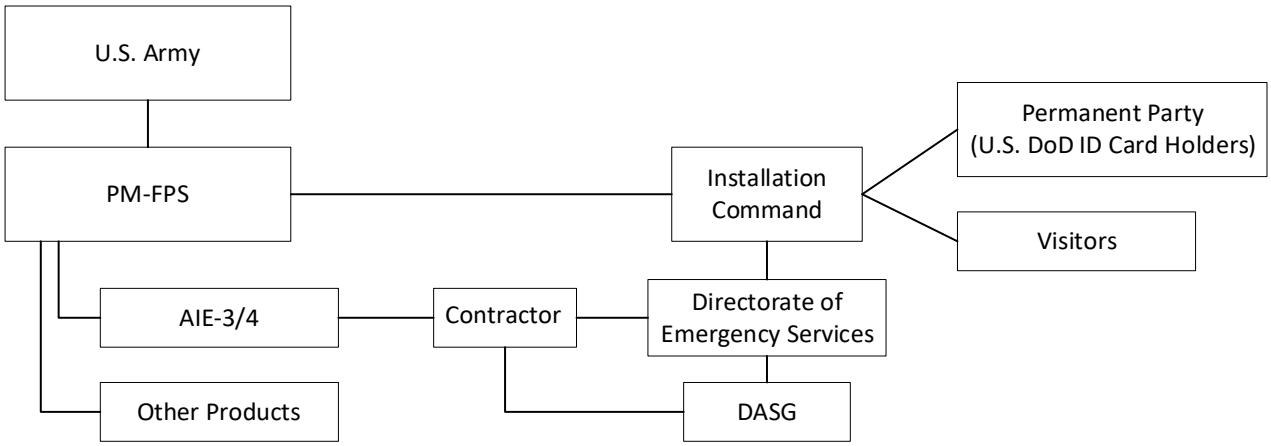

Figure 11: OV-4, Organizational Relationships Chart

APPENDIX G

OV-5 Operational Activity Model

APPENDIX G

OV-5 Operational Activity Model

DODAF V2.02 breaks Operational Viewpoint 5, Operational Activity Model, down into OV-5a, Operational Activity Decomposition Tree and OV-5b, Operational Activity Model.

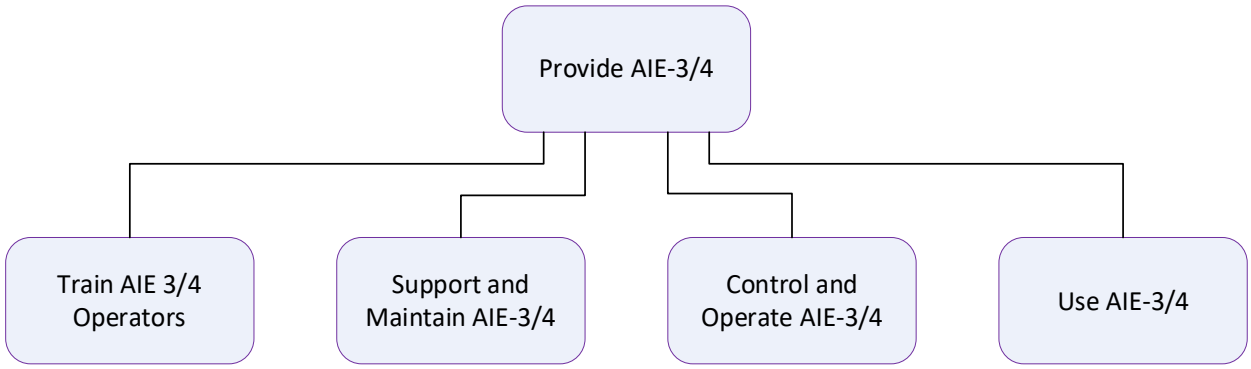

Figure 12: OV-5a-1, Top Level Operational Activity Decomposition

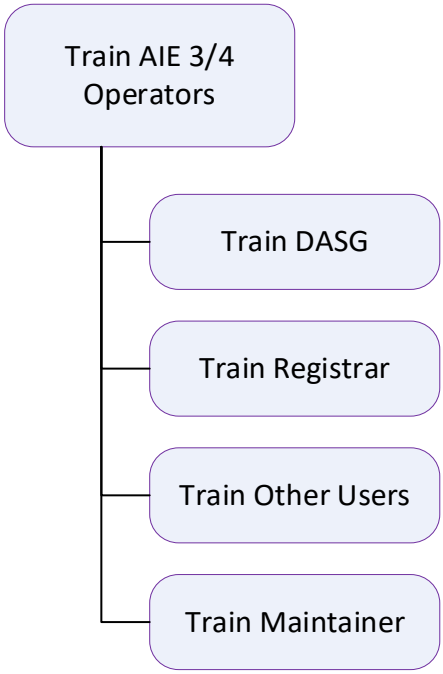

Figure 13: OV-5a-2, Decomposition of the Training Activity

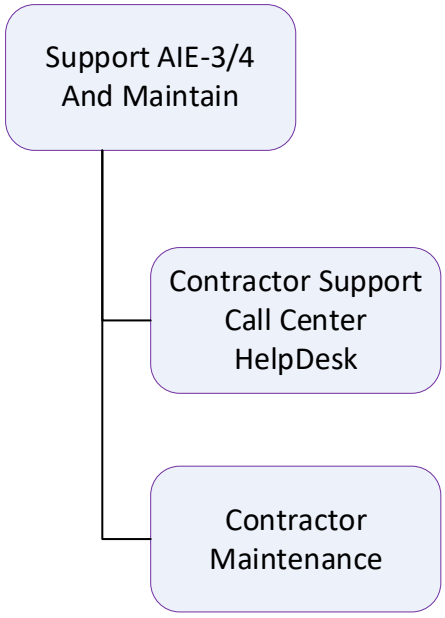

Figure 14: OV-5a-3, Decomposition of the Support Activity

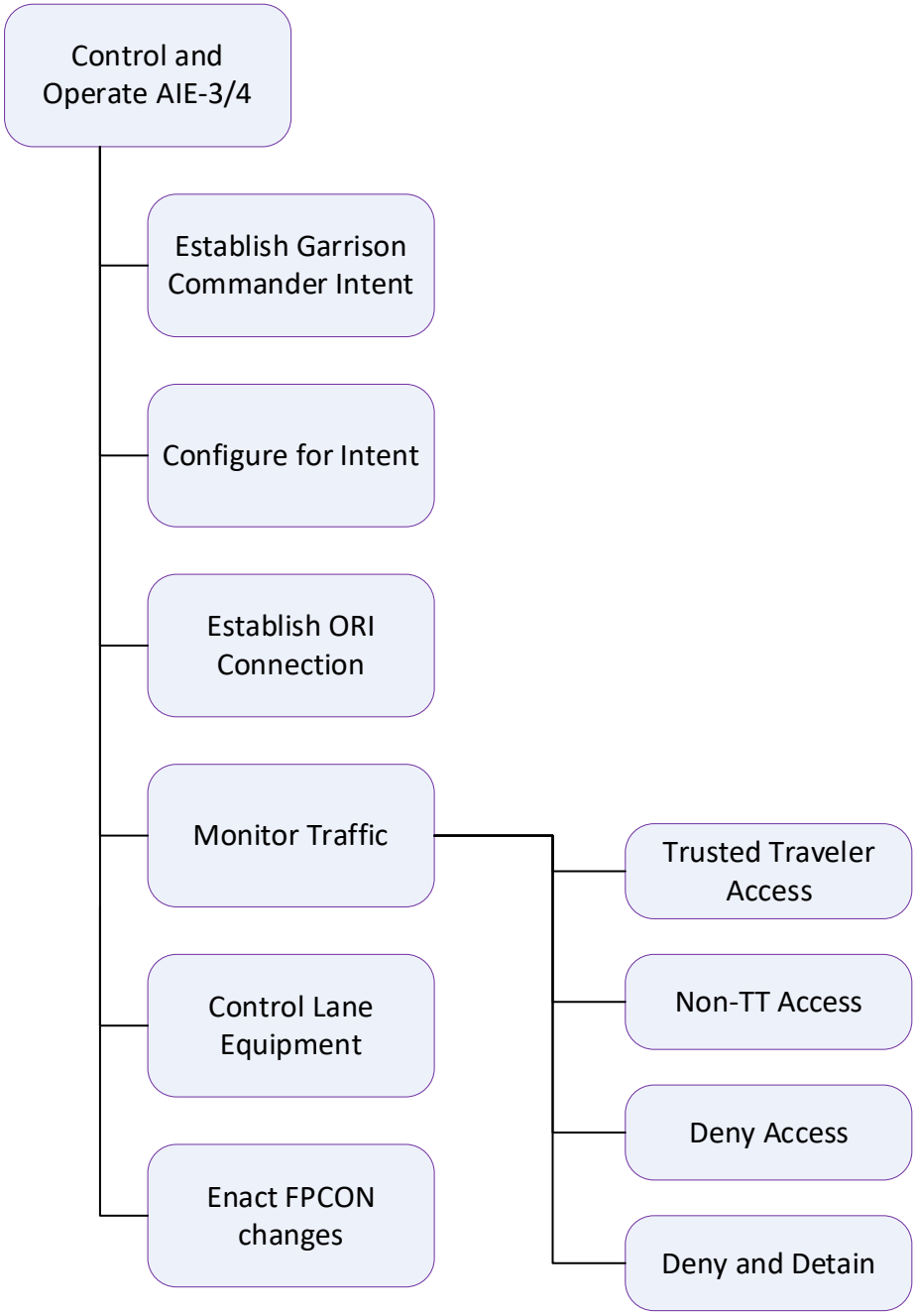

Figure 15: OV-5a-4, Decomposition of the Operate Activity

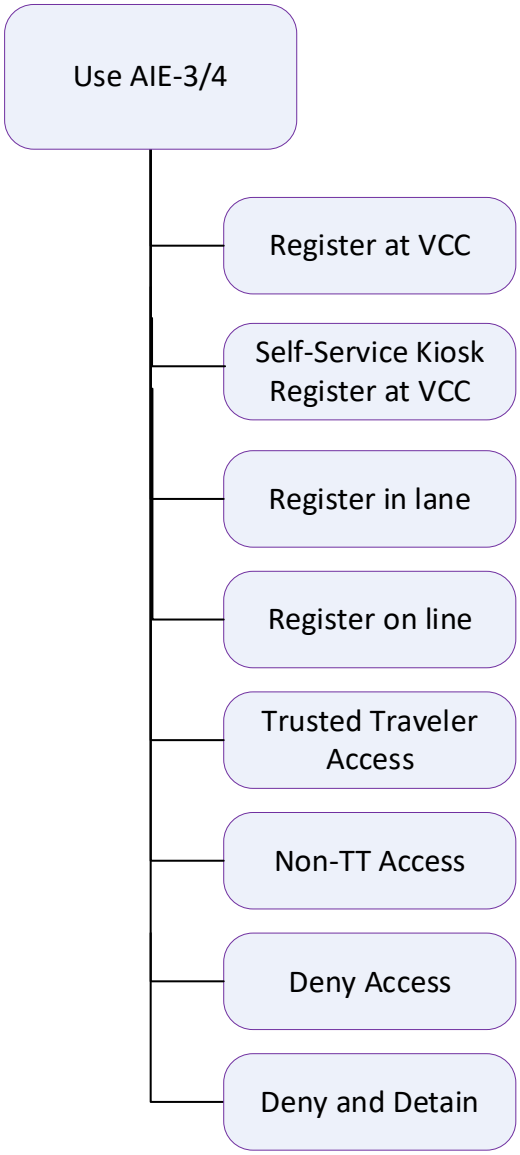

Figure 16: OV-5a-5, Decomposition of the Use Activity

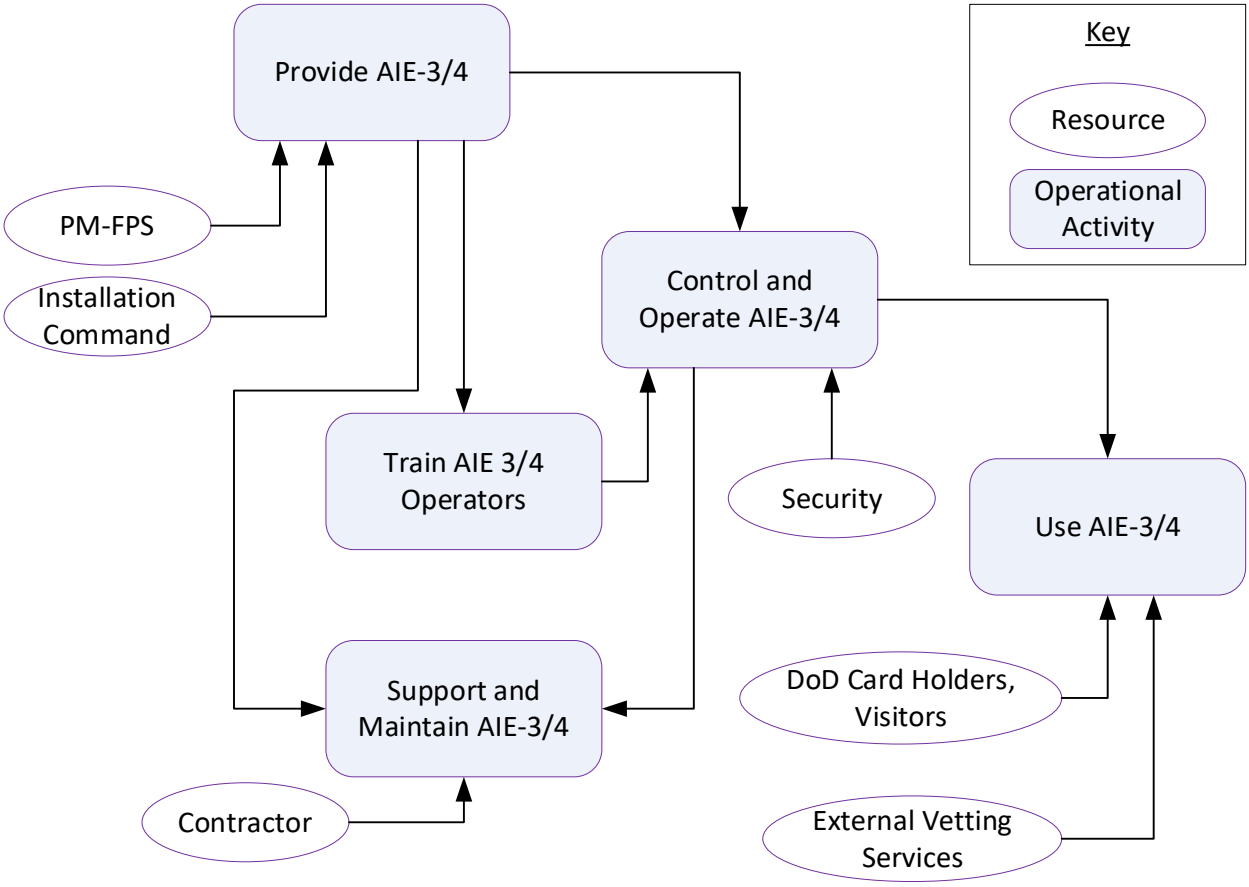

Figure 17: OV-5b, Operational Activity Model

APPENDIX H

OV-6a Operational Rules Model

APPENDIX H

OV-6a Operational Rules Model

The Operational Rules Model provides the operation rules and constraints for the AIE-3/4 System. This is provided in matrix form as it lends itself to detailing the rules and how they are related to the activities. The matrix is sorted by Operational Rule (OpR) and shows the mapping of the rule to one or more activities (as may be appropriate).

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
OpR-001	AIE-3/4 will provide one-way notifications of major alerts of physical security alarms, ACP gate crashes, AIE-3/4 Server building intrusions and other events impacting the physical security of Installations to the ICIDS system.	Control and Operate AIE-3/4	Automatic	Site Server ADAM Module	Not Implemented
OpR-002	The system will read, record and store credential and fingerprint information.	Register at VCC Register in Lane	Registrar User	Site/Cloud Server	
OpR-003	During the VCC registration process, the system will collect user information to include name, address, Date of Birth (DOB), signature, fingerprint, photo, expiration date of credential, user-specified PIN, class designation and unit of assignment.	Register at VCC	Registrar	Site/Cloud Server	
OpR-004	AIE-3/4 will also provide Automatic Registration at the ACP lanes for specific individuals holding valid credentials.	Register in Lane	User	Site/Cloud Server	
OpR-05	All visitors are required to be vetted against the National Crime Information Center (NCIC)/Interstate Identification Index (III) database.	Register at VCC	Registrar	RGWS Site/Cloud Server	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
OpR-06	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.	Register at VCC	Registrar	RGWS Site/Cloud Server	
OpR-07	Vetting through IoLS provides access to Defense Enrollment Eligibility Reporting System (DEERS), NCIC Wants and Warrants, authoritative databases, and shared data from other Services.	Register at VCC	Registrar	RGWS Site/Cloud Server	
OpR-08	During Registration, the AIE-3/4 System will identify individuals that are allowed Trusted Traveler privileges in accordance with applicable policies and regulations.	Trusted Traveler Access	Registrar	RGWS Site/Cloud Server	
OpR-09	Registration will produce a temporary pass (paper) and a long-term pass (plastic).	Register at VCC	Registrar	RGWS Site/Cloud Server	
OpR-010	Once registered, the user can immediately use the credential to enter the Installation via any AIE-3/4 enabled ACP as designated during registration.	Monitor Traffic	User	Site/Cloud Server Cache Box	
OpR-011	Portable registration capability is used to register users holding valid CACs, Teslin cards and state drivers' licenses.	Register with Portable System	Registrar	Portable Registration System	
OpR-012	AIE-3/4 will provide an automatic registration capability at the vehicle lanes for users holding valid CACs, Teslin, DBIDS cards and state drivers' licenses.	Register in Lane	User	Handheld Site/Cloud Server	
OpR-013	The system will query the driver for fingerprint and then capture and store as part of the PIR. This selectable configuration will be provided at each ACP and at each lane.	Register in Lane	User	Handheld Site/Cloud Server	
OpR-014	AIE-3/4 will display the retrieved image of the driver. Automatic access will not be granted if photo is not displayed.	Monitor Traffic	Guard	GBWS	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
OpR-015	If a fingerprint cannot be provided by the vehicle driver, then Guard intervention will be required.	Monitor Traffic	Guard	Handheld Site/Cloud Server	
OpR-016	The AIE-3/4 System allows the Installation Commander or authorized security official to electronically configure the system to require varying combinations of identification for any threat condition or FPCON level.	Enact FPCON Changes	Operator	Site/Cloud Server	
OpR-017	Cameras located at the front and rear of the lanes record activity in real-time, including images of license plates.	Monitor Traffic	Automatic	NVR	
OpR-018	Driver camera will capture the driver's image within a height range of three (3) to seven (7) feet from the ground.	Monitor Traffic	Automatic	NVR	
OpR-019	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.	Monitor Traffic	Guard	GBWS	
OpR-020	All access control transactions are recorded for potential reporting.	Monitor Traffic	Automatic	Site/Cloud Server	
OpR-021	The system will conspicuously identify to the Lane Guard whether the driver is allowed Trusted Traveler privileges.	Trusted Traveler Access	Guard	Handheld GBWS Site/Cloud Servrer	
OpR-022	A Gate Arm Assembly is integrated with the AIE-3/4 System to allow entry (arm goes up) upon successful user verification or deny entry (arm stays down) if access is denied.	Monitor Traffic	Guard	Symmetry Gate Controller	
OpR-023	The Gate Arm will not rise automatically for drivers who are denied Trusted Traveler privileges.	Non-Trusted Traveler Access	Auto	Symmetry Gate Controller	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
OpR-024	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 can grant/deny access, perform a lane override, and provide an integrated traffic hold.	Monitor Traffic	Guard	GBWS	
OpR-025	Wireless Handheld readers will have the ability to accept authorized credentials and PINs and may have the ability to capture fingerprints. 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 Wireless Handheld device will be configured such that the operator cannot modify configuration.	Monitor Traffic	Guard	Handheld	
OpR-026	The Site/Cloud Server, Cache Box store personal information records of all users enrolled at the Installation.	Control Lane Equipment	Automatic	Site/Cloud Server Cache Box	
OpR-027	The AIE-3/4 System will provide remote monitoring and control of all ACPs from a centralized location on site.	Monitor Traffic	Guard	CMWS	
OpR-028	One year of Contractor Logistics Support (CLS) will be provided upon Government acceptance of an installed AIE-3/4 System.	Support AIE-3/4	Contractor	AIE-3/4	

Figure 18: OV-6a, Operational Rules Model

APPENDIX I

OV-6b

APPENDIX I

OV-6b State Transition Description

The State Transition Description depicts how AIE-3/4 operational nodes or activities respond to various events by changing states and transitions through time.

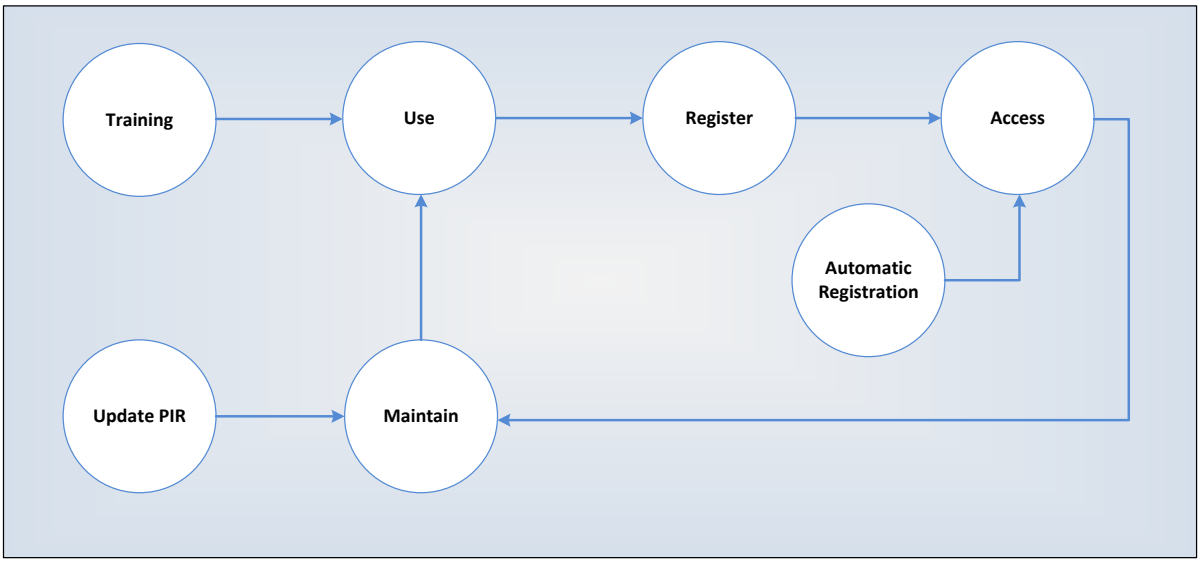

Figure 19: OV-6b, State Transition - Overview

APPENDIX J

OV-6c Operational Rules Model

APPENDIX J

OV-6c Event Trace Description

The AIE-3/4 Event Trace Description depicts a time-ordered process of performing activities associated with AIE-3/4 processes.

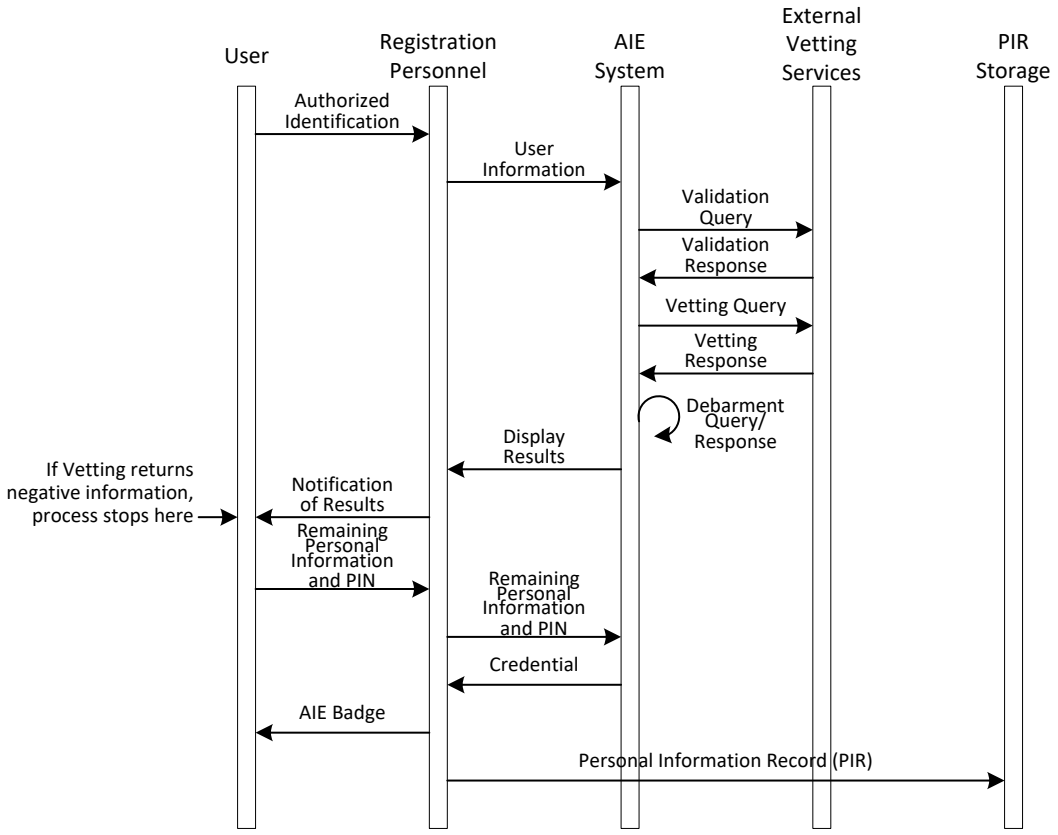

Figure 20: OV-6c, Event Trace - Registration

To facilitate understanding of the above event trace, the table below describes the same process; however, the tabular format enables more details to be incorporated.

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Registrant (user) requires AIE-3/4 registration	Authorized credentials such as DOD-issued credentials, driver's license, or passport.	Registrant (user)	Registrar (registration operator)	
EvTr-002	Registrar scans credential	2D barcode, 1D barcode, data read from chip-based smart card	Registrar	AIE-3/4 registration software	Registration software parses the 2D and 1D barcodes
EvTr-003	Request for additional information	SSN	Registrant	AIE-3/4 registration software	
EvTr-004	Receive SSN	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate. Query request command	AIE-3/4 registration software	Identity Management Middleware (IMM) at Site Server	Registrant enters SSN in case of DL
EvTr-005	Receipt of query request	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate. Query request command	IMM	Interoperability Layer Service (IoLS) or Law Enforcement (LE) vetting service	IMM determines which vetting service to use and implements the appropriate interface
EvTr-006	Receipt of response	Vetting details dependent on service used	IoLS or LE Vetting	IMM	LE Vetting provides limited Criminal Justice Information.
EvTr-007	Receipt of response	Vetting details dependent on service used, local or DOD credential number	IMM	Registration software	
EvTr-008		First Name, Middle Name, Last Name, DOB	Registration software	Debarment database	Registration software checks local Debarment DB
EvTr-009		Personal information and vetting responses	Registration software	Registrar	Vetting and partial personal information record (PIR) Information is displayed for Registrar
EvTr-010	Registrar Cancels Operation	Click on Cancel Button	Registrar	Registration software	Optional action if vetting provides red light.

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-011	Registrant enters additional information	PIN, signature capture, fingerprint capture, photo capture	Registrant	Registration software	Most information is optional. PIR is assembled.
EvTr-012		Various (optional)	Registrar	Registration software	Manager or Administrator operator can override existing data with comment.
EvTr-013		PIR	Registration software	Site Server Symmetry Import Database	
EvTr-014		First Name, Last Name, Start Date, Expiration Date, photo, credential number, Gold Star, Trusted Traveler	Registration software	Card printer or paper printer	Print badge
EvTr-015	Printing complete	AIE-3/4 badge	Registrar	Registrant	
EvTr-016		PIR	Hawkeye SyncServices	App/DB Servers Import DB	Hawkeye Sync Services transfers PIR
EvTr-017		Credential number, ACP Access, Trusted Traveler status	Site Server DB	Symmetry Local Processor	Record is ready for lane access

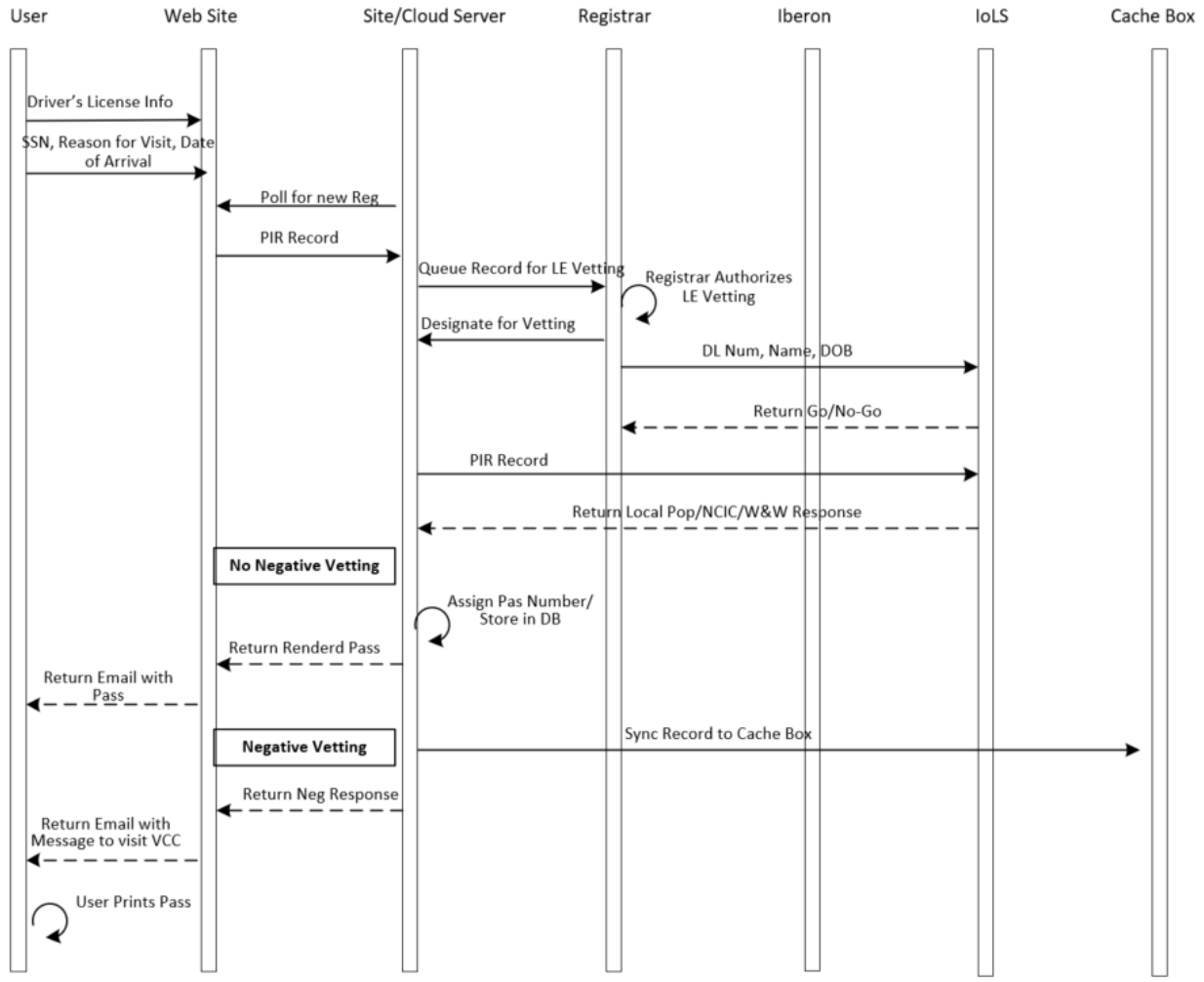

Figure 21: OV-6c, Event Trace – Visitor Self-Service Web Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Registrant (user) requires AIE-3/4 registration	Registrant engages kiosk, or navigates to web-based visitor registration site	Registrant	Visitor web-based registration site	
EvTr-002	Registrant enters data	Authorized credentials such as Driver's License, or identity information such as SSN, DOB, and Name	Registrant (user)	Visitor web-based registration site	
EvTr-003	Request for additional information	Date of visit, reason for visit, contact information	Registrant	Visitor web-based registration site	PIR record is created
EvTr-004	Data Submitted	PIR Record	Visitor web site	Visitor web site	Request is queued for Installation

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-005	Data collected from visitor web site	PIR Record	Visitor Web site	Identity Management Middleware (IMM) at Site Server	Data is collected by the site
EvTr-006	Vetting requests queued for operator	First Name, Middle Name, Last Name, SSN, DOB	AIE-3/4 Registration software	Identity Management Middleware (IMM) at Site Server	
EvTr-007	Vetting request is authorized	Vetting status field	Registrar	Identity Management Middleware (IMM) at Site Server	
EvTr-008	Background Vetting Process	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate.	Identity Management Middleware (IMM) at Site Server	NCITE Vetting Service	Happens in under 1 minute
EvTr-009	Receipt of response	Vetting response details limited to valid/not valid/detain	NCITE Vetting Service	IMM	
EvTr-010		First Name, Middle Name, Last Name, DOB	Registration software	Debarment database	Registration software checks local Debarment DB
EvTr-011	If negative response, print negative response document	Fixed text, “Additional processing required”, Name and picture if available	IMM	Designated printer	
EvTr-012	If positive response, create registration record	PIR	Registration software	Registration database	
EvTr-013	Print visitor pass	First Name, Last Name, Start Date, Expiration Date, photo, credential number	Registration software	Card printer or paper printer	Print badge
EvTr-014	Printing complete	AIE-3/4 badge	Registrar	Registrant	
EvTr-015		PIR	Hawkeye Sync Services	Cache Box Import DB	Only records for the Installation where the Cache box is located are replicated to the Cache box.
EvTr-016		Credential number, ACP Access, Trusted Traveler status	Site Server DB App/DB Servers	Symmetry Local Processor	Record is ready for lane access

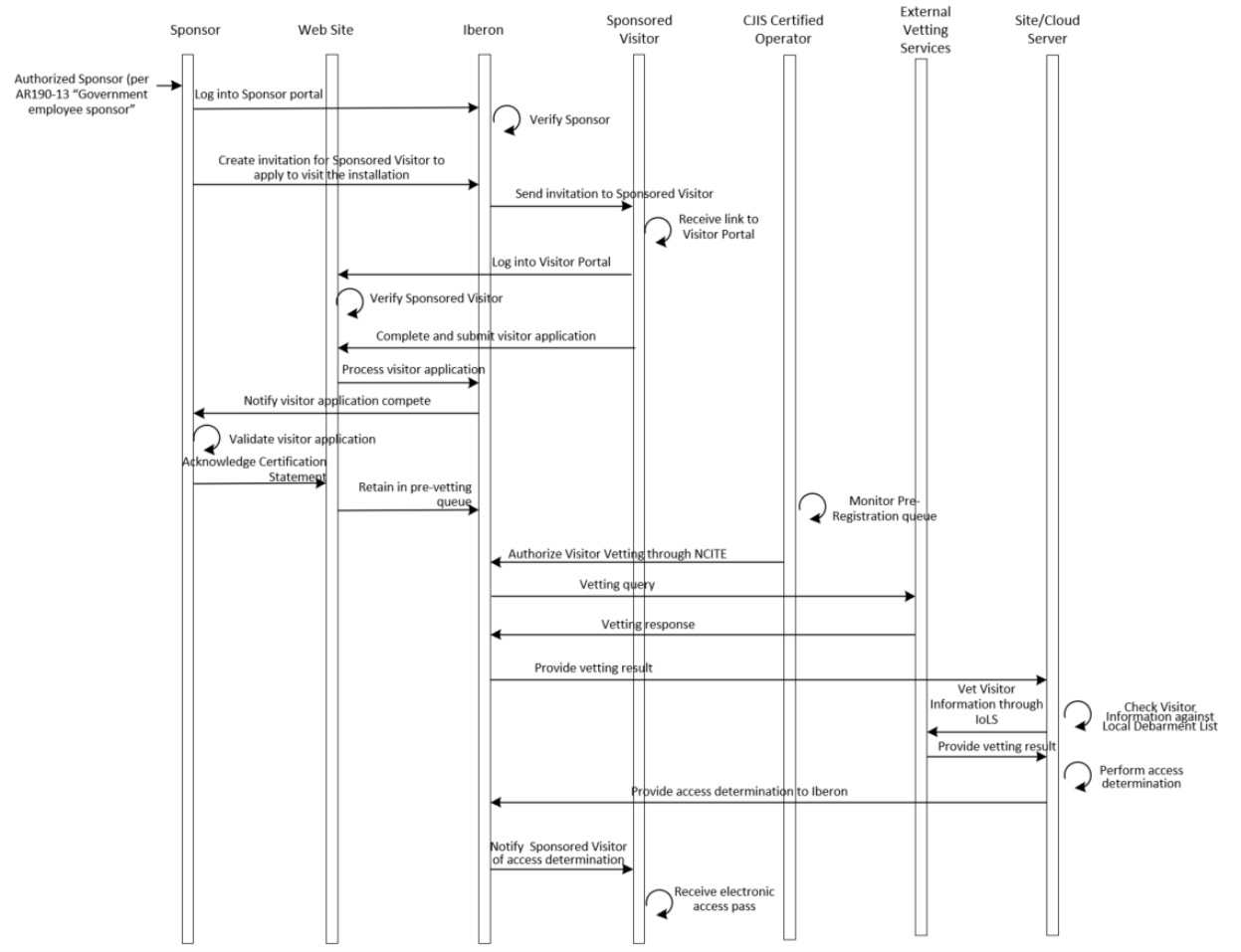

Figure 22: OV-6c, Event Trace – Online Vetting and Registration - Access Granted

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Sponsor				Sponsor must comply with AR190-13 "Government employee sponsor"
EvTr-002	Log on to Sponsor Portal	Sponsor login credentials	Sponsor	Sponsor Portal	Sponsor Portal hosted on Cloud Server
EvTr-003	Verify sponsor	Sponsor Login credentials	Sponsor	Sponsor Portal	
EvTr-004	Create invite	Sponsored Visitor information	Sponsor, Sponsor Portal	Iberon	Iberon provides user interface and workflow
EvTr-005	Send invite	Link to Visitor Portal	Iberon	Sponsored visitor email, phone	

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-006	Receive invite notification	Notification message	Iberon	Sponsored visitor email, phone	
EvTr-007	Log on to Visitor Portal	Visitor Login credential	Sponsored Visitor	Iberon	
EvTr-008	Verify visitor	Visitor Login credentials	Visitor	Visitor Portal	Visitor Portal hosted on Cloud Server
EvTr-009	Submit visitor application	Completed visitor application information	Visitor	Visitor Portal	
EvTr-010	Check information for completeness	Completed visitor application information	Visitor Portal	Iberon	
EvTr-011	Notify Sponsor that application is complete	Notification Message	Iberon	Sponsor	
EvTr-012	Sponsor validates visitor information	Completed visitor application information	Iberon	Sponsor Portal	
EvTr-013	Sponsor submits to vetting queue	Visitor application information	Sponsor Portal	Iberon	
EvTr-014	CJIS Certified Operator submits for vetting	Visitor application information	CJIS Certified Operator, Sponsor Portal	Iberon	
EvTr-015	Vet visitor through LE	Visitor application information	Iberon	External Vetting Service	LE Vetting provides limited Criminal Justice Information.
EvTr-016	Receipt of response	Vetting details dependent on service used	External Vetting Service	Iberon	
EvTr-017	Send LE vetting results to Cloud server	LE vetting results	Iberon	Cloud Server	Cloud server will use LE vetting results in access determination processing
EvTr-018	Vet visitor through IoLS	Visitor application information	IMM at Cloud server	IoLS	
EvTr-019	Receipt of response	Vetting details	External Vetting Service	IMM at Cloud Server	
EvTr-020	Perform access determination	Access determination status	IMM at Cloud Server	IMM at Cloud Server	
EvTr-021	Send access determination to sponsor	Access determination status access granted	Iberon	Sponsor	
EvTr-022	Send access determination to visitor	Access determination, Access granted electronic pass	Iberon	Visitor	An email and/or text is sent to the visitor with the scannable access pass

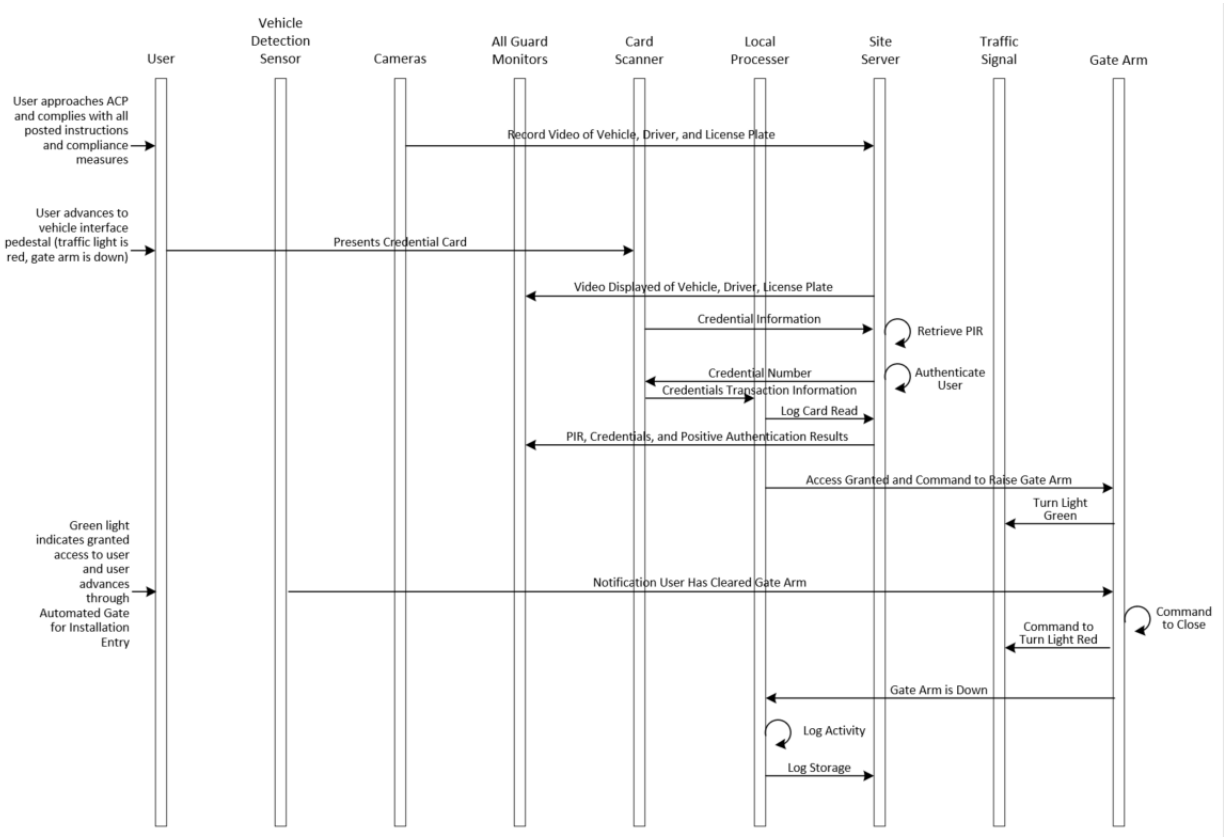

Figure 23: OV-6c, Event Trace - ACP Operations - Access Granted

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001					Removed
EvTr-002	Entry Detection	Command to record camera video (3 cameras)	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-003	Entry Detection	Command to capture license plate number	Symmetry (Site Server)	LPR Camera	LPR capability available but not in use.
EvTr-004		Video streams (3 cameras)	Video recorder	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display video of driver presenting credential, front, and rear of car
EvTr-005	User presents credential at barcode or CAC reader	Credential Number	Rhino Reader	IMM (Site Server)	IMM software manages credential workflow

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-005a	User presents credential at barcode or CAC reader	Credential Number	QScan Reader	IMM (Site Server)	IMM software manages credential workflow
EvTr-006		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-007	Credential is not known locally	Unknown Card Message to monitoring clients	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	If Automatic Registration enabled, see different Event Trace
EvTr-008	Credential is known locally	Wiegand credential number	Rhino Reader	Symmetry Gate Controller	
EvTr-009		PIR data	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display PIR for guard, and access decision
EvTr-010	Access Granted, with Trusted Traveler status	Raise gate arm, Turn light green	Symmetry gate controller	Gate Arm	Used with Rhino Reader
EvTr-010a	Access Granted, with Trusted Traveler status	Raise gate arm, Turn light green	IMM	ADAM Module	Used with Qscan Reader to set relay
EvTr-011	Valid Badge with no Trusted Traveler				Gate arm does not go up automatically
EvTr-012	Successful Credential read	Disable card reader	Symmetry	Symmetry Gate Controller, Rhino Reader,	Prevents next car in line from scanning before car exits lane
EvTr-012a	Successful Credential read	Disable card reader	IMM	ADAM Module, Qscan Reader	Prevents next car in line from scanning before car exits lane
EvTr-012b		Change Message Display	IMM	ADAM Module, Qscan Reader	
EvTr-013	Guard grants access after review	Grant access screen selection	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Symmetry	
EvTr-014		Raise gate arm, Turn light green	Symmetry gate controller,	Gate Arm, light	Used with Rhino Reader
EvTr-014a		Raise gate arm, Turn light green	ADAM Module, 24VDC Relay	Gate Arm, light	Used with Qscan Reader
EvTr-015		Credential number	Symmetry local processor	Symmetry	Symmetry logs transaction with date/time stamp Used with Rhino Reader

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-016	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	Symmetry Gate Controller	Used with Rhino Reader
EvTr-016a	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	ADAM Module	Used with Qscan Reader
EvTr-017		Command to turn light red, lower gate arm	Symmetry Gate Controller	Gate arm, light	Used with Rhino Reader
EvTr-017a		Command to turn light red, lower gate arm	ADAM Module, 24VDC Relay	Gate arm, light	Used with Qscan Reader
EvTr-018		Enable card reader	Symmetry	Symmetry Gate Controller, Rhino Reader	Used with Rhino Reader
EvTr-018a		Enable card reader	IMM Server	ADAM Module, Qscan Reader	Used with Qscan Reader
EvTr-018b		Change message Display	IMM Server	Qscan Reader	Used with Qscan Reader
EvTr-019	Obstruction in gate arm path	Emergency gate arm up	Obstruction detector	Gate arm	
EvTr-020		Transaction information	Symmetry Local Processor	Symmetry	All associated transactions are logged with time/date stamp. Used with Rhino Reader
EvTr-020a		Transaction information	IMM Server	Symmetry	Used with Qscan Reader

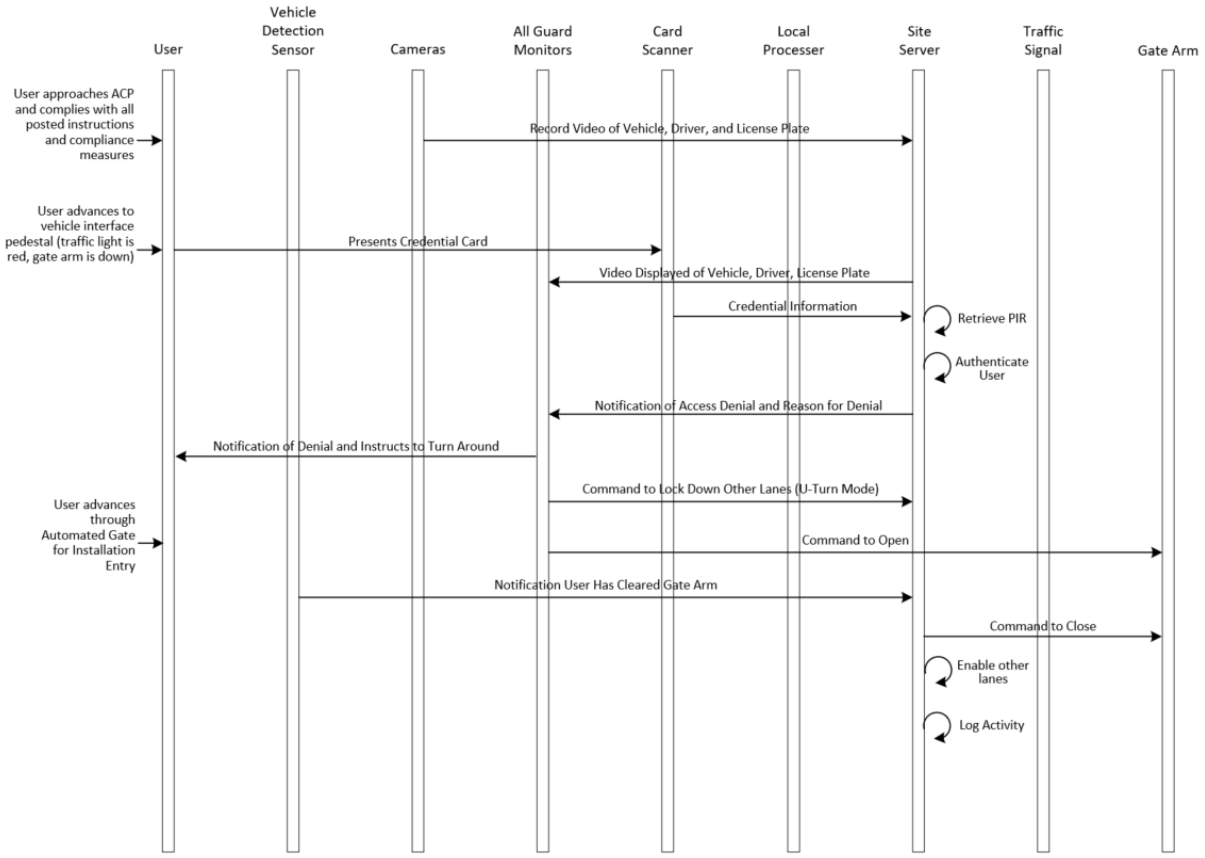

Figure 24: OV-6c, Event Trace - ACP Operations - Access Denied

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001					Removed
EvTr-002	Entry Detection	Command to record camera video (3 cameras)	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-003	Entry Detection	Command to capture license plate number	Symmetry (Site Server)	LPR Camera	LPR capability available but not in use.
EvTr-004		Video streams (3 cameras)	Video recorder	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display video of driver presenting credential, front, and rear of car
EvTr-005	User presents credential at barcode or CAC reader	Credential Number	Rhino Reader	IMM (Site Server)	IMM software manages credential workflow

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-005a	User presents credential at barcode or CAC reader	Credential Number	QScan Reader	IMM (Site Server)	IMM software manages credential workflow
EvTr-006		Credential Number	IMM (Server)	Symmetry DB	Look for existing credential in DB
EvTr-007	Credential is not known locally	Unknown Card Message to monitoring clients	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	If Automatic Registration enabled, see different Event Trace
EvTr-008	Credential is known locally	Wiegand credential number	Rhino Reader	Symmetry Gate Controller	
EvTr-009		PIR data	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display PIR for guard, and access decision
EvTr-010	Access Denied	Access Denied message to monitoring clients	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Could be due to periodic vetting update, or added to Debarment list
EvTr-011	Guard performs all lane hold	Screen selection	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Symmetry	
EvTr-012		Command to lower gate arms at all lanes, disable readers.	Symmetry gate controllers – all lanes	Gate arms, traffic light – all lanes	Used with Rhino Reader
EvTr-012a		Disable card reader all lanes	IMM (Server)	ADAM Module, Qscan Reader	
EvTr-012b		Change Message Display	IMM (Server)	ADAM Module, Qscan Reader	
EvTr-013		Command to raise gate arm at lane, light stays red	Symmetry gate controller	Gate arm, light	Guard instructs car to turn around
EvTr-013a		Command to raise gate arm at lane, light stays red	IMM (Server), ADAM Module, 24VDC Relay	Gate arm, light	Guard instructs car to turn around Used with Qscan Reader
EvTr-014	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	Symmetry Gate Controller	Used with Rhino Reader
EvTr-014a	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	ADAM Module	Used with Qscan Reader

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-015		Command to turn light red, lower gate arm	Symmetry Gate Controller	Gate arm, light	Used with Rhino Reader
EvTr-015a		Command to turn light red, lower gate arm	IMM (Server), ADAM Module, 24VDC Relay	Gate arm, light	Used with Qscan Reader
EvTr-016		Enable card reader – all lanes	Symmetry	Symmetry Gate Controller, Rhino Reader	Used with Rhino Reader
EvTr-016a		Enable card reader – all lanes	IMM (Server)	ADAM Module, Qscan Reader	Used with Qscan Reader
EvTr-017	Obstruction in gate arm path	Emergency gate arm up	Obstruction detector	Gate arm	
EvTr-018		Transaction information	Symmetry Local Processor	Symmetry	All associated transactions are logged with time/date stamp
EvTr-018a		Transaction information	IMM (Server)	Symmetry	Used with Qscan Reader

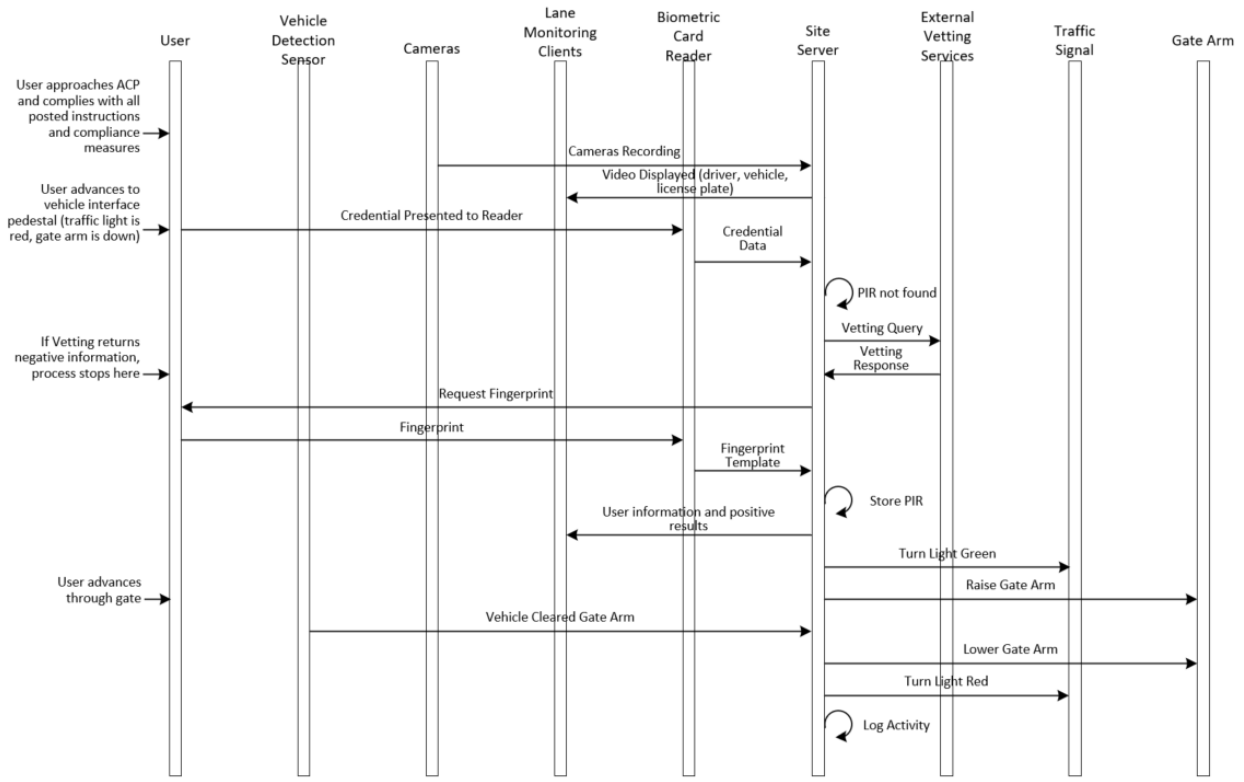

Figure 25: OV-6c, Event Trace - ACP Operations - Automatic Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001					Removed
EvTr-002	Entry Detection	Command to record camera video (3 cameras)	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-003	Entry Detection	Command to capture license plate number	Symmetry (Site Server)	LPR Camera	LPR capability available but not in use.
EvTr-004		Video streams (3 cameras)	Video recorder	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display video of driver presenting credential, front, and rear of car
EvTr-005	User presents credential at barcode or CAC reader	Credential Number	Driver, Rhino Reader	IMM (Site Server)	IMM software manages credential workflow
EvTr-005a	User presents credential at barcode or CAC reader	Credential Number	Qscan Reader	IMM (Site Server)	IMM software manages credential workflow
EvTr-006		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-007	Credential is known locally	Wiegand credential number	Rhino Reader	Symmetry Gate Controller	See Access Grant or Access Denied Event Trace Used with Rhino Reader
Ev Tr-007a	Credential is known locally	Credential number	Qscan Reader	ADAM module	See Access Grant or Access Denied Event Trace Used with Qscan Reader
EvTr-008	Credential is not known locally	Unknown Card (Access Denied) Message to monitoring clients	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	If Automatic Registration NOT enabled. Guard proceeds with Access Denied Flow
EvTr-009	Request for additional information through reader display	SSN	Driver, Rhino Reader	IMM AutoReg at Site server	Only when user presented Driver License. Jump to EvTr-014 for DOD Credential.
EvTr-009a	Request for additional information through reader display	SSN	Driver, Qscan Reader	IMM AutoReg at Site server	Only when user presented Driver License. Jump to EvTr-014 for DOD Credential.
EvTr-010	Receive SSN	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number. Query request command	IMM AutoReg	IMM at Site Server	

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-011	Receipt of query request	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate. Query request command	IMM at Site Server	Law Enforcement (LE) vetting service	IMM determines which vetting service to use and implements the appropriate interface
EvTr-012	Receipt of response	Vetting details dependent on service used	LE Vetting	IMM	LE Vetting provides limited Criminal Justice Information.
EvTr-013	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	
EvTr-014		DOD Credential Number	Rhino Reader	IMM AutoReg at Site server	Only when user presented DOD credential
EvTr-014a		DOD Credential Number	QScan Reader	IMM AutoReg at Site server	Only when user presented DOD credential
EvTr-015		DOD Credential Number	IMM AutoReg	IMM at Site Server	
EvTr-016		DOD Credential Number	IMM at Site Server	Interoperability Layer Service (IoLS)	IMM determines which vetting service to use and implements the appropriate interface
EvTr-017	Receipt of response	Vetting details dependent on service used	IoLS	IMM	IoLS provides User details (Name, DOB, security alerts, and other Credentials)
EvTr-018	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	
EvTr-019		First Name, Middle Name, Last Name, DOB	IMM AutoReg	Debarment database	Automatic Registration checks local Debarment DB
EvTr-020	IMM AutoReg requests FP	Fingerprint capture	Registrant	IMM AutoReg	PIR is assembled. Used with Rhino Reader
EvTr-021		PIR	IMM AutoReg	Symmetry DB	
EvTr-022		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-023		Command to send Wiegand data	IMM	Rhino Reader	Used with Rhino Reader
EvTr-024	Credential imported correctly	Wiegand credential number	Rhino Reader	Symmetry Gate Controller	Used with Rhino Reader
EvTr-025		PIR data	Symmetry	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display PIR for guard, and access decision
EvTr-026	Access Granted, with Trusted Traveler status	Raise gate arm, Turn light green	Symmetry gate controller	Gate Arm	Used with Rhino Reader

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-026a	Access Granted, with Trusted Traveler status	Raise gate arm, Turn light green	ADAM Module, 24VDC Relay	Gate Arm	Used with Qscan Reader
EvTr-027	Valid Badge with no Trusted Traveler				Gate arm does not go up automatically
EvTr-028	Successful Credential read	Disable card reader	Symmetry	Symmetry Gate Controller, Rhino Reader	Prevents next car in line from scanning before car exits lane
EvTr-28a	Successful Credential read	Disable card reader	IMM	ADAM Module Relay Qscan	Prevents next car in line from scanning before car exits lane Used with Qscan Reader
EvTr-028b		Change Message Display	IMM	ADAM Module, Qscan Reader	Used with Qscan Reader
EvTr-029	Guard grants access after review	Grant access screen selection	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Symmetry	
EvTr-030		Raise gate arm, Turn light green	Symmetry gate controller	Gate Arm, light	Used with Rhino Reader
EvTr-030a		Raise gate arm, Turn light green	ADAM Module, 24VDC Relay	Gate Arm, light	Used with Qscan Reader
EvTr-031		Credential number	Symmetry local processor	Symmetry	Symmetry logs transaction with date/time stamp
EvTr-032	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	Symmetry Gate Controller	Used with Rhino Reader
EvTr-032a	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	ADAM Module	Used with Qscan Reader
EvTr-033		Command to turn light red, lower gate arm	Symmetry Gate Controller	Gate arm, light	Used with Rhino Reader
EvTr-033a		Command to turn light red, lower gate arm	ADAM Module, 24VDC Relay	Gate arm, light	Used with Qscan Reader
EvTr-034		Enable card reader	Symmetry	Symmetry Gate Controller, Rhino Reader	Used with Rhino Reader
EvTr-034a		Enable card reader	IMM Server	ADAM Module, Qscan Reader	Used with Qscan Reader
EvTr-034b		Change message Display	IMM Server	Qscan Reader	Used with Qscan Reader
EvTr-035	Obstruction in gate arm path	Emergency gate arm up	Obstruction detector	Gate arm	Used with Qscan Reader
EvTr-036		Transaction information	Symmetry Local Processor	Symmetry	All associated transactions are logged with time/date stamp. Used with Rhino Reader
EvTr-036a		Transaction information	IMM Server	Symmetry	Used with Qscan Reader

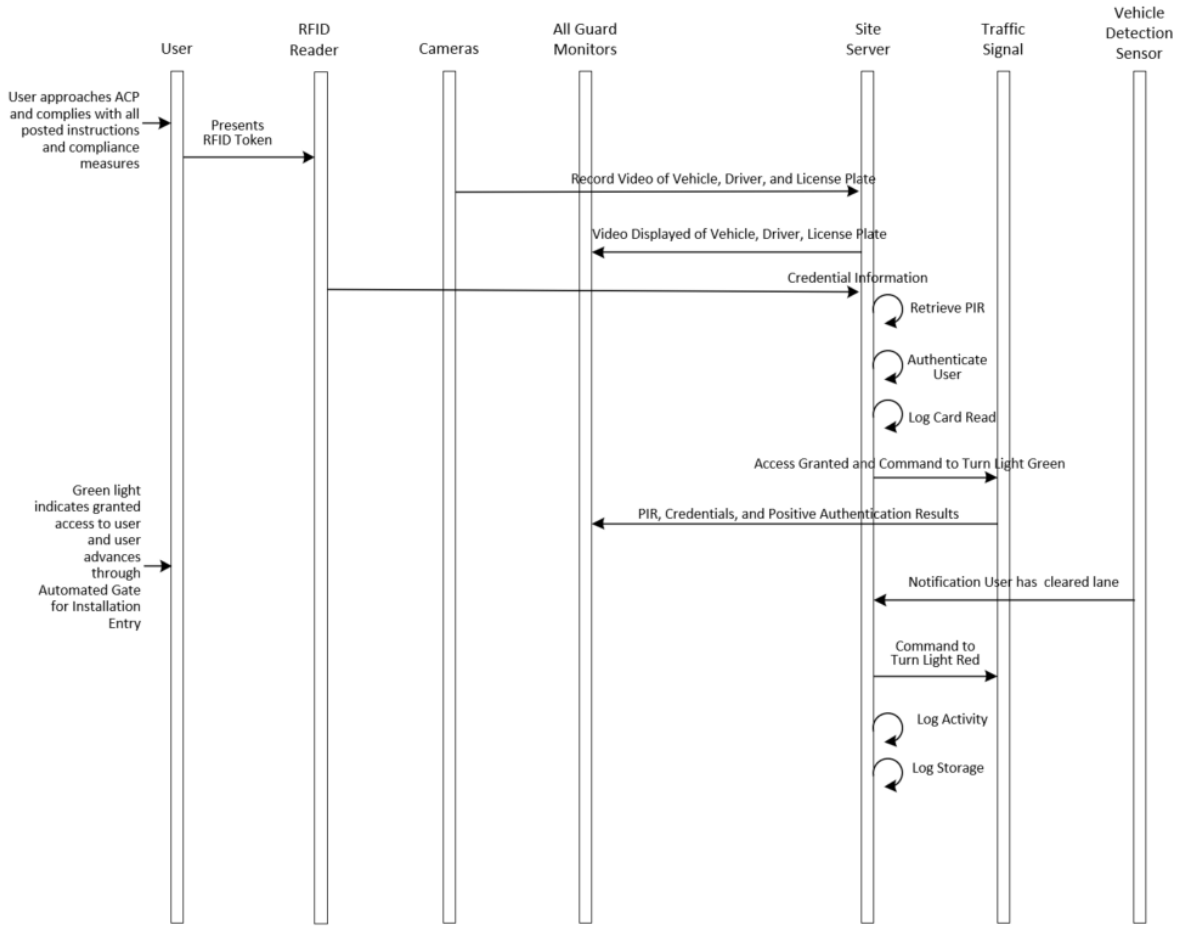

Figure 26: OV-6c, Event Trace - RFID Access Granted

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Vehicle enters “Fast Lane”				RFID used for “Fast Lane” Access
EvTr-002	User presents RFID Token Lane”	Credential Number	RFID Reader	IMM	
EvTr-003	Entry Detection	Command to record camera video (3 cameras)	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-004		Video streams (3 cameras)	Video recorder	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display video of driver presenting credential, front, and rear of car

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-005		PIR data	Visual Verifier	Guard booth lane client Gatehouse lane client Remote Central Monitoring client	Display PIR for guard, and access decision
EvTr-006	Access Granted, with Trusted Traveler status	Turn light green	ADAM Module, 24VDC Relay	Traffic Light	Gate Arm not in automatic mode with Fast Lane
EvTr-007		Credential number	IMM	Symmetry	Symmetry logs transaction with date/time stamp
EvTr-008	Vehicle crosses exit detector	Contact closure	Exit Loop Controller	ADAM Module	
EvTr-009		Command to turn light red	IMM	ADAM Module, 24VDC Relay	
EvTr-009		Transaction information	IMM Server	Symmetry	

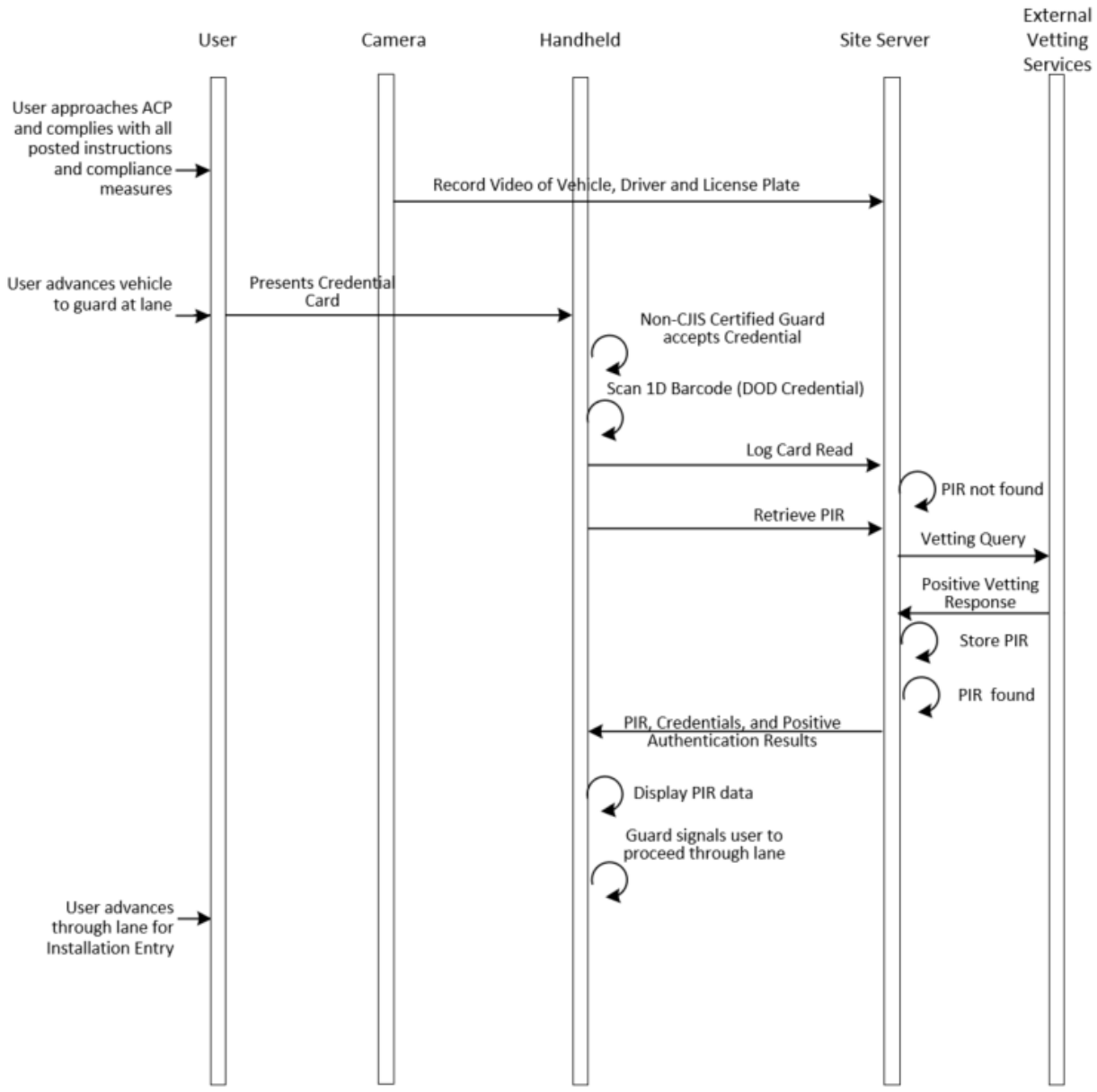

Figure 27: OV-6c, Event Trace - Handheld Operations - Tier 1 Access Granted/Auto Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Vehicle approaches ACP	Video motion detection	Overview camera	Video Recorder	
EvTr-002	Entry Detection	Command to record camera video	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-003	User presents credential to Non-CJIS certified guard with handheld	Credential Number	Driver, Handheld	IMM (Site Server)	IMM software manages credential workflow

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-004		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-005	Credential is known locally	PIR data	IMM	Handheld	Display PIR for guard, and access decision. Continue to EvTr-017
EvTr-006	Credential is not known locally	Unknown Card (Access Denied) Message to monitoring clients	IMM	Handheld	Automatic Registration enabled.
EvTr-007		DOD Credential Number	Handheld	IMM AutoReg at Site server	Only when user presented DOD credential
EvTr-008		DOD Credential Number	IMM AutoReg	IMM at Site Server	
EvTr-009		DOD Credential Number	IMM at Site Server	Interoperability Layer Service (IoLS)	IMM determines which vetting service to use and implements the appropriate interface
EvTr-010	Receipt of response	Vetting details dependent on service used	IoLS	IMM	IoLS provides User details (Name, DOB, security alerts, and other Credentials)
EvTr-011	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	Positive result
EvTr-012		First Name, Middle Name, Last Name, DOB	IMM AutoReg	Debarment database	Automatic Registration checks local Debarment DB
EvTr-013	IMM AutoReg requests FP	Fingerprint capture	Registrant	IMM AutoReg	PIR is assembled. Used with fingerprint enabled handheld only
EvTr-014		PIR	IMM AutoReg	Symmetry DB	
EvTr-015		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-016		PIR data	IMM	Handheld	Display PIR for guard, and access decision
EvTr-017	Access Granted	Handheld	IMM	Guard	Handheld displays granted access notification and green background
EvTr-018	Guard signals user to proceed through lane	Guard Signal	Guard	User	

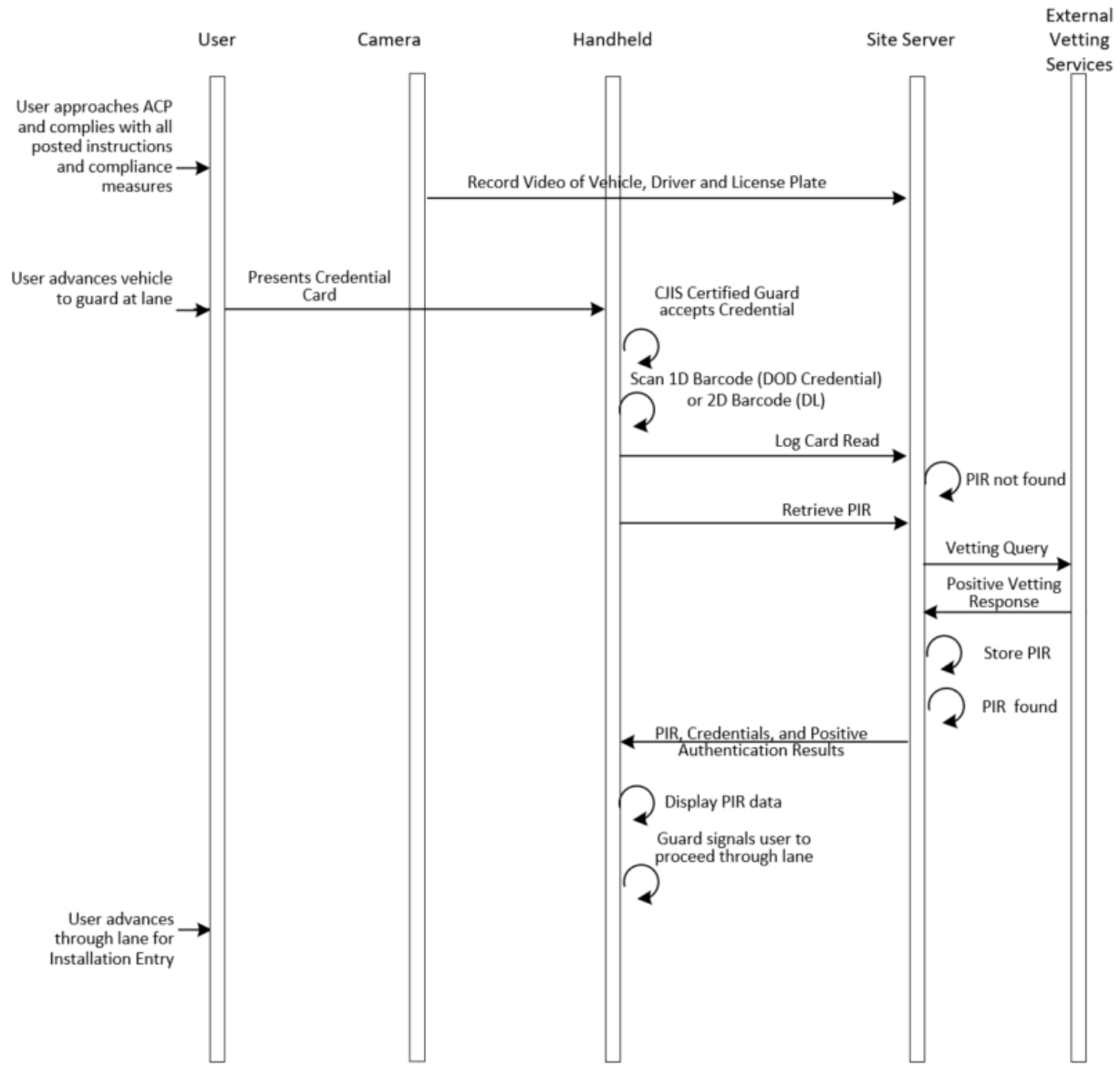

Figure 28: OV-6c, Event Trace - Handheld Operations - Tier 1 Access Granted/In Lane Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Vehicle approaches ACP	Video motion detection	Overview camera	Video Recorder	
EvTr-002	Entry Detection	Command to record camera video	Symmetry (Site Server)	Video recorder (NVR)	
EvTr-003	User presents credential to Non-CJIS certified guard with handheld	Credential Number	Driver, Handheld	IMM (Site Server)	IMM software manages credential workflow
EvTr-004		Credential Number	IMM	Symmetry DB	Look for existing credential in DB

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-005	Credential is known locally	PIR data	IMM	Handheld	Display PIR for guard, and access decision. Continue to EvTr-022
EvTr-006	Credential is not known locally	Unknown Card (Access Denied) Message to monitoring clients	IMM	Handheld	Automatic Registration enabled.
EvTr-007	Request for additional information through display	SSN	Driver, Handheld	IMM AutoReg at Site server	Only when user presented Driver License. Jump to EvTr-012 for DOD Credential.
EvTr-008	Receive SSN	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number. Query request command	IMM AutoReg	IMM at Site Server	
EvTr-009	Receipt of query request	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate. Query request command	IMM at Site Server	Law Enforcement (LE) vetting service	IMM determines which vetting service to use and implements the appropriate interface
EvTr-010	Receipt of response	Vetting details dependent on service used	LE Vetting	IMM	LE Vetting provides limited Criminal Justice Information.
EvTr-011	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	Positive result continues to with EvTr-022.
EvTr-012		DOD Credential Number	Handheld	IMM AutoReg at Site server	Only when user presented DOD credential
EvTr-013		DOD Credential Number	IMM AutoReg	IMM at Site Server	
EvTr-014		DOD Credential Number	IMM at Site Server	Interoperability Layer Service (IoLS)	IMM determines which vetting service to use and implements the appropriate interface
EvTr-015	Receipt of response	Vetting details dependent on service used	IoLS	IMM	IoLS provides User details (Name, DOB, security alerts, and other Credentials)
EvTr-016	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	
EvTr-017		First Name, Middle Name, Last Name, DOB	IMM AutoReg	Debarment database	Automatic Registration checks local Debarment DB.

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-018	IMM AutoReg requests FP	Fingerprint capture	Registrant	IMM AutoReg	PIR is assembled. Used with fingerprint enabled handheld only.
EvTr-019		PIR	IMM AutoReg	Symmetry DB	
EvTr-020		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-021		PIR data	IMM	Handheld	Display PIR for guard, and access decision
EvTr-022	Access Granted	Handheld	IMM	Guard	Handheld displays granted access notification and green background
EvTr-023	Guard signals user to proceed through lane	Guard Signal	Guard	User	

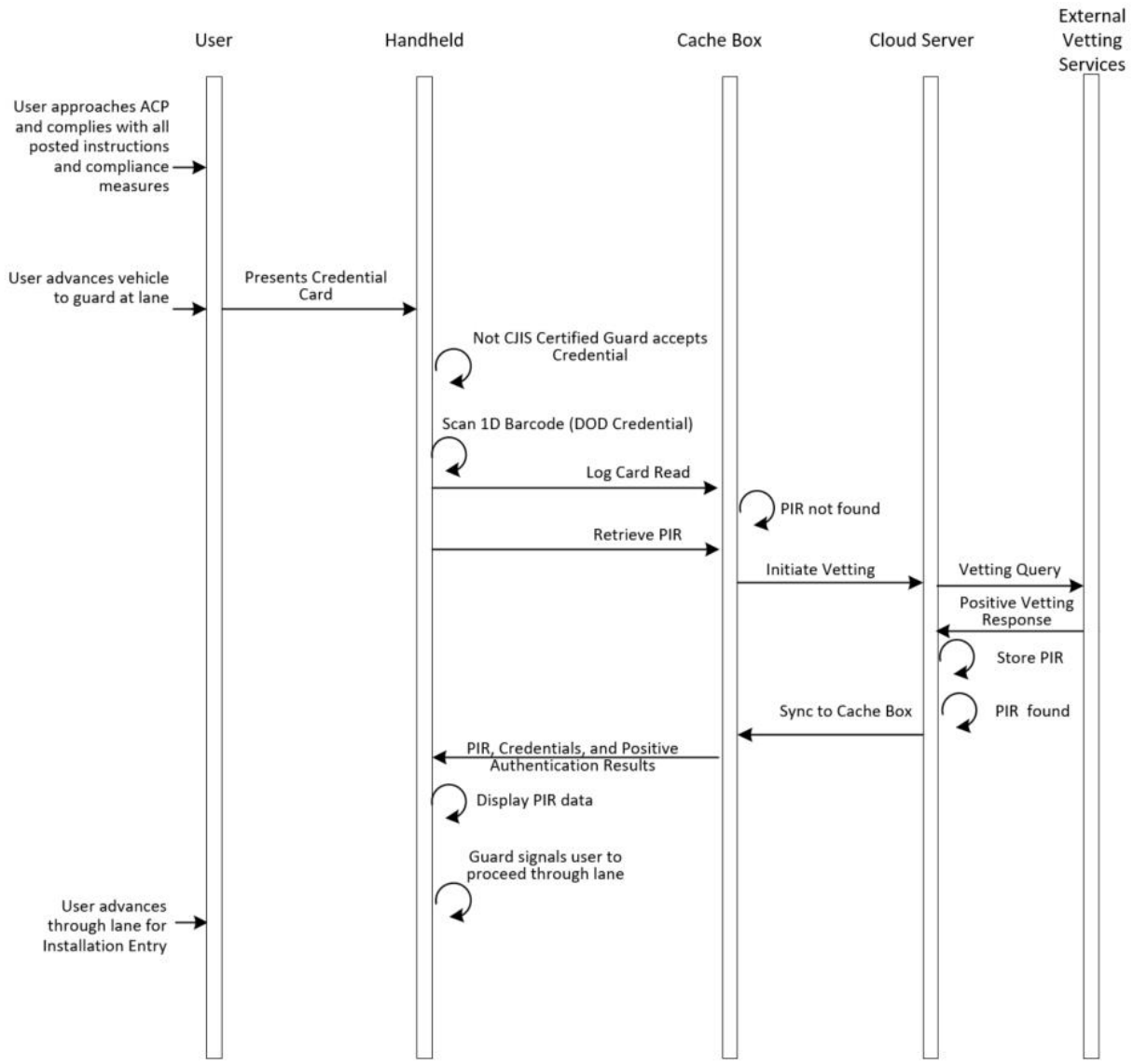

Figure 29: OV-6c, Event Trace - Handheld Operations - Tier 2 Access Granted/Auto Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Vehicle approaches ACP				
EvTr-002	User presents credential to Non-CJIS certified guard with handheld	Credential Number	Driver, Handheld	IMM (Cache Box)	IMM software manages credential workflow
EvTr-003		Credential Number	IMM	Symmetry DB	Look for existing credential in DB

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-004	Credential is known locally	PIR data	IMM	Handheld	Display PIR for guard, and access decision. Continue to EvTr-017
EvTr-005	Credential is not known locally	Unknown Card (Access Denied) Message to monitoring clients	IMM	Handheld	Automatic Registration enabled.
EvTr-006		DOD Credential Number	Handheld	IMM AutoReg at Cloud server	Only when user presented DOD credential
EvTr-007		DOD Credential Number	IMM AutoReg	IMM at Cloud Server	
EvTr-008		DOD Credential Number	IMM at Site Server	Interoperability Layer Service (IoLS)	IMM determines which vetting service to use and implements the appropriate interface
EvTr-009	Receipt of response	Vetting details dependent on service used	IoLS	IMM	IoLS provides User details (Name, DOB, security alerts, and other Credentials)
EvTr-010	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Site Server	Positive result
EvTr-011		First Name, Middle Name, Last Name, DOB	IMM AutoReg	Debarment database	Automatic Registration checks local Debarment DB.
EvTr-012	IMM AutoReg requests FP	Fingerprint capture	Registrant	IMM AutoReg	PIR is assembled. Used with fingerprint enabled handheld only.
EvTr-013		PIR	IMM AutoReg	Symmetry DB	
EvTr-014		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-015		PIR data	IMM	Handheld	Display PIR for guard, and access decision
EvTr-016	Synch with Cache box	PIR	Cloud Server	Cache Box	
EvTr-017	Access Granted	Handheld	IMM	Guard	Handheld displays granted access notification and green background
EvTr-018	Guard signals user to proceed through lane	Guard Signal	Guard	User	

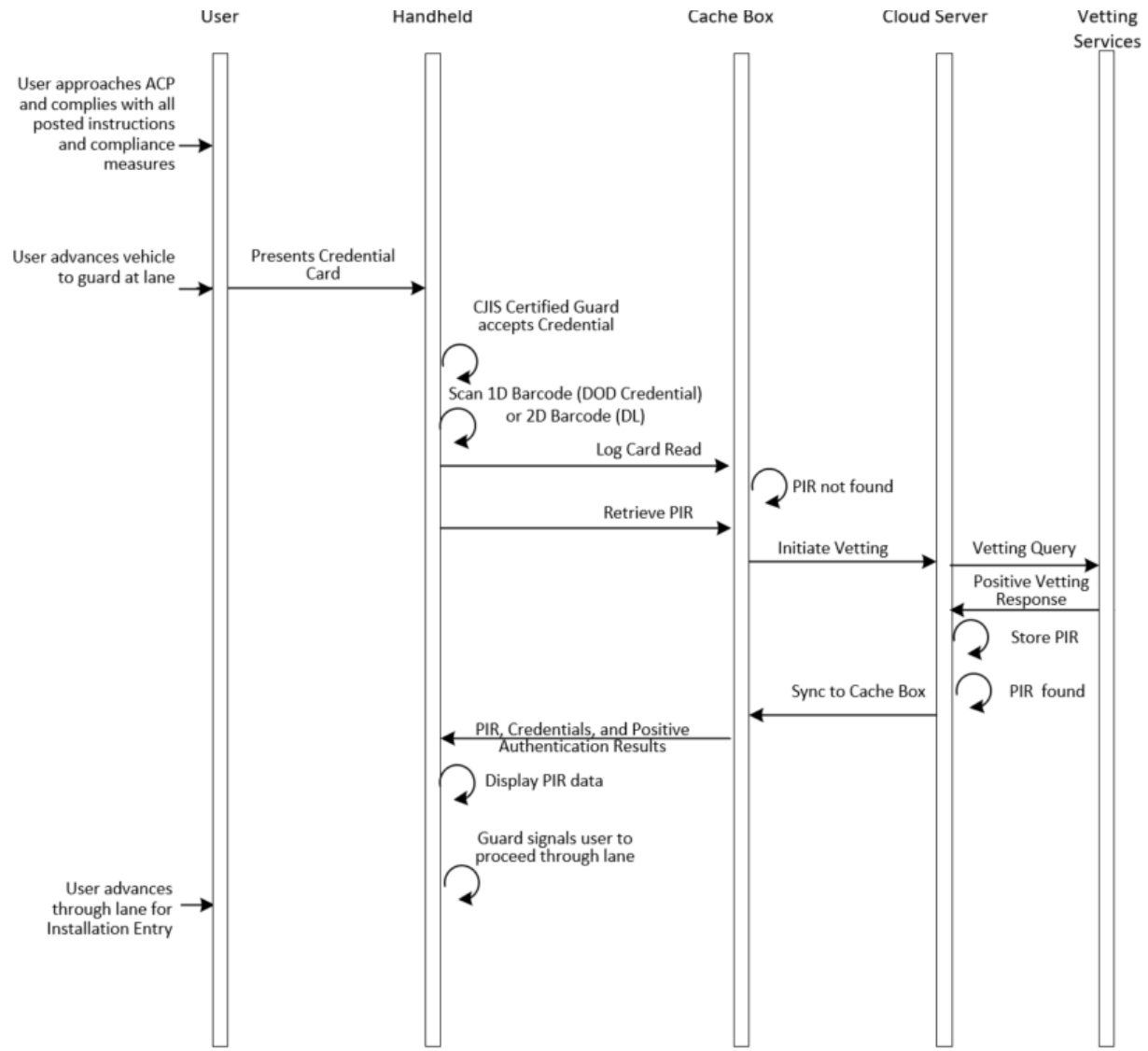

Figure 30: OV-6c, Event Trace - Handheld Operations - Tier 1 Access Granted/In Lane Registration

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-001	Vehicle approaches ACP				
EvTr-002	User presents credential to CJIS certified guard with handheld	Credential Number	Driver, Handheld	IMM (Cache Box)	IMM software manages credential workflow
EvTr-003		Credential Number	IMM	Symmetry DB	Look for existing credential in DB

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-004	Credential is known locally	PIR data	IMM	Handheld	Display PIR for guard, and access decision. Continue to EvTr-022
EvTr-005	Credential is not known locally	Unknown Card (Access Denied) Message to monitoring clients	IMM	Handheld	Automatic Registration enabled.
EvTr-006	Request for additional information through display	SSN	Driver, Handheld	IMM AutoReg at Site server	Only when user presented Driver License. Jump to EvTr-011 for DOD Credential.
EvTr-007	Receive SSN	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number. Query request command	IMM AutoReg	IMM at Site Server	
EvTr-008	Receipt of query request	First Name, Middle Name, Last Name, SSN, DOB, DL State, DL number, Passport Number as appropriate. Query request command	IMM at Cloud Server	Law Enforcement (LE) vetting service	IMM determines which vetting service to use and implements the appropriate interface
EvTr-009	Receipt of response	Vetting details dependent on service used	LE Vetting	IMM	LE Vetting provides limited Criminal Justice Information.
EvTr-010	Receipt of response	Vetting details dependent on service used	IMM at Site Server	IMM AutoReg at Cloud Server	Positive result continues to EvTr-020.
EvTr-011		DOD Credential Number	Handheld	IMM AutoReg at Cloud server	Only when user presented DOD credential
EvTr-012		DOD Credential Number	IMM AutoReg	IMM at Cloud Server	
EvTr-013		DOD Credential Number	IMM at Cloud Server	Interoperability Layer Service (IoLS)	IMM determines which vetting service to use and implements the appropriate interface
EvTr-014	Receipt of response	Vetting details dependent on service used	IoLS	IMM	IoLS provides User details (Name, DOB, security alerts, and other Credentials)
EvTr-015	Receipt of response	Vetting details dependent on service used	IMM at Cloud Server	IMM AutoReg at Cloud Server	
EvTr-016		First Name, Middle Name, Last Name, DOB	IMM AutoReg	Debarment database	Automatic Registration checks local Debarment DB.

Event ID	Initiating Event	Data Transferred	Data Source	Data Destination	Comments
EvTr-017	IMM AutoReg requests FP	Fingerprint capture	Registrant	IMM AutoReg	PIR is assembled. Used with fingerprint enabled handheld only
EvTr-018		PIR	IMM AutoReg	Symmetry DB	
EvTr-019		Credential Number	IMM	Symmetry DB	Look for existing credential in DB
EvTr-020	Synch with Cache box	PIR	Cloud Server	Cache Box	
EvTr-021		PIR data	IMM	Handheld	Display PIR for guard, and access decision
EvTr-022	Access Granted	Handheld	IMM	Guard	Handheld displays granted access notification and green background
EvTr-023	Guard signals user to proceed through lane	Guard Signal	Guard	User	

APPENDIX K

OV-7 Logical Data Model

APPENDIX K
OV-7 Logical Data Model

K.0. Background

DODAF V2.02 classifies Operational Viewpoint 7 (OV-7), Logical Data Model in the new category, Data, and Information Viewpoint 2 (DIV-2). It maintains the title of Logical Data Model.

K.1. COTS Interfaces

AIE-3/4 is comprised of Commercial off the Shelf (COTS) products that have open and published Application Programming Interfaces (APIs) that allow the sharing of data from one system to another. By utilizing these API's, the COTS component manufacturers have worked together to produce the AIE-3/4 System that will be deployed. Therefore, the Logical Data Model described here is simply the data sharing capability that allows the interface of one system to another. The internal data models of the COTS products are not available to Prime Contractor or to the Government due to their proprietary and trade secret nature.

K.1.1. IMM Client Local Vetting Gateway

The following table lists the parameters of the Identity Management Middleware interface that is exposed to the IMM-AutoReg (in-lane registration).

ICD Parameter	Description	I / O	Comment
Plugin	Defines the Authoritative Service to use for credential validation	Input	
credentialTypeCode	Type of credential submitted. See Reference 3 below for enumeration.	Input	
tokenTypeCode	Type of token submitted. See Reference 3 below for enumeration.	Input	
tokenString	The token data. See Reference 3 below	Input	
valid	0 for not valid, or 1 for valid	Output	
validSpecified	0 for "valid" not specified, or 1 for "valid" specified in response	Output	
credentialStatusCode	Additional validity data. See Reference 3 below for enumeration.	Output	

credentialStatusDate	Last update of credential status. See Reference 3 below.	Output	
credentialStatusDateSpecified	1 if credentialStatusDate has been specified, otherwise 0.	Output	
_IMM_Success	1 if the request was completed successfully, otherwise 0.	Output	
_IMM_ErrorString	If an error occurred, contains the error string, otherwise <null>	Output	
PN_SYS_ID	Person System Identifier. See Reference 3 below for detail.	Output	
PN_SYS_ID_TYP_CD	Person System Identifier Type Code. See Reference 3 below for enumeration.	Output	
PN_ID	Person Identifier. See Reference 3 below for detail.	Output	
PN_ID_TYP_CD	Person Identifier Type Code. See Reference 3 below for enumeration.	Output	
PN_LST_NM	Person Last Name. See Reference 3 below for detail.	Output	
PN_1ST_NM	Person First Name. See Reference 3 below for detail.	Output	
PN_SEX_CD	Person Gender. See Reference 3 below for enumeration.	Output	
PN_BRTH_DT	Person Birth Date. See Reference 3 below for detail.	Output	
PN_BRTH_DTSpecified	1 if the PN_BRTH_DT was specified, otherwise 0	Output	
US_CTZP_STAT_CD	Code indicating US Citizen Status. See Reference 3 below for enumeration.	Output	
PHT_IMG	Photo Image in JPG format.	Output	Generally low resolution
MA_LN1_TX	Mailing Address Line 1 text	Output	
MA_CITY_NM	Mailing Address City Name	Output	
MA_ST_CD	Mailing Address State Code. See Reference 3 below for enumeration.	Output	
MA_CTRY_CD	Mailing Address Country Code. See Reference 3 below for enumeration.	Output	
MA_PR_ZIP_CD	Mailing Address Postal Region Code (i.e., ZIP code).	Output	
MA_PR_ZIPX_CD	Mailing Address Postal Region Extended Code.	Output	
CRD_EXP_DT	Card Expiration Date.	Output	
CRD_EXP_DTSpecified	1 if the CRD_EXP_DT was specified, otherwise 0	Output	
NAC_STAT_CD	National Agency Check Status Code. See Reference 3 below for enumeration.	Output	
NAC_LST_DT	National Agency Check Last Performed Date.	Output	
NAC_LST_DTSpecified	1 if the NAC_LST_DT was specified, otherwise 0	Output	
TKN_TYP_CD	Token Type Code. See Reference 3 below for enumeration.	Output	
TKN_ID	Token Identifier data. See Reference 3 below.	Output	
TKN_END_DT	The TKN_END_DT will always be equal to CRD_EXP_DT	Output	

TKN_END_DTSpecified	1 if the TKN_END_DT was specified, otherwise 0	Output

Figure 31: Identity Management Middleware Interface Definition

K.1.2. IMM Client Interface to External Resource, IoLS

The Interoperability Layer Services (IoLS) is a cloud service offered by DMDC and provides credential and identity validation services as well as continuous information management engine (CIME) for identity related security alerts. The IoLS interface is defined by DMDC and is documented as indicated in the reference section below.

K.1.3. IMM Client Interface to External Resource, LE Vetting Service

The Law Enforcement (LE) Vetting Service is a cloud service offered by Iberon, LLC. The interface is described in the document as indicated in the reference section below. The vetting service is exposed as a web service. The inputs and outputs are described in the following table:

ICD Parameter	Description	I / O	Comment
First Name	First Name	Input	Required
Middle Name	Middle Name	Input	Optional
Last Name	Last Name	Input	Required
SSN	Social Security Number	Input	Optional (if DL provided)
DOB	Date of Birth	Input	Required
DL Number	Driver's License or ID Card number	Input	Optional (if SSN provided)
DL State	State that issued ID/DL	Input	Required with DL Number
Vetting Result	Result of the Person Adjudication	Output	Pass Fail Inconclusive Error
Identity Verification Result	Result of the Identity verification component	Output	Pass Fail Inconclusive DMV Error DMV Down
Proofing Alerts	A component of the Identity Verification Result, includes detail on issues with either the credential data (DL) or the SSN/ID data	Output	

Credential	Alert details related to credential	Output	Active Expired Flagged Inactive Revoked Suspended Unknown Unlicensed
SSN	Alert details related to Identity	Output	No response No SSN response No SSN provided SSN mismatch

Figure 32: NCITE Vetting Service Interface Definition

K.1.4. Symmetry Interfaces

The Symmetry Security Management System by AMAG Technology acts as the management resource for personal information record (PIR) data. There are two interfaces defined by AMAG Technology that are used in the AIE-3/4 System. The Data Connect interface is used to store PIR data in the database after a successful registration and during the PIR synchronization process, and to retrieve PIR data for operational use. The XML Open Integration Module is not presently used in AIE-3/4.

The following figure lists the fields stored by Symmetry, and the data type. Where there is no definition for the field in the AIE-3/4 Permanent Party (U.S. DoD ID Card Holders) or Visitor data record, this represents a field that can be used in the future for expanded functionality.

The fingerprint data is stored in a different table in the Symmetry database. The fingerprint template data is stored in a format defined by the ANSI/INCITS 378 standard.

Symmetry Generic Field Name	Permanent Party Definition	Visitor Definition	Data Type	Comments
LastName	LastName	LastName	nvarchar(40)	
FirstName	FirstName	FirstName	nvarchar(40)	
CardNumber	CredentialID	CredentialID	integer	
CredentialIssueLevel	Not used	Not used	tinyint	Valid Range 0 to 7
CredentialNumber	FacilityID	FacilityID	integer	
SystemCode			smallint	Valid Range 0 to 9999 (not for SR cards)
AgencyCode	9999	9999	smallint	Valid Range 1 to 9999 (not for SR cards)
PIN	PIN	PIN	nvarchar(10)	A PIN can have up to 8 digits (e.g., 0001-9999 for a 4-digit PIN), as set in the Maintenance/User & Preferences/ System Preferences screen). See page 7.
PersonalData1	Cadency	Cadency	nvarchar(40)	
PersonalData2	Email address	Email address	nvarchar(40)	
PersonalData3	Drivers' License Issuing State	Drivers' License Issuing State	nvarchar(40)	
PersonalData4	Drivers' License Number	Drivers' License Number	nvarchar(40)	
PersonalData5	Drivers' License Expiration Date	Drivers' License Expiration Date	nvarchar(40)	
PersonalData6	Passport Issuing Country	Passport Issuing Country	nvarchar(40)	
PersonalData7	Passport Number	Passport Number	nvarchar(40)	
PersonalData8	Passport Expiration	Passport Expiration	nvarchar(40)	
PersonalData9	Non-truncated EDI/PI		nvarchar(40)	PN_SYS_ID in IoLS, can include other ID types
PersonalData10	NLETS PASS/FAIL + Timestamp	NLETS PASS/FAIL + Timestamp	nvarchar(40)	
ActiveDate	RegistrationDate	RegistrationDate	datetime	
ExpiryDate	ExpiresDate	ExpiresDate	datetime	

Symmetry Generic Field Name	Permanent Party Definition	Visitor Definition	Data Type	Comments
InactiveComment	InactiveComment	InactiveComment	nvarchar(40)	Reason for Making inactive
FaceFile	UserPhoto	UserPhoto	nvarchar(128)	Points to record in FaceTable
SignatureFile	UserSignature	UserSignature	nvarchar(128)	Points to record in SignatureTable
MiddleName	MiddleName	MiddleName	nvarchar(40)	Middle initial or middle name
BadgeFormatID	BadgeFormat	BadgeFormat	integer	
PersonalData11	IoLS PASS/FAIL + Timestamp	IoLS PASS/FAIL + Timestamp	nvarchar(40)	
PersonalData12	Debarment List PASS/FAIL + Timestamp	Debarment List PASS/FAIL + Timestamp	nvarchar(40)	
PersonalData13	Street Address	Street Address	nvarchar(40)	
PersonalData14	City	City	nvarchar(40)	
PersonalData15	State	State	nvarchar(40)	
PersonalData16	ZIP	ZIP	nvarchar(40)	
PersonalData17	Mobile Operator Flag		nvarchar(40)	
PersonalData18	Mobile Op CJIS Training Exp		nvarchar(40)	
PersonalData19		Local token category code	nvarchar(40)	“8” for visitor
PersonalData20	1-D Barcode Data for printing	1-D Barcode Data for printing	nvarchar(40)	TKN_ID in IoLS.
PersonalData21	Vehicle #1 License Plate State	Vehicle #1 License Plate State	nvarchar(40)	
PersonalData22	Vehicle #1 License Plate Num	Vehicle #1 License Plate Num	nvarchar(40)	
PersonalData23	Vehicle #2 License Plate State	Vehicle #2 License Plate State	nvarchar(40)	
PersonalData24	Vehicle #2 License Plate Num	Vehicle #2 License Plate Num	nvarchar(40)	
PersonalData25	Vehicle #3 License Plate State	Vehicle #3 License Plate State	nvarchar(40)	
PersonalData26	Vehicle #3 License Plate Num	Vehicle #3 License Plate Num	nvarchar(40)	

Symmetry Generic Field Name	Permanent Party Definition	Visitor Definition	Data Type	Comments
PersonalData27	Security Alert Summary	Security Alert Summary	nvarchar(40)	
PersonalData28		Guest Escort Name	nvarchar(40)	
PersonalData29		Reason for Visit	nvarchar(40)	
PersonalData30	Original Token Exp Date	Original Token Exp Date	nvarchar(40)	
PersonalData31	Trusted traveler	Trusted traveler	nvarchar(40)	
PersonalData32	DL Issue Date	DL Issue Date	nvarchar(40)	
PersonalData33	ACP Distribution Mask	ACP Distribution Mask	nvarchar(40)	
PersonalData34	CJIS Login	CJIS Login	nvarchar(40)	
PersonalData35	Gold Star	Gold Star	nvarchar(40)	
PersonalData36	Home Phone #	Home Phone #	nvarchar(40)	
PersonalData37	Record Origin	Record Origin	nvarchar(40)	
PersonalData38	Reg Info	Reg Info	nvarchar(40)	
PersonalData39	Trusted Traveler (no)	Trusted Traveler (no)	nvarchar(40)	
PersonalData40	Rank Code		nvarchar(40)	
PersonalData41	Personnel Category Code		nvarchar(40)	
PersonalData42	Date Of Birth	Date Of Birth	nvarchar(40)	
PersonalData43	Service Code / Branch Code (DoD)	Service Code / Branch Code (DoD)	nvarchar(40)	
PersonalData44	System ID type code (L=LPEDIPI, D=EDIPI, A=ARN)	System ID type code (L=LPEDIPI, D=EDIPI, A=ARN)	nvarchar(40)	Defines ID used in PDF #9
PersonalData45	Not Used	Not Used	nvarchar(40)	
PersonalData46	PN_SEX_CD	Gender Code	nvarchar(40)	M/F/Other
PersonalData47	CRD_RVK_CD	Revocation Code	nvarchar(40)	
PersonalData48	Not Used	Not Used	nvarchar(40)	
PersonalData49	PN_ID	SSN	nvarchar(40)	
PersonalData50	PN_ID_TYP_CD	Person Identifier Type Code	nvarchar(40)	
CardFormat			tinyint	0=Legacy; 1=CAC;

Symmetry Generic Field Name	Permanent Party Definition	Visitor Definition	Data Type	Comments
PersonIdentifier	PersonIdentifier		integer	PIV cards only
OrganisationCategory	OrganisationCategory		smallint	PIV cards only (mandatory). Range 0-9.
OrganisationIdentifier	OrganisationIdentifier		smallint	PIV cards only (mandatory). Range 0-9999.
OrganisationAssociation	OrganisationAssociation		smallint	PIV cards only (mandatory). Range 0-9.
CredentialSeriesCode	CredentialSeriesCode		smallint	PIV cards only (mandatory). Range 0-9.
EmployeeReference			nvarchar(128)	
CompanyID			integer	

Figure 33: Symmetry PIR Data Record

K.1.5. Removed

K.2. OPMG Dashboard Database

AIE-3/4 provides a centralized SQL database that collects summary data from local Installation's Symmetry and uses this data to produce a variety of reports referred to as the OPMG Dashboard Reports. The following diagram depicts the logical associations of this data.

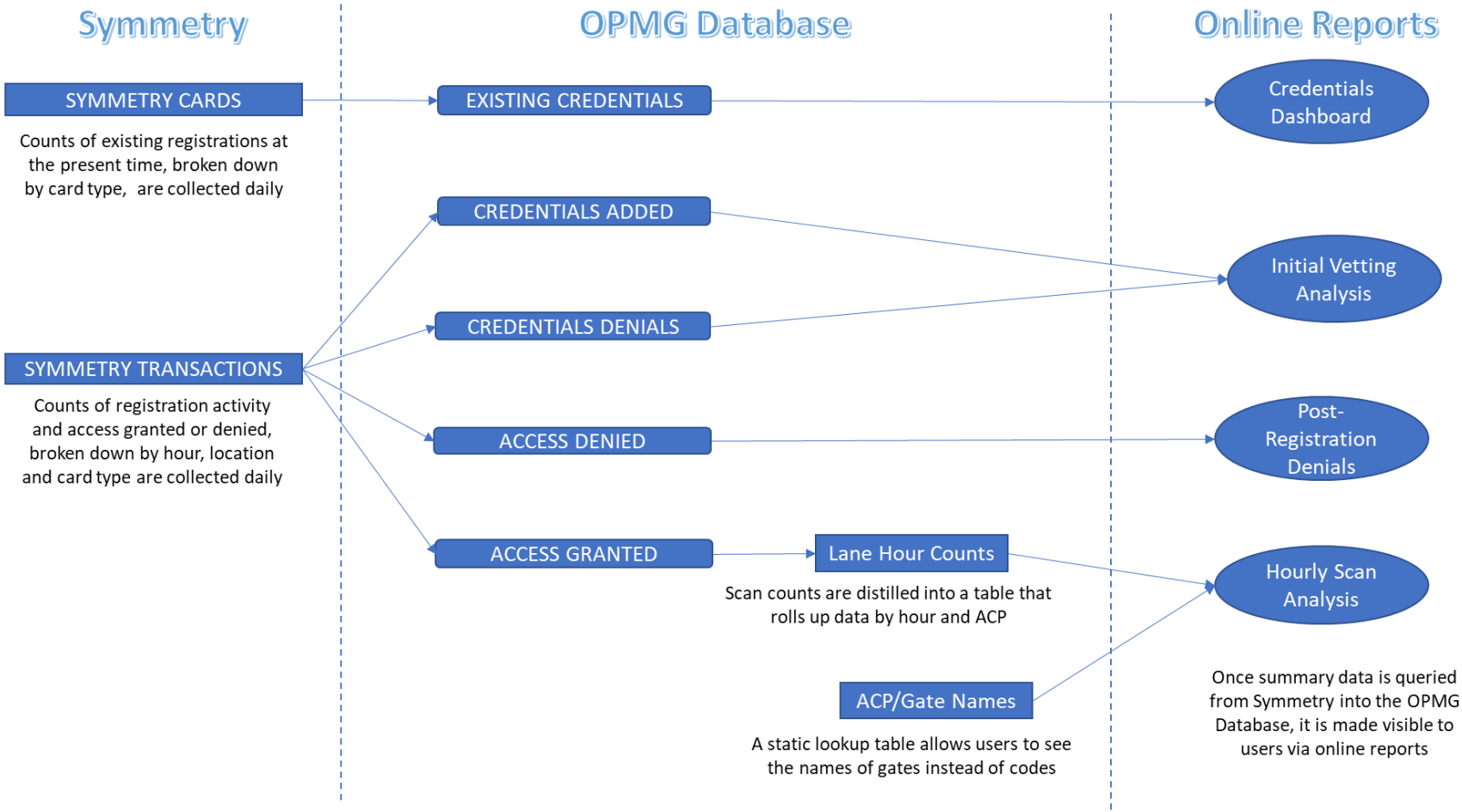

Figure 34: AIE-3/4 OPMG Dashboard Reports Logical Data Model

K.3 References

1. *Symmetry Homeland Security Edition Data Connect Manual 9.3.0v1 (9600-0459) G4S TECHNOLOGY, 13 February 2020*

2. *Symmetry XML Open Integration Module User Guide 9.3.0v1 (9600-0469) G4S TECHNOLOGY, 13 February 2020*

3. *Interoperability Layer Services Software Development Guide v2.1.1, Defense Manpower Data Center, February 2015*

4. *Identity Matching Engine for Security and Analysis (IMESA) Interface Control Document (ICD) 1.3 v, February 2020.*

5. *Iberon NCITE Vetting Service Interface Control Document*

APPENDIX L

SV-1 Systems Interface Description

APPENDIX L

SV-1 Systems Interface Description

This System Interface Description (SV-1) depicts the system nodes and systems that support the AIE-3/4 operations. The diagram lays out the AIE-3/4 areas of operation, servers, other installation access assets and systems which connect to the AIE-3/4 servers, external entities, and the systems which AIE-3/4 interfaces with to receive or transmit information.

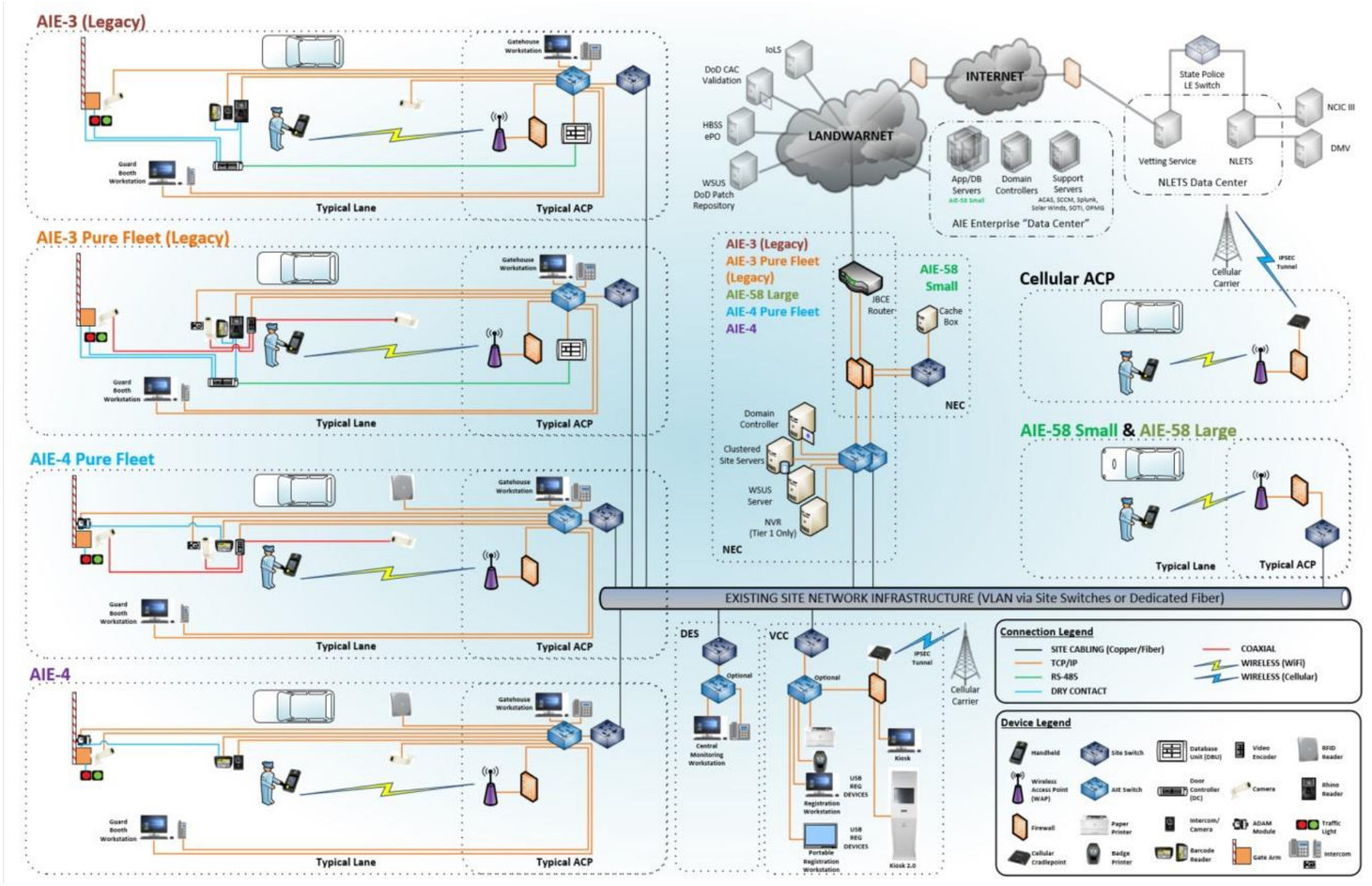

Figure 35: SV-1, AIE-3/4 & Pure Fleet Configurations with RFID

APPENDIX M

SV-2 Systems Resource Flow Description

APPENDIX M

SV-2 Systems Resource Flow Description

This System Resource Flow Description (SV-2) depicts the AIE-3/4 communications between systems and components. The accompanying diagrams depict multiple views to individually identify the flow of resources by the specific configuration. They also include external entities and systems with which AIE-3/4 receives or transmits information between them.

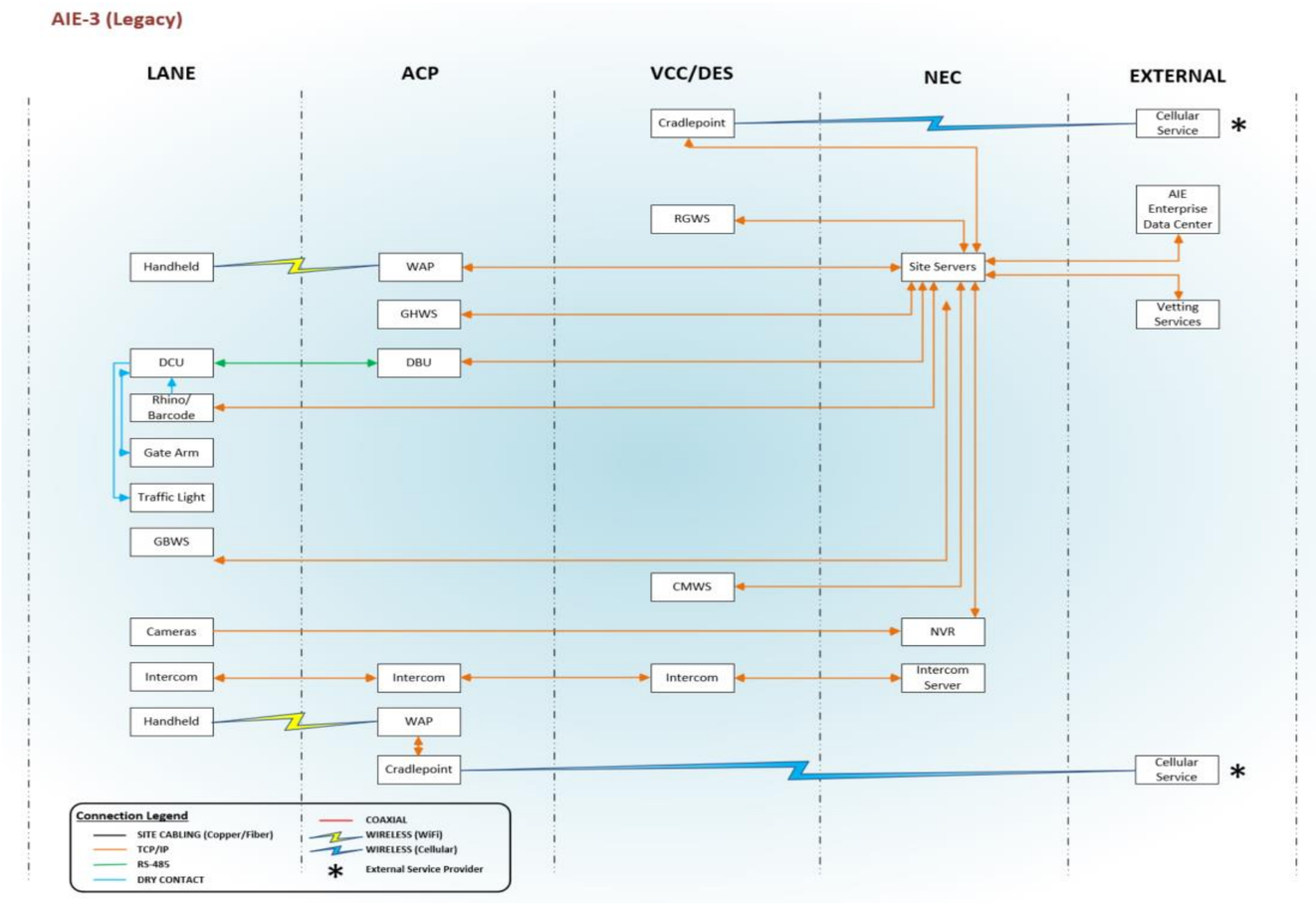

Figure 36: SV-2a, AIE-3 System Resource Flow

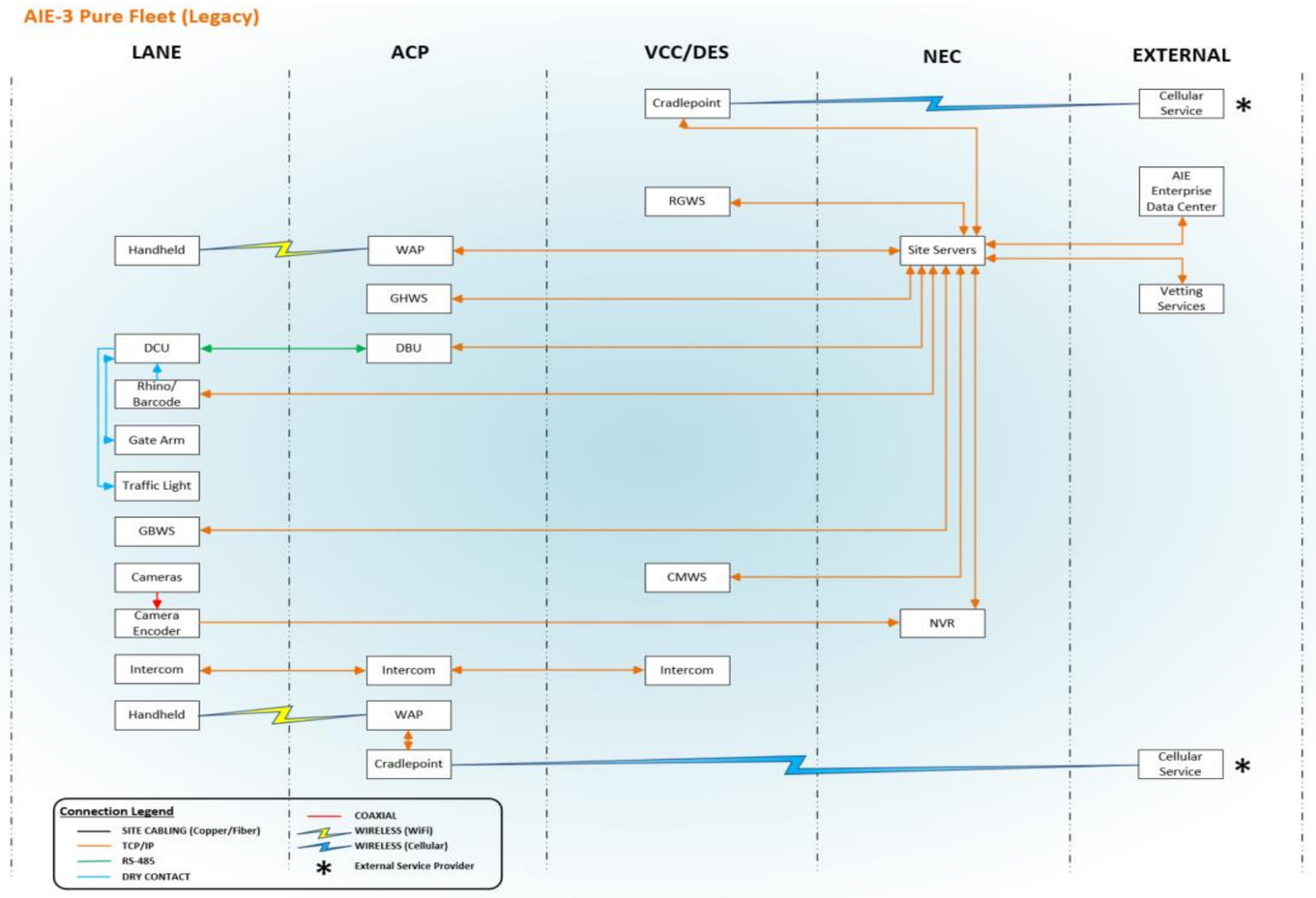

Figure 37: SV-2b, AIE-3 Pure Fleet System Resource Flow

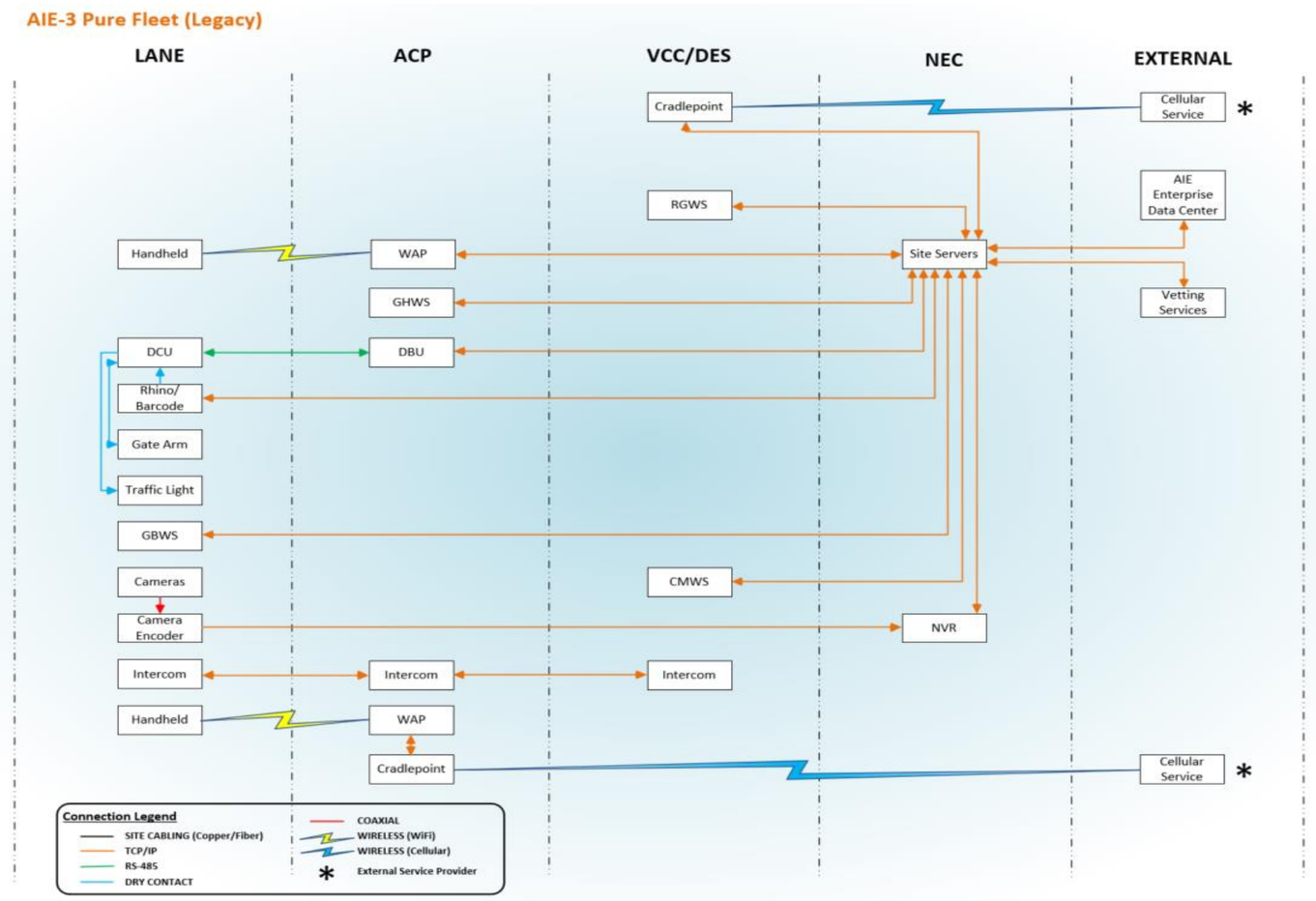

Figure 38: SV-2c, AIE-4 Pure Fleet System Resource Flow

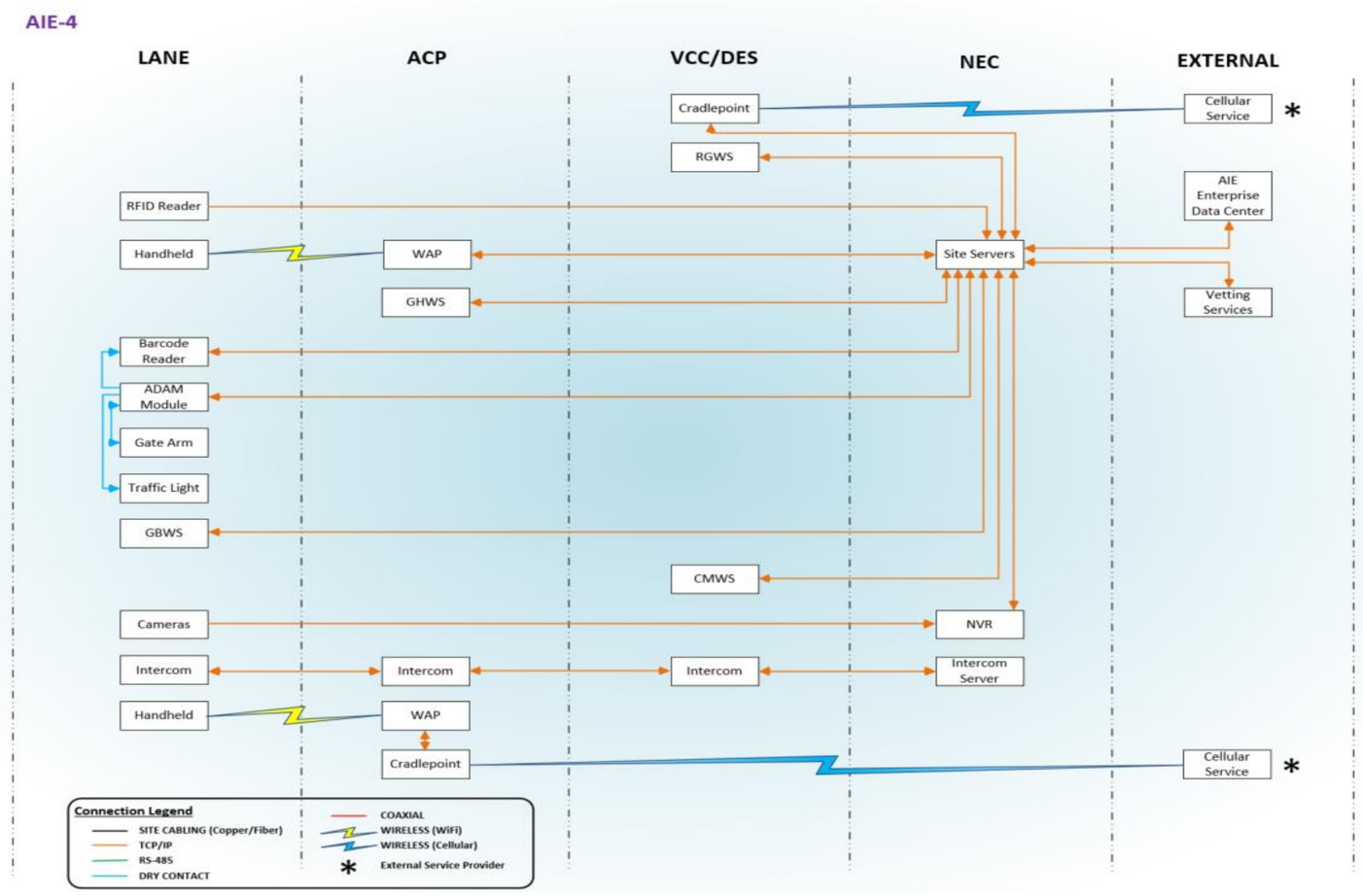

Figure 39: SV-2d, AIE-4 Pure Fleet System Resource Flow

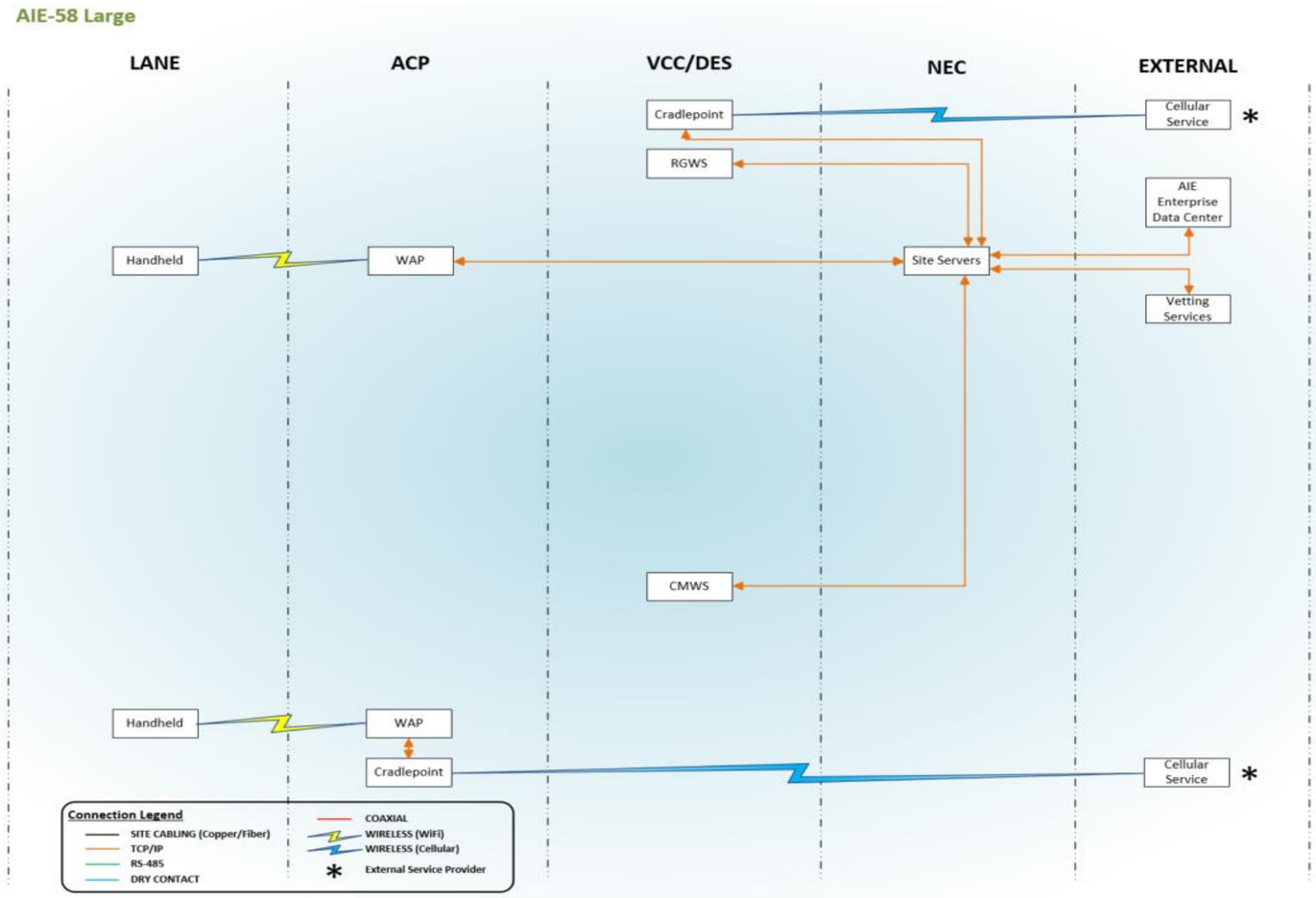

Figure 40: SV-2e, AIE-58 Large System Resource Flow

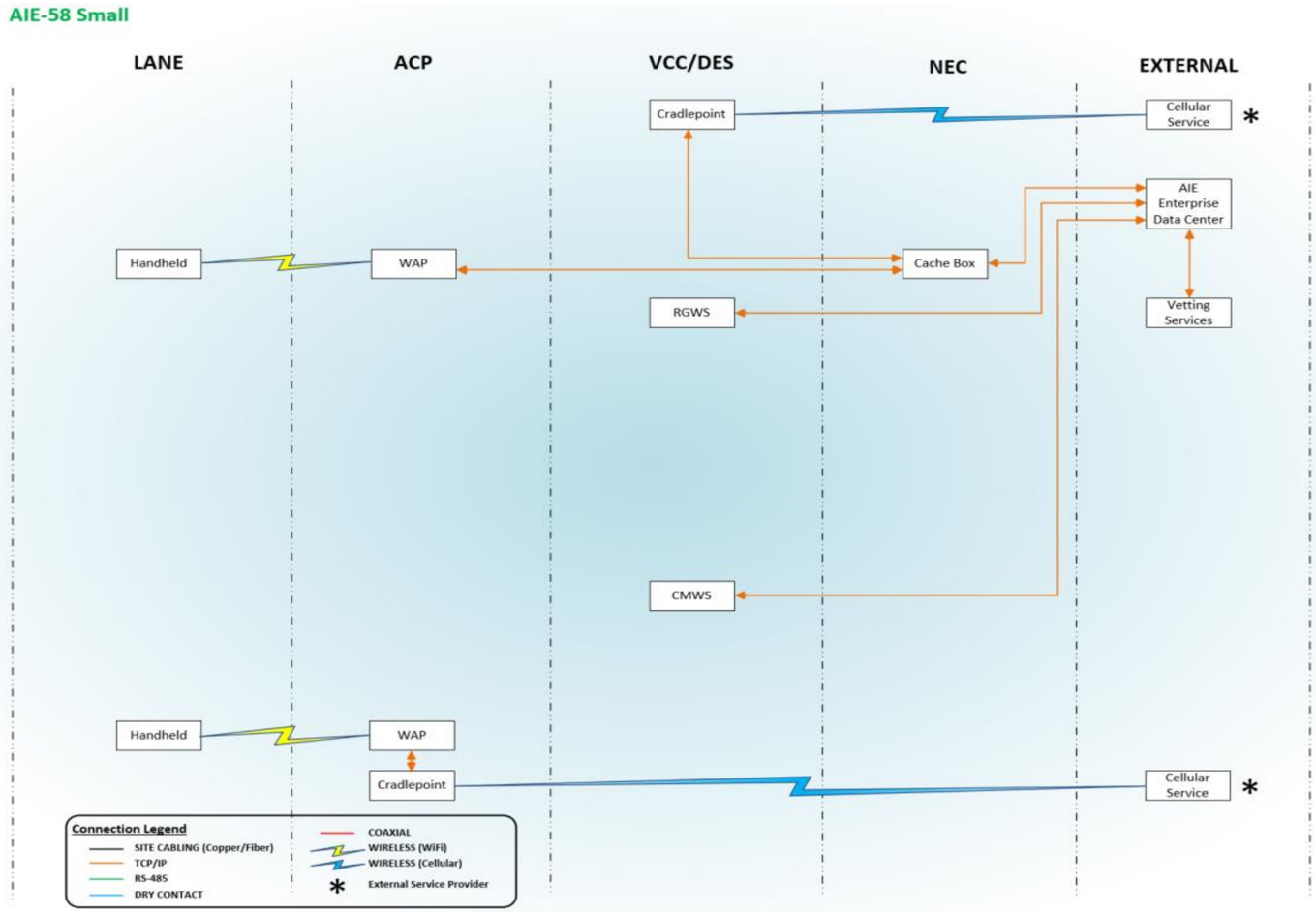

Figure 41: SV-2f, AIE-58 Small System Resource Flow

APPENDIX N

SV-3 Systems-Systems Matrix

APPENDIX N

SV-3 Systems-Systems Matrix

The SV-3 Systems-Systems Matrix is a summary of the systems and resources indicated in SV-1. SV-3 shows the interaction of these different systems and the types of data that are exchanged among different systems.

	EXTERNAL		NEC					VCC/DES/ACP			ACP/LANE				LANE						
From ------> To	*Vetting Services*	*AIE Enterprise Data Center*	*Site Servers*	*Domain Controllers*	*Cache Box*	***NVR (Tier 1 only)***	***Intercom Server (AIE-3, AIE-4)***	***RGWS, Portable RGWS***	***CMWS***	***Cradlepoint (Hub & Spoke)***	***WAP***	***Handheld***	***DBU***	***GHWS, GBWS***	***Intercom (All Locations)***	***Camera (AIE-3, AIE-4) & Camera Encoder (Pure Fleet)***	***DCU***	***Rhino/Barcode Reader***	***Gate Arm***	***Traffic Light***	***ADAM Module***	***Qscan***
Vetting Services		Vetting Response	Vetting Reponse																		
AIE Enterprise Data Center	Vetting Request		Login Response Support Services	Domain Fallover Support Services	Login Response PIR Response Support Services	Login Response Support Services		Login Response Support Services	Login Response Reporting Response Support Services					Login Response Support Services								
Site Servers	Vetting Request	Login Request		Login Request		Retrieve Video		PIR Response	Reporting Response	PIR Transit	PIR Transit	PIR Response	PIR Sync	PIR Response Client Service Reponses				Access Reponse				Access Reponse
Domain Controllers		Domain Fallover	Login Response			Login Response		Login Response	Login Response					Login Response								
Cache Box		Login Request PIR Request								PIR Transit	PIR Transit	PIR Response										
NVR (Tier 1 only)			Stored Video	Login Request					Video Stream Stored Video Response					Video Stream								
Intercom Server (AIE-3, AIE-4)															Call Management							
RGWS, Portable RGWS		Login Request PIR Request	PIR Request	Login Request																		
CMWS		Reporting Request	Reporting Request	Login Request	Reporting Request	Video Stream Stored Video Request																
Cradlepoint (Hub & Spoke)			PIR Transit		PIR Transit					PIR Transit	PIR Transit	PIR Transit										
WAP					PIR Transit					PIR Transit		PIR Transit										
Handheld			PIR Request		PIR Request					PIR Transit	PIR Transit											
DBU			PIR Sync														Send Commands	Access Reponse				
GHWS, GBWS		Login Request	Client Service Requests	Login Request		Video Stream																
Intercom (All Locations)							Call Management								Call Requests Call Responses							
Camera (AIE-3, AIE-4)						Send Video Stream																
Camera Encoder (Pure Fleet)						Send Video Stream																
DCU													Receive Commands					Command Transit	Send Commands	Send Commands		
Rhino/Barcode Reader			PIR Request										Access Request				Command Transit					
Gate Arm																	Receive Commands			Send Commands	Receive Commands	
Traffic Light																	Receive Commands		Receive Commands		Receive Commands	
ADAM Module																			Send Commands	Send Commands		Send Commands
Qscan			PIR Request Access Request																		Receive Commands	

Figure 42: SV-3, System-System Matrix

APPENDIX O

SV-4 Systems Functionality Description

APPENDIX O
SV-4 System Functionality Description

O.1 Overview

This System Functionality Description (SV-4) lays out the AIE-3/4 System, sub-systems and functions which perform the activities deemed critical to support the AIE-3/4 mission. The diagram provides a decomposition of the AIE-3/4 systems into their sub-systems. Resource flow is shown through connections and where published APIs are utilized. This decomposition provides insight into the functionality that each of the systems and sub-systems provide to make up the capabilities of AIE-3/4.

SV-4a in Appendix P describes the system functions depicted in SV-4.

SV-4b in Appendix Q describes the services indicated in SV-4 and SV-4a.

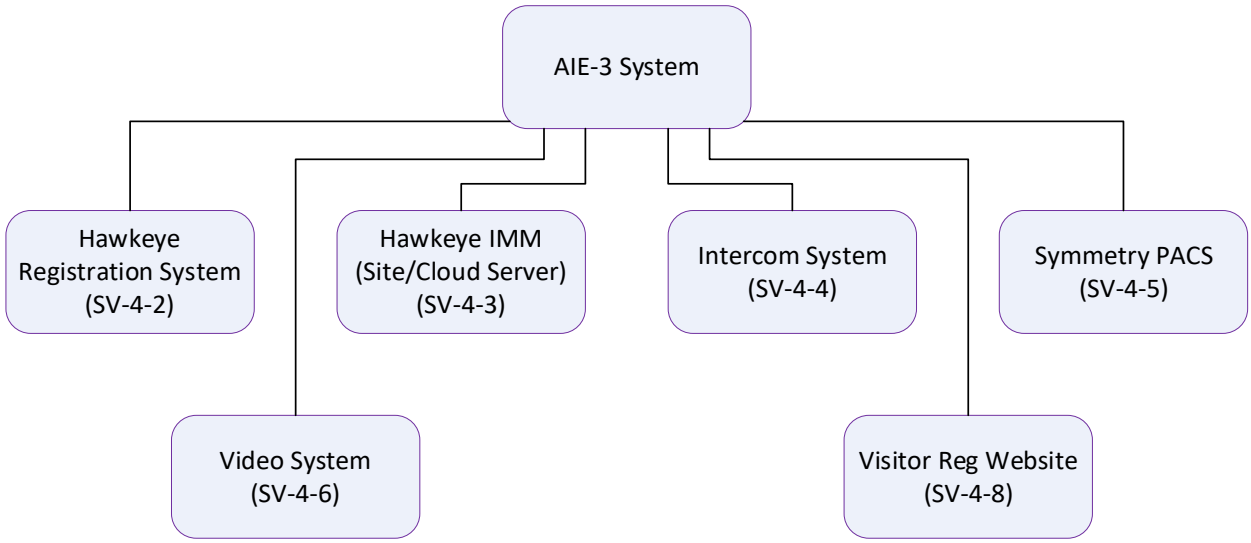

Figure 43: SV-4-1, AIE-3/4 Major System Decomposition

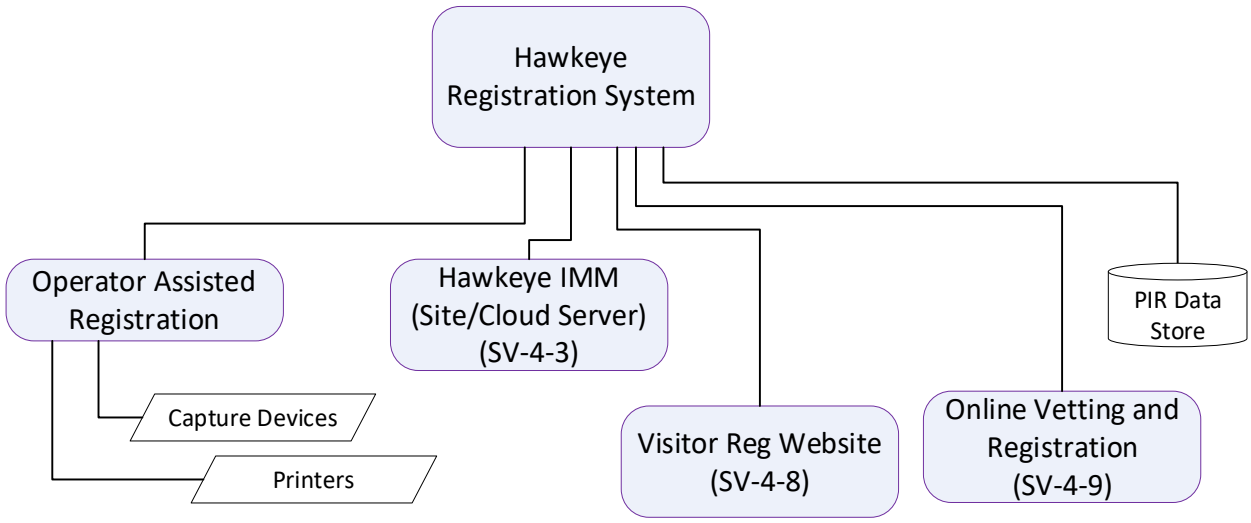

Figure 44: SV-4-2, Registration System Decomposition

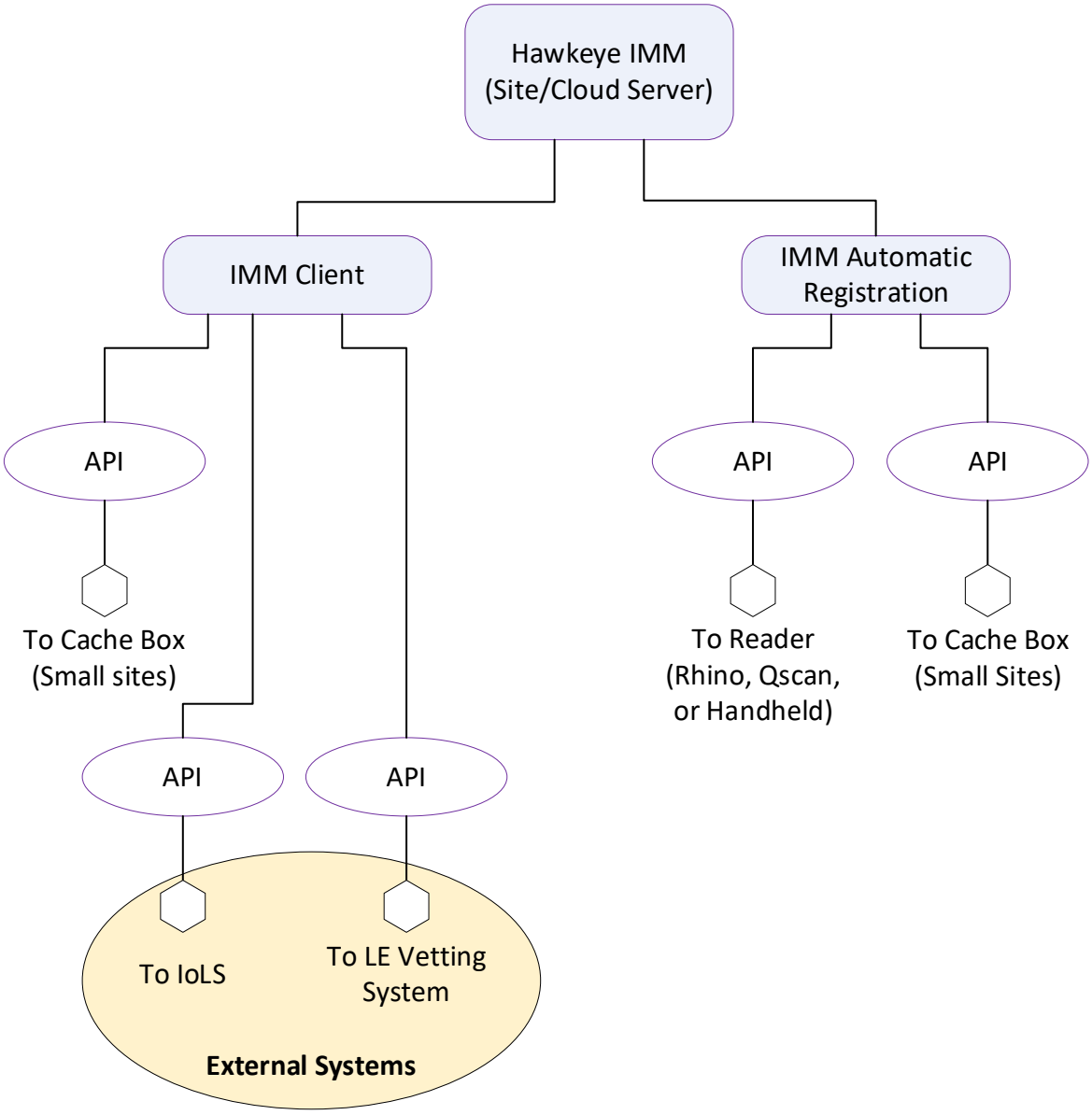

Figure 45: SV-4-3, IMM Interface System Decomposition

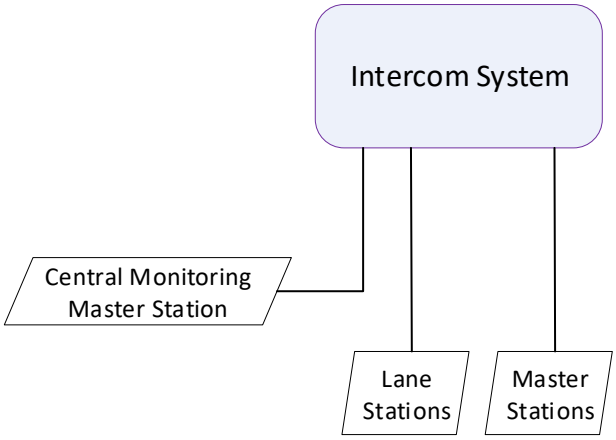

Figure 46: SV-4-4, Intercom System Decomposition

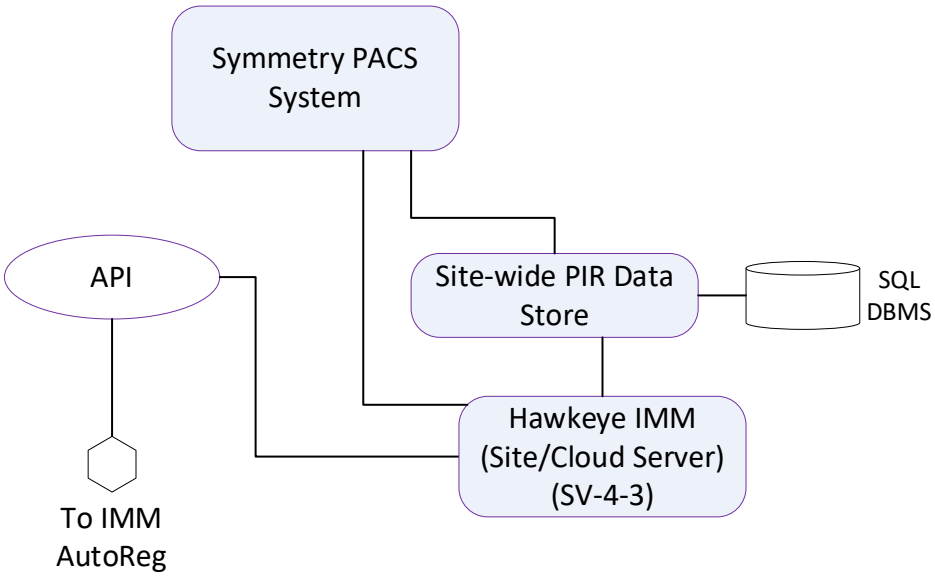

Figure 47: SV-4-5, Symmetry PACS Decomposition

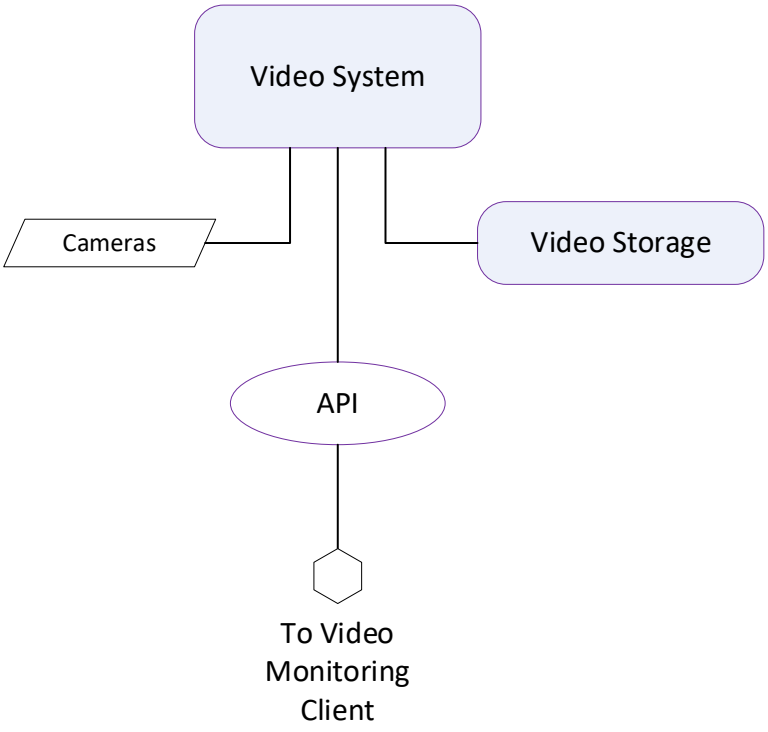

Figure 48: SV-4-6, Video System Decomposition

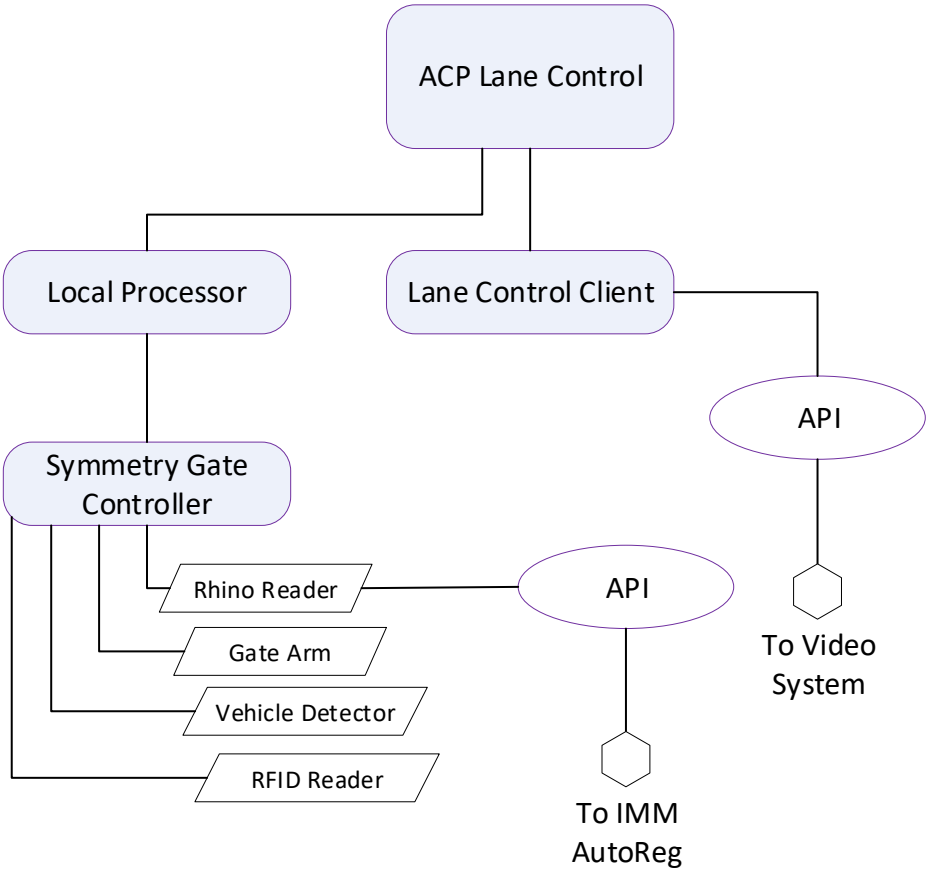

Figure 49: SV-4-7, ACP Lane Control Decomposition

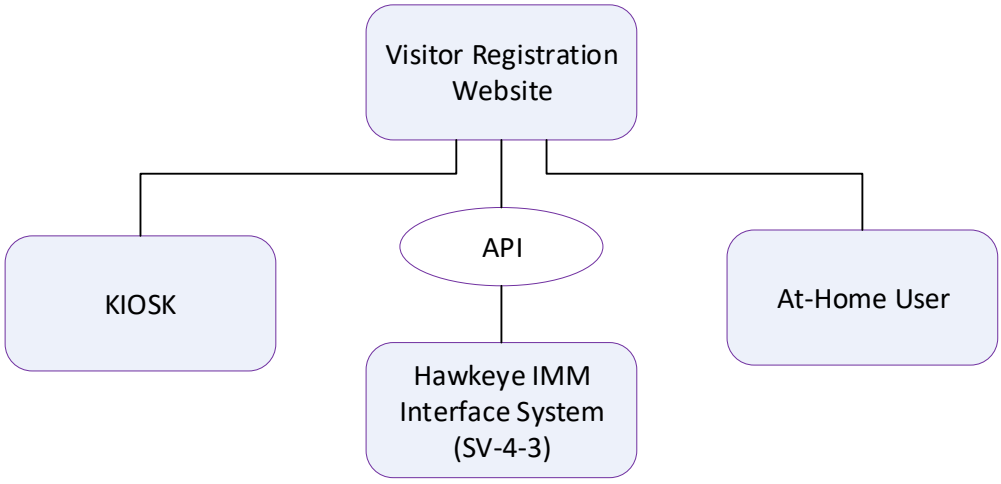

Figure 50: SV-4-8, Visitor Registration Website Decomposition

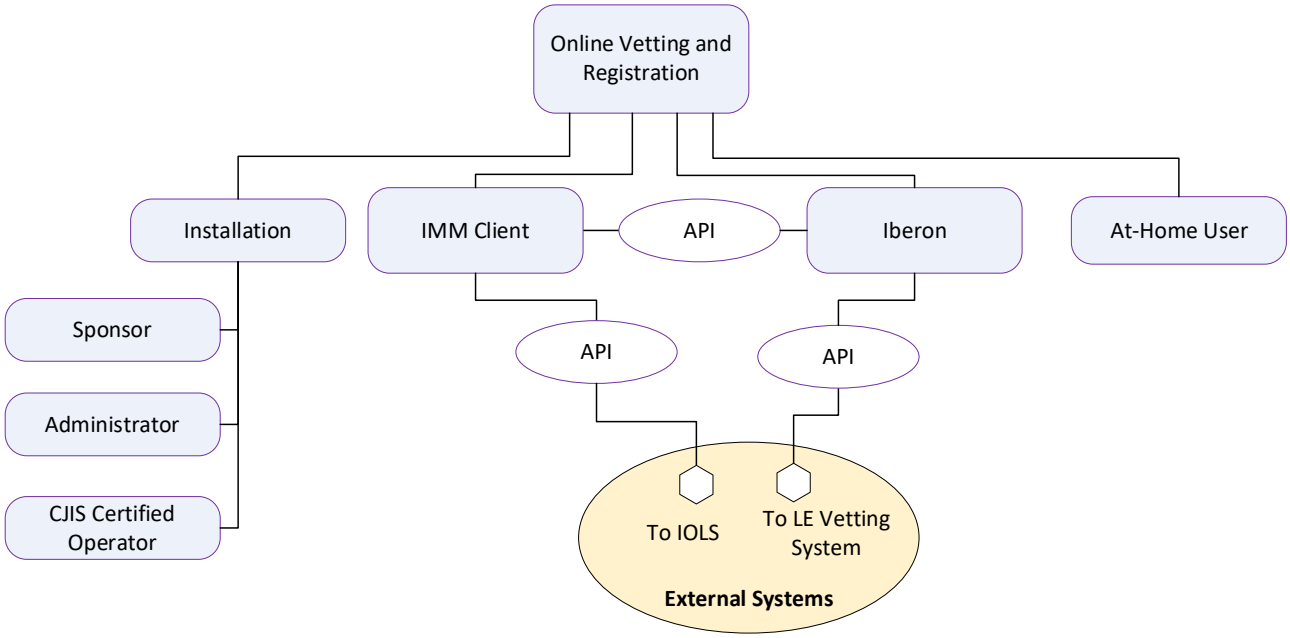

Figure 51: SV-4-9, Online Vetting and Registration

APPENDIX P

SV-4a Systems Functionality Description

APPENDIX P
SV-4a Systems Functionality Description

P.1 Overview

P.2 AIE-3/4 System Functionality Description

P.2.1 Registration

The Registration System (SV-4-2, Figure 38) decomposes into the Operator-Assisted Registration, the Web-based Pre-registration to include Online Vetting and Registration, storage of PIR data, and management and control of the Local Barred List. These High Level Functions are further decomposed as follows.

P.2.1.1 Operator Assisted Registration

P.2.1.1.1 Capture PIR data from applicant

The Registrar (actor) and applicant (actor) work cooperatively to electronically capture the following information:

- Photo of applicant;
- I-9 Breeder document credentials for Identity Validation and Vetting;
- Digitized signature showing acceptance of facility use agreement, liability waiver, or other locally determined information;
- Fingerprint biometric;
- Biographic data;
- User-selected PIN.

P.2.1.1.2 Submit PIR data for Validation and Vetting

The Hawkeye Registration software submits the collected PIR data for validation and vetting. If security alerts are indicated in the vetting response, an indication of such alerts is noted to the Registrar. The security alerts are adjudicated and action taken.

The credential validation response includes PII data previously associated with the submitted credential. If the information doesn't match with in-person captured data, discrepancies are to be adjudicated.

P.2.1.1.3 Print local badge

The Registrar has the ability to print an Installation badge. Options exist to print to a plastic card printer for extended use applications, or to a paper badge printer for one-day or other short term use.

P.2.1.1.4 Submit PIR data

Once the process is complete and the information is deemed appropriate for use in AIE, the record is imported into the Symmetry Physical Access Control System (PACS).

P.2.1.2 Web-based Pre-Registration

The original Web-based Pre-Registration was implemented at the AIE-3/4 System Enterprise Data Center. The registration function supports self-service input of credential and biographic information for visitors, and can be accessed at home or at the VCC through a kiosk. The system responds to the visitor with an email informing them of the status of their pass request. If no negative vetting is received, the garrison has the option of having the pass print at home and the visitor go directly to the ACP. Based on Army poilicy and Installation commander's intent, the visitor's DL or ID can be used as a credential.

If negative vetting is received, the visitor must go to the VCC if they wish to proceed with further adjudication or redress.

Online Vetting and Registration is an enhanced cloud based capability that provides visitor online vetting using NLETS, and if vetting is successful, registration into the AIE database for continuous vetting and visitor pass.

P.2.1.3 Manage and Control Installation Barred Person List

The Hawkeye Registration System supports a function to manage (add, modify, and delete) names on a locally maintained list. The registration system utilizes features of the Symmetry Database to maintain this list, so the information is automatically available to the in-lane automatic registration function and the Symmetry PACS once PIR records are synchronized.

P.2.1.4 PIR Data Store

The Hawkeye Registration System captures data (See P.2.1.1.1) and stores this as a Personal Information Record (PIR) in the Symmetry database at the Site-wide PIR data store. The PIR is also synchronized to the Cache Box data stores.

P.2.2 IMM Interface System

The Identity Management Middleware (IMM) Interface System (SV-4-3, Figure 29) decomposes into the IMM Client and IMM Automatic Registration functions.

P.2.2.1 IMM Client

The IMM Client acts as a gateway for various local systems to receive identity vetting and validation from local and external systems. These functions include Barred List Vetting, IoLS Credential Validation and Identity Vetting, Law Enforcement (LE) Vetting, and audit and alarm management.

P.2.2.1.1 Barred List Vetting

The IMM Client utilizes the Symmetry PIR database to store barred person's information in the SQL database. Barred Person List checking is performed on an as-needed basis during Automatic Registration in-lane and during credential authorization at time of access.

P.2.2.1.2 IoLS Credential Validation and Identity Vetting

The IMM Client utilizes the published IoLS ICD to submit credential validation requests to the external IoLS for DoD issued identity documents. The response from IoLS includes validation status as well as any security alerts against the credential owner.

P.2.2.1.3 LE Vetting

The IMM Client utilizes an API to access the external LE vetting service and submit requests for identity vetting utilizing driver's license information. The external LE Vetting service accesses NCIC III, DMV, and local and out-of-state LE information systems. The response includes information on the fitness for access to the Installation.

P.2.2.1.4 Audit an Alarm Management

The IMM Client logs all transaction activity, imports alarm notifications to the Site/Cloud Server data store and ACP local processor for presentation to security personnel.

P.2.2.1.5 Periodic Revetting

IMM Client utilizes the API connections to authoritative services to periodically update the vetting status of the local population. The IoLS ICD includes a service that provides updates to a tracked local population. The LE Vetting service is used to revet individuals upon pass renewal, in accordane with local CONOPS and State regulations.

P.2.2.2 IMM Automatic Registration

The IMM Automatic Registration (AutoReg) is an ACP function that controls the Lane Reader to identify that a presented credential does not exist in the Installation PIR database.

P.2.2.1.1 Determine credential type

IMM AutoReg controls the Lane Reader and retrieves the credential information when presented to the Lane Reader by the user requesting access. IMM AutoReg determines the credential type through several unique characteristics of the different credentials supported in the system. This process is documented in the reference, "How to read and interpret cards in AIE-3 - Rev F" by AMAG Technology, April 2013. Once credential type is determined, the credential data is decoded and parsed to determine the credential identifier.

P.2.2.1.2 Credential exists locally

The credential identifier (determined in Section P.2.2.1.1) is used to look up in the ACP local processor for an existing user for Tier 1 sites using the Rhino Reader. If one exists, the reader sends the credential identifier by Wiegand to the Symmetry Gate Controller.

P.2.2.1.3 Request vetting/validation

If the credential does not exist locally (from Section P.2.2.1.2) IMM AutoReg routes the credential information to the appropriate Authoritative Source depending on the credential type. Federal Government and DoD issued credentials are validated through IoLS. Driver's Licenses are validated through the LE Vetting Service. Validation and Vetting responses determine if user is fit for access to the base. If the user is fit for access the process continues, but if not the Automatic Registration process halts, the record is imported into the ACP local processor for Tier 1 sites using the Rhinio reader with the appropriate information and a an "Invalid" flag so that when the reader indicates the access request the Guard is notified of the Invalid access attempt.

P.2.2.1.4 Capture fingerprint data

If vetting response indicates fitness for access (from Section P.2.2.1.3), the process continues. IMM AutoReg collects fingerprint templates through the Lane Reader.

P.2.2.1.5 Store PIR record

The fingerprint templates, user biographic information (collected from credential and/or validation response), and credential information are stored as PIR in the Installation-wide Data Store. The Lane Reader sends the credential data to the Lane Controller and the PIR is presented to the Guard.

P.2.2.1.6 Respond to User

IMM AutoReg controls the Lane Reader display as well as the card reader and fingerprint scanner. IMM AutoReg displays information to the user to provide direction and feedback.

P.2.3 Intercom System

The Intercom System (SV-4-4, Figure 30) decomposes into the Installation-wide Intercom and ACP Intercom functions.

P.2.3.1 Installation Wide Intercom Services

In order to meet the system availability requirements, each ACP acts as a separate intercom system. A separate intercom server at the Site Server location provides dynamic routing of calls from one intercom server to another as well as to Intercom master stations at the Central Monitoring Workstation Location.

P.2.3.1.1 Route calls among different intercom servers

When the Central Monitoring Workstation location needs to open an intercom channel to a vehicle or pedestrian lane, or to an ACP Gatehouse, they dial the destination address. The Installation-wide Intercom recognizes the address as belonging to a connected server and routes the call appropriately.

P.2.3.1.2 Route calls to/from Central Monitoring Workstation Location

When a Guard Booth is not staffed, the vehicle lane intercom station pushbutton will ring several locations including the Gatehouse and the Central Monitoring Workstation location. The Installation-wide Intercom server receives the dial request from the ACP Intercom server and routes the call to the master station at the Central Remote Monitoring Location.

P.2.3.2 ACP Intercom Services

The intercom system provides functions to create communication channels among the different actors at the vehicle and pedestrian lanes, Guard Booth, and Gatehouse.

P.2.3.2.1 In-Lane Call Initiation

The user at the vehicle or pedestrian lane can push the button on the Intercom station to request to speak with a Guard. The button push rings the intercom master stations at the Guard Booth, ACP Gatehouse, and Central Monitoring Workstation location. Any of

these can answer. The system can be configured to ring all simultaneously or to ring sequentially if not picked up.

P.2.3.2.2 Guard Booth Call Initiation

The Guard can initiate a call to any defined location from the master station in the Guard Booth. The Guard dials the appropriate number or uses the hyperlink on the map display of the Lane Control Client to open a communication channel.

P.2.3.2.3 Gatehouse Call Initiation

The Guard in the Gatehouse can initiate a call to any defined location from the master station in the Gatehouse. The Guard dials the appropriate number or uses the hyperlink on the map display of the Lane Control Client to open a communication channel.

P.2.3.2.2 Guard Booth Call Answer

The Guard answers a call by pressing the call connect button on the master station.

P.2.3.2.3 Gatehouse Call Answer

The Guard answers a call by pressing the call connect button on the master station.

P.2.3.3 Symmetry PACS

The Symmetry PACS is decomposed in SV-4-5 (Figure 31). This system decomposes into the Installation-wide PIR data store, and the ACP Lane Control Client (shown in Figure 33, SV-4-7).

P.2.3.3.1 Installation-wide Data Store

The Installation-wide Data Store is responsible for managing the SQL Server database that holds the PIR data. The Data Store hosts an API used by Registration software as well as the IMM Client to copy the PIR captured at registration into the Data Store.

P.2.3.3.2 Cache Box Data Store

The Cache Box Data Store provides local storage of the local population at Tier 2 sites. It is synchronized with the Cloud Server to act as a backup in the event that commnications connectivity between the Cloud server and the installation is disrupted.

P.2.3.3.3 ACP Lane Control

The ACP Lane Control system is decomposed (see Figure 33, SV-4-7) into functions to support hardware interaction (Gate Arm, Lane Reader, and Vehicle loop detectors) and operator interaction (Symmetry Lane Control Client).

The Lane Control Client presents the Guard (operator) with a view that includes the three cameras in a vehicle lane, a picture of the user attempting access from the local database that can be used to compare with the live video of the driver face, information about the credential presented to the reader and the credential owner. The Lane Control Client also displays a graphic map view of a vehicle lane with icons for the controlable devices. The operator can perform actions on these devices through interacting with the on-screen icons.

P.2.3.3.3.1 Grant Trusted Traveler Access

If the driver presenting credentials is a designated Trusted Traveler (TT) and their credential is valid, the gate arm will rise automatically and the traffic light will turn green. There is no action for the Guard to take.

P.2.3.3.3.2 Grant Non-TT Access

If the driver presenting credentials is not a designated TT, the gate arm will not rise automatically. Instead the system waits for the guard to grant access after reviewing the on-screen information. This action is performed by touching an on-screen icon to grant access (touch-enabled monitor) or by clicking with the mouse.

P.2.3.3.3.3 Deny Access

If the driver presenting credentials is not a designated TT, the gate arm will not rise automatically. Instead the system waits for the guard to make an access decision after reviewing the on-screen information. The Guard can choose to deny access. For instance, driver's not granted TT designation are not permitted to escort personnel onto the base and this may be cause for denying access. This action is performed by touching an on-screen icon (touch-enabled monitor) or by clicking with the mouse. The Guard must then allow the vehicle driver to exit the lane and turn around (see P.2.3.3.3.4).

P.2.3.3.3.4 Traffic Hold and Turn Around

If the driver is not granted access, the Guard must assist the driver and vehicle to exit the lane and leave the facility. This is done by stopping other lane traffic to allow for a safe egress, and then raising the gate arm for the driver to perform a U-turn.

P.2.3.4 Video Systems

Multiple in lane cameras work in tandem to support the collection and storage of video from the rear of vehicle, driver, and front of vehicle cameras (or alternatively just the user in a pedestrian gate). The cameras deliver video streams to the various operators who select to view the video associated with vehicle and pedestrian lanes. The Video system limits video streaming bandwidth by transcoding the video to support the end-point size and resolution.

APPENDIX Q

SV-4b Services Functionality Description

APPENDIX Q

SV-4b Services Functionality Description

DODAF v2.02 removes SV-4b, Services Functionality Description from the System Viewpoints.

APPENDIX R

SV-5 Operational Activity to Systems Function Traceability Matrix

APPENDIX R

SV-5 Operational Activity to Systems Function Traceability Matrix

DODAF v2.02 removes SV-5, Operational Activity to Systems Function Traceability Matrix from the System Viewpoints. This System Viewpoint is shown in SV-5a in Appendix S.

APPENDIX S

SV-5a Operational Activity to Systems Function Traceability Matrix

APPENDIX S

SV-5a Operational Activity to Systems Function Traceability Matrix

The SV-5a addresses the linkage between System Functions described in SV-4 Systems Functionality Description and Operational Activities specified in OV-5a Operational Activity Decomposition Tree. The SV-5a depicts the mapping of system functions to operational activities. The SV-5a identifies the transformation of an operational need into a purposeful action performed by a system or solution.

SV-4 Reference	System Function	Operational Activity
P.2.1	Registration	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.1	Operator Assisted Registration	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.1.1	Capture PIR data from applicant	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.1.2	Submit PIR data for Validation and Vetting	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.1.3	Print local badge	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.1.4	Submit PIR data	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.2	Web-based Preregistration	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.3	Manage and Control Installation Barred Person List	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.1.4	PIR Data Store	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2	IMM Interface System	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1	IMM Client	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.1	Barred List Vetting	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.1	Determine credential type	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.2	IoLS Credential Validation and Identity Vetting	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.2	Credential exists locally	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.3	LE Vetting	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.3	Request vetting/validation	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance

SV-4 Reference	System Function	Operational Activity
P.2.2.1.4	Audit and Alarm Management	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.4	Capture fingerprint data	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.5	Periodic Re-vetting	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.5	Store PIR record	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.1.6	Respond to User	Register at VCC, Train Registrar, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.2.2	IMM Automatic Registration	Register In Lane, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3	Intercom System	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.1	Installation Wide Intercom Services	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.1.1	Route calls among different intercom servers	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.1.2	Route calls to/from Central Remote Monitoring Location	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.2	Intercom Services	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.2.1	In-Lane Call Initiation	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.2.2	Guard Booth Call Initiation	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.2.2	Guard Booth Call Answer	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.2.3	Gatehouse Call Initiation	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance

SV-4 Reference	System Function	Operational Activity
P.2.3.2.3	Gatehouse Call Answer	Use AIE-3/4, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3	Symmetry PACS	Trusted Traveler Access, Non-Trusted Traveler Access, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.1	Installation-wide Data Store	Register at VCC, Register in Lane, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.2	Cache Box Data Store	Register at VCC, Register in Lane, Handheld operation, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.3	ACP Lane Control	Trusted Traveler Access, Non-Trusted Traveler Access, Control Lane Equipment, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.3.1	Grant Trusted Traveler Access	Trusted Traveler Access, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.3.2	Grant Non-TT Access	Non-Trusted Traveler Access, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.3.3	Deny Access	Denied Access, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.3.3.4	Traffic Hold and Turn Around	Denied Access, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
P.2.3.4	Video Systems	Use AIE-3/4, Train Guards, Train Users, Contractor Support Call Center, Contractor Maintenance
	Manage System Configuration	Establish Commander Intent, Configure for Commander Intent, Establish ORI Connection, Enact FPCON Changes

Figure 52: SV-5a, Operational Activity to Systems Function Traceability Matrix

APPENDIX T

APPENDIX T

This page intentionally left blank

APPENDIX U

SV-5c Operational Activity to Systems Function Traceability Matrix

APPENDIX U

SV-5c Operational Activity to Systems Function Traceability Matrix

DODAF v2.02 removes SV-5c, Operational Activity to Systems Function Traceability Matrix from the System Viewpoints.

APPENDIX V

SV-6 Systems Resource Flow Matrix

APPENDIX V

SV-6 Systems Resource Flow Matrix

The Systems Resource Flow Matrix (SV-6) details characteristics of the information exchanged between systems within the AIE-3/4 Architecture. The flow of information, instructions, and material between the various systems are broken down and the attributes of the exchanges are laid out. Some of the attributes include:

- System Interface (SI) ID
- System Description
- Resources Exchanged
- Source/Producer of Data
- Destination/Consumer of Data
- Data Content
- Data Format

System Interface Identifier	System Description	Resources Exchanged	Source	Destination	Content	Format
SI-001	Registration	Personal Information and credentials	Registrants	Registration Client RGWS	Capture PII and credential data to vet registrant for Installation access suitability	PIR Data: JPG for photo and signature, ANSI 378 FP template, Text for biographical information and parsed credential data
SI-002	Removed					
SI-003	Registration	PIR data	Registration Client	Site/Cloud Server Cache Box	Store PIR data	PIR Data
SI-004	Visitor Website Registration	Personal Information	Registrants	Cloud Server	Capture biographical data and DL or other ID information	PIR Data
SI-005	Monitoring and Control	Voice and control data	Central Remote Monitoring Workstation	Site Server	Control commands for lane equipment, Intercom	PIR Data
SI-006	Monitoring and Control	Voice, Video, and alarms	Intercom Camera Gate arm	Central Remote Monitoring Workstation	Video streaming from lane cameras, intercom, and locally generated alarm information	RTSP streaming protocol, MPEG-4 compression, intercom protocol
SI-007	Hawkeye Sync Services	PIR data	Cloud Server	Cache Box	Synchronize PIR database from Cloud Server to Installation Cache Box for high operational availability.	PIR data
SI-008	Monitoring and Control	Voice and control data	Guard workstation (Gatehouse)	Site/Cloud Server	Control commands for lane equipment, Intercom	AMAG proprietary protocol for commands, XML, intercom protocol

System Interface Identifier	System Description	Resources Exchanged	Source	Destination	Content	Format
SI-009	Monitoring and Control	Voice, Video, and alarms	Intercom Camera Gatearm	Guard workstation (Gatehouse)	Video streaming from lane cameras, intercom, and locally generated alarm information	RTSP streaming protocol, MPEG-4 compression, intercom protocol
SI-010	Monitoring and Control	Voice and control data	Guard workstation (Guard Booth)	Site/Cloud Server	Control commands for lane equipment, Intercom	AMAG proprietary protocol for commands, XML, intercom protocol
SI-011	Monitoring and Control	Voice, Video, and alarms	Intercom Camera Gatearm	Guard workstation (Guard Booth)	Video streaming from lane cameras, intercom, and locally generated alarm information	RTSP streaming protocol, MPEG-4 compression, intercom protocol
SI-011a	IMM AutoReg	Personal Information and credentials	Unregistered party	RGWS Site/Cloud Server	Capture PII and credential data to vet registrant for Installation access suitability	Innometriks protocol, XML
SI-012	Access	Credentials	AIE-3/4 registered party	Symmetry Gate Controller	Decoded Credential data	Wiegand interface, XML
SI-013	Access	Control Signals	Symmetry Gate Controller ADAM Module 24VDC Relay	Gate Arm, Traffic light	Control signals	Dry contacts
SI-014	Handheld	Log data, Request PIR	Handheld	Site/Cloud Server	Transaction accounting, Credential data	Time/Date and Text
SI-015	Handheld	Personal Information and credentials	Site/Cloud Server	Handheld	Person information record for display on handheld	PIR Data

System Interface Identifier	System Description	Resources Exchanged	Source	Destination	Content	Format
SI-016	Handheld	Credential data	AIE-3/4 registered party	Handheld	Credential	Smart Card (CAC/PIV/PIV-I), barcode
SI-017	Vehicle Entry/Exit	Control Signals	Vehicle detectors	Symmetry Gate Controller	Control signals	Dry contacts

Figure 53: SV-6, System Resource Flow Matrix

APPENDIX W

SV-7 System Measures Matrix

APPENDIX W

SV-7 System Measures Matrix

DODAF v2.02 redefines Systems Viewpoint 7 (SV-7) as System Measures Matrix rather than Systems Performance Parameters. SV-7 specifies qualitative and quantitative measures (metrics) of resources; it specifies all the measures. One of the primary purposes of SV-7 is to communicate which measures are considered most crucial for the successful achievement of the mission goals assigned and how those performance parameters will be met.

System Specification Identifier	Requirement	How Measured	How Met
SS_100	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 registration.	Demonstrate function	Registration Client sends data to IMM Client which interfaces with external resources such as IoLS and Law Enforcement vetting services to verify credentials and user identity.
SS_101	The System shall vet credentials with authoritative databases through IoLS and populate registration fields without the operator having to re-key information. The System will connect to IoLS for access to DEERS, the local database, NCIC and out to the Federal Bridge. The System will connect to DEERS, independently of IoLS and be available in the event IoLS is unavailable.	Demonstrate function	IMM Client vets credentials with authoritative databases through IoLS and the Iberon NCITE LE Vetting service. Registration client connects to local databases for Barred Persons list and automatically populates registration fields. Registration Client stores PIR in local Installation-wide PIR data store.
SS_102	The System shall deny registration to personnel registering as permanent party who receive negative results from authoritative databases and shall proceed with the registration process for those receiving positive results.	Demonstrate function	Registration Client notifies Registrar of the negative results and Registrar can quit registration process.
SS_104	The System shall be capable of reading and recording a Federal Information Processing Standard (FIPS) Publication (PUB) 201-1 compliant credential for personnel access control during registration, vehicle lane operations, and pedestrian portal operations.	Demonstrate function	Registration Client can read CAC and PIV credentials during registration. Rhino Reader and Qscan Reader can read CAC and PIV credentials during Fixed Full vehicle and pedestrian lane operations. The handheld device can read CAC and PIV credentials during vehicle and pedestrian lane operations.
SS_105	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) and verifying credentials with DEERS.	Demonstrate function	Registration Client can read DOD Teslin credentials during registration. Rhino Reader and Qscan Reader can read DOD Teslin credentials during Fixed Full vehicle and pedestrian lane operations. The handheld device can read DOD Teslin credentials during vehicle and pedestrian lane operations.
SS_107	The System shall display information obtained from credentials along with a captured digital image of the credential holder to the enrollment operator.	Demonstrate function	Registration Client captures digital image locally or retrieves it from authoritative source.
SS_109	The System shall be capable of reading fingerprints, recalling templates for everyone enrolled in the database and authenticating the individual's identity by their fingerprint with the registration database.	Demonstrate function	Registration stores template in ANSI 378 format. Rhino Reader reads template and matches against live fingerprint scan.

System Specification Identifier	Requirement	How Measured	How Met
SS_110	The System shall have the capability to accept no fingerprints and continue the enrollment process.	Demonstrate function	A button on screen allows the operator to skip the step.
SS_112	The System shall store an enrollee Personal Identification Number (PIN) of up to ten digits with the registration record.	Demonstrate function	Registration Client collects a PIN up to 10 digits and stores it with the Personal Information Record (PIR). Note: Symmetry presently only supports PIN up to 8 digits.
SS_113	The System shall allow input at the time of registration the Force Protection Condition (FPCON) levels at which the individual is authorized to enter the facility.	Demonstrate function	Registration Client requests input for designation of FPCON at which level individual authorization is removed.
SS_115	The Registrar shall be capable of designating a user's TT privileges based on applicable Installation policies and regulations.	Demonstrate function	TT status is stored with PIR and propagates through the system.
SS_119	The System shall be capable of querying user for input, allowing user to enter information and collecting credential information, PIN, digital photo, signature, and fingerprint data for all registrants. The System shall store all valid forms of identification for users.	Demonstrate function.	The collected data is included in the PIR and propagated throughout the system.
SS_120	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.	Demonstrate function	Registration Client scans the 2D barcode from a driver's license and decodes the data and parses out the desired information.
SS_124	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.	Demonstrate function	Registration Client notifies Registrar of the negative results and Registrar can quit registration process.
SS_125	The System shall electronically read and record information from an individual's driver's license or state issued identification card into the System database and issue a visitor pass.	Demonstrate function	Registration Client scans the 2D barcode from a driver's license and decodes the data and parses out the desired information.
SS_127	The System shall allow the Registrar to manually enter and update user personal information into the Registration System including access denied and debarments.	Demonstrate function	Collected information is editable.
SS_129	The System shall generate long-term badges (plastic) and short-term visitor passes (paper) and	Demonstrate function	Registration Client includes the expiration date with the PIR record.

System Specification Identifier	Requirement	How Measured	How Met
	allow Registrar to assign expiration date and time. Badge formats shall be IAW with AIE Concept of Operations.		Registration has different label formats when printing to paper or plastic card.
SS_131	The System shall have the capability to allow CAC, Teslin card and Driver's License holders to use their authorized credential to automatically register at both Fixed Full and Handheld vehicle lanes.	Demonstrate function	CAC and Teslin cards are defined in the referenced document, "How to read and use credentials in AIE3". IMM AutoReg and Rhino Reader and Qscan Reader support the ability to scan and decode a driver's license for use as a credential.
SS_132	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 barcode and vet against authoritative databases.	Demonstrate function	The Rhino Reader and Qscan Reader under control of the IMM AutoReg service running at the Site server is designed to read the credentials, decode, and parse the credential data, and submit the vetting request to IMM Client.
SS_134	The System shall deny registration for personnel who receive a negative response from vetting process.	Demonstrate function	The Rhino Reader and Qscan Reader under control of the IMM AutoReg service running at the Site server is designed to deny registration for negative vetting response. Partial PIR record is stored in PIR data store with flag that credential is invalid.
SS_135	The System shall display the retrieved image of the driver from the DEERS database, DMV (if available) or other authoritative databases.	Demonstrate function	The IMM Client retrieves the photo from the authoritative source where available and stores it with the PIR.
SS_200	The System shall perform a Wants and Warrant checks through IoLS using data from National Crime Information Center (NCIC) during registration of permanent parties and at automatic registration.	Demonstrate function	IMM Client submits the vetting request to IoLS, and all CIME checks are automated by IoLS.
SS_201	The System shall perform a check of in-state and out-of-state law enforcement and DMV data sources using data from a driver's license captured and decoded during registration at a registration station, vehicle lane or handheld.	Demonstrate function	IMM Client connects to an LE Vetting service in a manner like how it connects to IoLS. The LE Vetting service supports NCIC III, NCIC Hotfile, in-state and out-of-state law enforcement and DMV data sources.
SS_203	The System shall maintain a list of personnel that are denied access onto the Installation.	Demonstrate function	Registration System supports the ability to maintain and manage a local barred list.
SS_204	The System shall update user records through IoLS every 15 minutes.	Demonstrate function	IMM Client is configurable to request population updates from IoLS every 15 minutes.
SS_206	The System shall perform verification of state issued credentials with DMV databases via the Installation's Originating Agency Identifier (ORI) connection in real-time independent of IoLS.	Demonstrate function	IMM Client connects to an LE Vetting service in a manner like how it connects to IoLS. The LE Vetting service supports NCIC III, NCIC Hotfile, in-state and out-of-state law enforcement and DMV data sources.

System Specification Identifier	Requirement	How Measured	How Met
SS_207	The System shall perform initial vetting of visitors via the Installation's ORI connection to the NCIC (Interstate Identification Index (III) files), DMV and in-state or out-of-state law enforcement sources in real-time independent of IoLS.	Demonstrate function	IMM Client connects to an LE Vetting service in a manner like how it connects to IoLS. The LE Vetting service supports NCIC III, NCIC Hotfile, in-state and out-of-state law enforcement and DMV data sources.
SS_208	The System shall perform re-vetting at selectable time intervals via the Installation ORI connection of enrolled personnel using data from NCIC (Interstate Identification Index (III) files), DMV and in-state or out-of-state law enforcement sources.	Demonstrate function	IMM Client connects to an LE Vetting service in a manner like how it connects to IoLS. The LE Vetting service supports NCIC III, NCIC Hotfile, in-state and out-of-state law enforcement and DMV data sources.
SS_209	The System shall deny access at the lanes and pedestrian portal to individuals who fail periodic vetting.	Demonstrate function	IMM Client processes any negative vetting responses in the update request and flags these records as Invalid to prevent access.
SS_301	The System shall allow the operator from the Guard Booth or Gatehouse to switch to manual control of pedestrian and vehicular lane operations.	Demonstrate function	Symmetry Lane Control Client supports the ability to change modes of operation. With appropriate operator credentials, this can be accomplished at Guard Booth, Gatehouse, or Remote Central Monitoring location.
SS_302	The System shall provide continuous digital video surveillance of pedestrian portal and vehicle lanes.	Demonstrate function	Symmetry CompleteView receives video streams from all cameras at the ACP and can provide this video to any Lane Control Client requesting the video.
SS_303	The System shall record digital video of all access control transactions that occur in each pedestrian lane for seven days and the ability to store 180 days of events requiring intervention.	Measure incremental storage required and calculate capacity.	The Site/Cloud Server storage is sized to support the necessary scale and growth.
SS_305	The System shall compare applicant information against the access denied list and alert gate guard staff when a denied individual attempts to gain access. The access denied list shall be automatically updated to each ACP upon status change.	Demonstrate function	As individuals are added to the Barred list, they are checked against the Installation-wide PIR database. If a match is found, the record is flagged as Invalid. Changes to records are additionally queued for synchronization to ACP's with a Cache Box. Therefore, ACP has all Barred list persons flagged. Furthermore, IMM AutoReg will submit credentials to IMM Client for vetting which includes Barred list checking.
SS_308	The System shall provide the System Administrator the capability to select the FPCON level. The System shall provide the Operators the capability to configure each lane using a selectable menu to increase the following access criteria for the FPCON requirements: automatic registration, personal credentials plus PIN, personal credentials plus fingerprint, personal credentials plus PIN and fingerprint, at any FPCON Level.	Demonstrate function	Symmetry Lane Control Client allows operator with appropriate privilege to make FPCON changes.

System Specification Identifier	Requirement	How Measured	How Met
SS_313	The System shall have the capability for ACP, lane and Pedestrian Portal monitoring and control at the Guard Booth.	Demonstrate function	Symmetry Lane Control Client supports the ability to run reports including transaction history. Real-time transactions are viewable through the client as well.
SS_316	The System shall provide the capability for a FIPS 201-1 compliant wireless Handheld capable of reading PIV, PIV-I, CAC, DD Form 2, DA Form 1602, Defense Biometric Identification System (DBIDS), state driver's license, Transportation Worker Identification Card (TWIC) and displaying user data and image.	Demonstrate function NOTE: DA Form 1602 does not contain machine readable information	Hawkeye Mobile software running on the ZebraTC72, or CrossMatch handheld can read all the indicated credentials except for the DA Form 1602 which is not machine-readable.
SS_320	The System shall provide a minimum lane throughput of six authorized vehicles per minute.	Measure time to process and calculate throughput	Authorized credentials are processed very quickly through the Rhino Reader and Symmetry Gate Controller or Qscan Reader and ADAM Module.
SS_325	The System shall display a stored image of the driver from the local database to the lane control guard and deny automated access when not available.	Demonstrate function	Symmetry Lane Control Client displays photo from stored PIR data as referenced by the credential processed at the Rhino Reader. Visual Verify displays photo for use of the Qscan Reader. IMM Mobile displays phot for use on the handheld.
SS_326	The System vehicle lane digital 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.	Demonstrate function	Driver camera is part of the intercom station. The device has a vertical FOV of 45 degrees. The intercom is mounted to provide the desired range.
SS_327	The System shall display a real time video or image to the lane control guard of the vehicle rear license plate.	Demonstrate function	Symmetry Lane Control Client displays real-time video from rear camera.
SS_328	The lane digital 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.	Measure incremental storage and calculate capacity.	Symmetry CompleteView NVR manages video recordings. The Site Server and NVR Server storage is sized to support this requirement in concert with SS_130.
SS_329	The System shall enable authorized personnel to access enrollment records and electronic entry control equipment.	Demonstrate function	Symmetry Lane Control Client supports the ability to access PIR database and manage entry control equipment. With appropriate operator credentials, this can be accomplished at Guard Booth, Gatehouse, or Remote Central Monitoring location.
SS_330	The System shall prominently identify to the lane control guard whether the driver is allowed Trusted Traveler privileges.	Demonstrate function	Symmetry Lane Control Client displays information including TT status from stored PIR data as referenced by the credential processed at the Rhino Reader, Qscan Reader, or handheld. Hawkeye Visual Verify is also used to display information when using the Qscan.

System Specification Identifier	Requirement	How Measured	How Met
SS_332	The System shall display description information to the Guard Booth, Gatehouse, and central remote location for all access denial events.	Demonstrate function	Access Denied events are classified as alarms in the system and communicated to all clients.
SS_333	The System shall provide an integrated traffic light (green, red).	Demonstrate function	Traffic Light is controlled by the Symmetry Gate Controller or 24VDC Relay or ADAM Module.
SS_334	The System shall provide a traffic hold capability that allows the Lane Guard to hold all traffic and allow a vehicle to turn around.	Demonstrate function	Symmetry Lane Control Client provides a traffic hold function that can temporarily restrict traffic at other lanes and allow manual raising of the gate arm to allow the vehicle to turn around.
SS_337	The System shall generate a signal capable of indicating alarm conditions to remote workstations and Installation's Intrusion Detection System if a vehicle crashes into the traffic arm when it is in the down position.	Demonstrate function	Symmetry Gate Controller receives an alarm condition from the gate crash sensor and communicates this to all Symmetry clients. Other systems are notified either through software integration or through dry contact closure from Symmetry Gate Controller.
SS_344	The System shall have the capability to scan and compare fingerprint and display results at the vehicle lane.	Demonstrate function	Rhino Reader scans and verifies fingerprint. When in biometric mode, access is only granted after successful verification.
SS_348	The System shall provide a minimum ACP pedestrian throughput rate of three authorized personnel per minute per lane.	Measure time to process and calculate throughput	Authorized credentials are processed very quickly through the Rhino Reader and Symmetry Gate Controller, or Qscan and ADAM Module.
SS_406	The System shall be capable of reporting alarm conditions that remain off normal for periods exceeding 500 milliseconds.	Demonstrate function	Symmetry Local Processor selected to meet requirement.
SS_407	The System shall provide an alarm notification within three seconds of unauthorized attempts to access the Installation or System component failure (tamper, power failure, or System failure).	Demonstrate function	Symmetry Local Processor selected to meet requirement.
SS_500	The System shall provide Uninterruptible Power Supply (UPS) to supply power to the AIE System in the event of power loss. The 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. The 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.	Demonstrate function	UPS selected to meet requirement.
SS_501	The System (defined for RAM as one ACP with two vehicle lanes) shall be configured and installed to	Demonstrate design features to support	COTS equipment is reliable and designed for the intended use.

System Specification Identifier	Requirement	How Measured	How Met
	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.	requirement. Endurance Test	
SS_502	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 becomes unusable when the System cannot automatically validate or verify the credentials presented at the ACP.	Demonstrate design features to support requirement. Endurance Test	COTS equipment is reliable and designed for the intended use. Site/Cloud Server configured for high availability cluster.
SS_503	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).	Demonstrate design features to support requirement. Endurance Test	ACP local processor or Cache Box provide for local access in the event the Site Server or Cloud server are not reachable. COTS equipment is reliable and designed for the intended use.
SS_504	The System shall have an A_o of 97% per pedestrian portal.	Demonstrate design features to support requirement. Endurance Test	ACP local processer or Cache Box provide for local access in the event the Site Server or Cloud Server are not reachable. COTS equipment is reliable and designed for the intended use.
SS_505	The probability of the System granting entry to an unauthorized individual (false acceptance rate) shall be less than 0.1 percent.	Documentation from manufacturer	Attestation from manufacturer per National Industrial Security Program Operating Manual (NISPOM), section 5-312, 5-313, 5-314.
SS_506	The probability of the System denying entry to an authorized individual (false rejection rate) shall be less than 1.0 percent.	Documentation from manufacturer	Attestation from manufacturer per National Industrial Security Program Operating Manual (NISPOM), section 5-312, 5-313, 5-314.
SS_507	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.	Demonstrate function	Gate Arm can be raised to up position manually or electronically.

System Specification Identifier	Requirement	How Measured	How Met
SS_512	The Registration System shall have an A_o of 97% (the Registration System as defined for RAM shall be two Registration Workstations).	Demonstrate design features to support requirement. Endurance Test	COTS products selected to meet the requirement.
SS_513	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.	Demonstrate design features to support requirement. Endurance Test	COTS products selected to meet the requirement.
SS_514	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).	Demonstrate design features to support requirement. Endurance Test	COTS products selected to meet the requirement. The Site/Cloud Server is configured in a high availability cluster in support of this requirement.
SS_515	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.	Demonstrate design features to support requirement. Endurance Test	COTS products selected to meet the requirement. The Site/Cloud Server is configured in a high availability cluster in support of this requirement.
SS_516	The System shall conduct a graceful shutdown in the event of power loss and automatically restart upon restoration of power.	Demonstrate function	Site Server will be powered by UPS. The OS will be integrated to the UPS and will shut down gracefully when UPS indicates main power failure.
SS_600	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.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_601	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.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_602	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.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_603	The System components installed in interior locations having uncontrolled environments shall be rated for continuous operation under ambient	Manufacturer's data sheet	COTS products selected to meet the requirement.

System Specification Identifier	Requirement	How Measured	How Met
	environmental conditions of minus 18 to plus 50 degrees C dry bulb and 10 to 95 percent relative humidity and non-condensing.		
SS_604	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.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_605	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.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_606	All exterior System components shall be operable in precipitation of up to two inches/hour.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_607	All System components shall be operable in icing conditions.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_608	All exterior components shall withstand exposure to solar ultraviolet radiation without performance degradation for a period of 10 years.	Manufacturer's data sheet	COTS products selected to meet the requirement.
SS_609	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.	Manufacturer's data sheet	Appropriate components are selected to meet rugged operational and environmental requirements.
SS_713	The System shall be able to securely create, store, update, and delete PIR data for all registrants.	Demonstrate function	Registration Client supports operators with appropriate privilege to create, modify, and delete PIR data in the system.
SS_716	The System shall provide uninterrupted entry control processing despite loss of data connectivity from the network or site server.	Demonstrate function	ACP local processor and Cache Box provide for local access in the event the Site Server or Cloud Server are not reachable. COTS equipment is reliable and designed for the intended use.
SS_719	The System shall record date, time, location, and identity of all personnel granted access in the access control events records.	Demonstrate function	Symmetry Local Processor time stamps all transactions and uploads to the Site Server in real-time.
SS_720	The System shall store access control event records for 30 days. NCIC III transaction records shall be stored for three years.	Demonstrate function	The Site Server and NVR Server are sized to store the access control and video data as specified.

System Specification Identifier	Requirement	How Measured	How Met
			NOTE: NCIC III transactions are stored at LE Vetting Service due to CJIS restrictions.
SS_722	The System shall be able to discriminate between individual switches, sensors, entry control devices, and report status to the Network Management Workstation, Central Remote Station, and Registration Station.	Demonstrate function	Network monitoring and control equipment selected to meet the requirement.
SS_727	The System shall provide the capability to count and tally vehicle entry per ACP per vehicle lane.	Demonstrate function	Contractor provides additional tools to generate the requested reports.
SS_730	The System shall have the capability for the ACP Gatehouse, Guard Booth, and central remote location to login to the System and use touch screen technology to control/override ACP transactions.	Demonstrate function	Symmetry Lane Control Client supports touch screen technology.
SS_731	The System shall provide the capability for all credential readers to be equipped with visual and audible feedback when credential is read.	Demonstrate function	Rhino Reader, Qscan Reader, and handheld support visual and audible feedback.
SS_732	The System should not register the same person more than once.	Demonstrate function	Registration Client does not allow registration when a match exists in the system.
SS_734	The System shall provide the capability for the Guard Booth to monitor and control multiple vehicle lanes using the AIE System.	Demonstrate function	Symmetry Lane Control Client supports the ability to monitor and control multiple lanes from a single workstation.
SS_735	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. Gate crash and tail gate alarms are inactive.	Demonstrate function	Handheld operates independently of vehicle lane and can be used in tandem.
SS_803	The System shall verify the fingerprint read at the vehicle lane and wireless Handheld device against registration database and provide results within 5.0 seconds.	Measure transaction time	Rhino Reader and Hawkeye Mobile software running on CrossMatch handheld device perform fingerprint match in less than 5 seconds. The Qscan Reader and Zebra TC72 do not have fingerprint capabilities.
SS_804	The System program software shall electronically connect with in-state and out-of-state law enforcement sources and local DMV databases.	Demonstrate function	IMM Client interfaces with the external LE vetting service that connects to NLETS which supports in-state and out-of-state law enforcement and DMV.
SS_809	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	Demonstrate function	IMM Client interfaces with the external IoLS. Locally generated credentials and PIR can be uploaded to IoLS for CIME verification.

System Specification Identifier	Requirement	How Measured	How Met
	any of the following three categories: 1. Does not have a digital identity in DoD-wide DEERS 2. Does not have a DoD ID card 3. 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.		

Figure 54: SV-7, System Measures Matrix

APPENDIX X

SV-8 Systems Evolution Description

APPENDIX X
SV-8 Systems Evolution Description

The SV-8 presents a whole lifecycle view of resources (systems), describing how they change over time. It shows the structure of several resources mapped against a timeline and allows for planning technology insertion.

X.1 Modular COTS Systems Overview

The AIE-3/4 System is made of modular COTS components selected for their suitability to the AIE-3/4 system performance specifications, and their interoperability. The systems selected utilize published and manufacturer-supported interfaces. Since the solution is modular, it is amenable to subsystem replacement and feature expansion to support future needs.

X.2 Technology Insertion Capability

Technology insertion is manageable due to the modular design of the AIE-3/4 solution. As computer systems fail or simply age compared to future state of the market capabilities, the technology can be inserted into the AIE-3/4 solution very easily. If the software components to run on the new technology platform are compatible, the technology insertion should have no impact on operation. If a compatibility issue is identified, the modular components can be updated individually given the API between the modules does not change.

The modular solution also lends itself to enhanced technology introductions. As new capabilities are identified and developed, they can easily be added to the AIE-3/4 solution with minimal effort to incorporate the new service or system through API support. An example of this is the addition of the LE Vetting service. The AIE-3 demonstration system did not support an LE Vetting service, but once one was identified, the IMM Client was updated to support the new service and other processing was not impacted.

X.3 Lifecycle Events

SV-9, Systems Technology Forecast identifies technologies that could be incorporated into the AIE-3/4 system to improve performance. These are not depicted in a lifecycle timeline in this SV-8 since they are not identified by the program office.

APPENDIX Y

SV-9 Systems Technology Forecast

APPENDIX Y
SV-9 Systems Technology Forecast

SV-9 summarizes predictions about trends in technology and personnel. Architects may produce separate SV-9 products for technology and human resources. The forecast is focused on technology and human resource areas that are related to the AIE-3/4 mission.

Y.1 Biometrics at Stand-Off Distances

Biometric technologies continue to improve in accuracy and performance. The latest biometric technologies can capture the biometric data in a contactless way. Fingerprint readers can read fingerprints from five (5) feet away, and iris readers can read iris data from up to 10 feet away. These capabilities are enabled through optical zoom lenses, and therefore the user must cooperate to a degree and be in a defined area for the system to read the biometric data.

The addition of contactless biometric capture in AIE-3/4 could provide faster throughput during times at higher FPCON when biometrics are required. This technology is presently available and could be integrated into AIE-3/4 within 12-18 months.

Y.2 Facial Recognition (FR)

Use of FR as a biometric credential has been successfully piloted on AIE-3/4 at the Redstone Arsenal. The success of this pilot provides a useful benchmark to gauge the future challenges in expanding the capability to provide fast, reliable, and accurate processing of through-the-windshield detection and extraction of driver and vehicle occupants to make access determinations at commensurate costs. There are various technology factors that affect the efficacy of FR to expedite traffic flow such as number and types of cameras being used, type of illuminator used, detection and extraction processing at the edge, facial matching algorithms and processing speeds.

In addition, there are the human factors that present challenges to the use of FR such as users adhering to best practice behavior (i.e., removing large dark glasses, remaining face forward as approaching, removing obstructions within the vehicle) as well as having current up-to-date photographs populated in the facial matching gallery as part of the registration process.

Y.3 Integrated Security Solutions

Integrating security solutions into a seamless enterprise can maximize the security posture of an Installation. For example, an integrated system approach for AIE with the Integrated Commercial Intrusion Detection System (ICIDS) improves security by connecting key components of the security enterprise and increases visibility by creating a common operating picture across the enterprise. This integration enables efficient operations by 1) consolidating and automating tasks, leveraging existing infrastructure, site activities and support; 2) optimizing existing AIE technology investments especially with the Cloud and the various monitoring and management capabilities enabled by the Cloud; and 3) minimizing the system's managerial and administrative activities.

Y.4 Centralized Law Enforcement Vetting

Technology advancements are making it possible for law enforcement data to be shared across multiple states and jurisdictions providing a centralized consolidated repository of information about an individual. Having access to such information in a secure automated way can greatly increase the effectiveness of the vetting process. Additionally applying Artificial Intelligence and Machine Learning (AI/ML) techniques against such data can expedite the vetting process.

APPENDIX Z

SV-10a Systems Rules Model

APPENDIX Z

SV-10a Systems Rules Model

The Systems Rules Model provides the systems rules and constraints for the AIE-3/4 System. This is provided in matrix form as it lends itself to detailing the rules and how they are related to the activities. The matrix is sorted by System Rule (SyR) and shows the mapping of the rule to one or more activities (as may be appropriate).

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
SyR-001	The AIE-3/4 System will be installed at US Military Installations (predominantly US Army Facilities).	Provide AIE-3/4	PM FPS	AIE-3/4	
SyR-002	The AIE-3/4 System will be installed at all locations by civilian contractors.	Provide AIE-3/4	PM FPS	AIE-3/4	
SyR-003	The AIE-3/4 System will be mission capable in environments that meet basic cold and hot weather criteria and be capable of continuous operation under harsh weather and environmental conditions.	Provide AIE-3/4	PM FPS	AIE-3/4	
SyR-004	The AIE-3/4 System will operate using local commercial power and be equipped with an Uninterruptible Power Source (UPS).	Provide AIE-3/4	PM FPS	AIE-3/4	
SyR-004	The system will be operational 24 hours a day, seven days a week.		Installation	AIE-3/4	
SyR-005	Portable Registration will be provided for remote registration at pre-determined locations.		PM FPS	Portable Registration Workstation	
SyR-006	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.		PM FPS	Registration Workstation, Portable Registration Workstation	
SyR-007	The Enrollment Workstation is operated by Installation registration personnel.		Installation	Registration Workstation, Portable Registration Workstation	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
SyR-008	Pursuant to 5 USC. §552a (e) (3), an AIE Privacy Act Statement will be displayed on a placard at each Registration station, portable registration station, at each vehicle lane, and at each pedestrian portal.		PM FPS	Registration Workstation, Portable Registration Workstation, Vehicle Pedestal, Pedestrian Pedestal	
SyR-009	Data does not reside permanently on the Enrollment Workstation.		Contractor	Registration Workstation, Portable Registration Workstation	
SyR-010	All communication is encrypted using a network encryption method that is transparent to the system operator(s).		Installation	AIE-3/4	
SyR-011	Portable Registration capability will be provided with an accompanying carrying case.		PM FPS	Portable Registration Workstation	
SyR-012	The system will have the capability to function with different configurations: Automatic Registration; Gate Arm down; Gate Arm up with traffic light functioning; Credential Reader only; Credential and PIN; Credential and fingerprint; or Credential, PIN, and fingerprint.		Contractor	AIE-3/4	
SyR-013	A Vehicle Pedestal, located at each lane, contains an intercom, credential reader with PIN capability, 1D and 2D barcode scanner, driver camera and a fingerprint scanner.		Contractor	Vehicle Pedestal	
SyR-014	Driver camera will capture the driver's image within a height range of three (3) to seven (7) feet from the ground.		Installation	Driver Intercom, Vehicle Pedestal	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
SyR-015	Wireless Handheld readers will be FIPS 201-1 compliant with the ability to capture fingerprints and accept authorized credentials and PINs. The device will have the ability to display user information, photos, and fingerprint data. The device will not store user data and all data transmissions will be encrypted. The Wireless Handheld device will be configured such that the operator cannot modify configuration.		Contractor	Handheld	The Government waived the fingerprint requirement for ACP operations.
SyR-016	The Site Server stores personal information records of all Installation users and can store at least 2,000,000 (scalable up to 20,000,000) personal records.		Contractor	Site Server	
SyR-017	The Site Server will utilize a web service open architecture interface to IoLS for vetting to DEERS and other authoritative databases.		Contractor	IMM	
SyR-018	AIE-3/4 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).		Installation Personnel	NEC Equipment	
SyR-019	Communication between AIE-3/4 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-3 System will also encrypt data at rest.		Contractor	All servers	
SyR-020	The AIE-3/4 System will be subjected to Government Security Test and Evaluation (ST&E) for yearly cybersecurity risk assessments. Documents, data, certification tests results, and access will be provided as required for major changes and recertification/reauthorization.		Government	Network Components	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
SyR-021	The AIE-3/4 System will receive a Certificate of Net worthiness (CoN).		Contractor	Network Components	CoN superseded by RMF ATO process
SyR-022	AIE-3/4 System operators continuously assess and monitor security policies and procedures to incorporate an Information Assurance Vulnerability Management (IAVM) program.		Contractor	Network Components	
SyR-023	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-3/4 System owner as a part of the system DIACAP/RMF Documentation.		Contractor	Network Components	
SyR-024	AIE-3/4 will employ IA and IA-enabled products as part of the security architecture. These products must be on the DoD Unified Capabilities Approved Products List (DoD UC APL) and be National Security Telecommunications and Information Systems Security Policy Number11 (NSTISSP-11) compliant.		Contractor	Network Components	
SyR-025	All AIE-3/4 equipment will be configured for IPv6. Internal client applications that communicate with public internet servers and supporting networks using IPv4 must be upgraded to use dual-stack IPv6.		Contractor	Network Components	
SyR-026	The AIE Product Support Strategy uses all 10 elements of logistics support contained in AR 700-127 Integrated Logistics Support (ILS) as a guide for sustaining the AIE system during its life cycle.		Contractor and PM FPS	AIE-3/4	

Rule ID	Rule/Constraint	Activity	Primary Performer	Primary System	Comments
SyR-027	The AIE-3/4 System will employ Total Package Fielding (TPF) in accordance with AR 700-142 to ensure fully supportable systems and their required support are provided to using units with minimal disruption of their day-to-day missions.		Contractor and PM FPS	AIE-3/4	
SyR-028	Following completion of the one year of CLS, sustainment of a fielded AIE-3/4 System transitions to the CECOM SEC Lab located at Aberdeen Proving Ground (APG), MD to provide organic AIE System sustainment support after the CLS period. Arrangements are also made with other Army Support Commands as appropriate for the life cycle sustainment of the AIE System.		CECOM SEC Lab located at Aberdeen Proving Ground (APG), MD	AIE-3/4	

Figure 55: OV-10a, System Rules Model

APPENDIX AA

SV-10b Systems State Transition Description

APPENDIX AA

SV-10b Systems State Transition Description

The AIE-3/4 System is a system of integrated COTS products. The products have been selected to meet operational needs. Therefore, the System Viewpoints line up with Operational Viewpoints, and the reader is directed to Appendix I for the OV-6b System State Descriptions.

APPENDIX BB

SV-10c Systems Event-Trace Description

APPENDIX BB

SV-10c Systems Event-Trace Description

The AIE-3/4 System is a system of integrated COTS products. The products have been selected to meet operational needs. Therefore, the System Viewpoints line up with Operational Viewpoints, and the reader is directed to Appendix J for the OV-6c Event Trace Descriptions.

APPENDIX CC

SV-11 Physical Schema

APPENDIX CC
SV-11 Physical Schema

CC.0. Background

DODAF V2.02 reclassifies System Viewpoint 11 (SV-11), Physical Schema in the new category, Data Information Viewpoint 3 (DIV-3), and Physical Data Model. This is a complement to DIV-2, Logical Data Model (see Appendix K).

CC.1. COTS Interfaces

AIE-3/4 is comprised of Commercial off the Shelf (COTS) products that have open and published Application Programming Interfaces (APIs) that allow the sharing of data from one system to another. By utilizing these API's, the COTS component manufacturers have worked together to produce the AIE-3/4 System that will be deployed. Therefore, the Logical Data Model described here is simply the data sharing capability that allows the interface of one system to another. The internal data models of the COTS products are not available to the Prime Contractor or to the Government due to their proprietary and trade secret nature.

CC.1.1. IMM Client Local Vetting Gateway

The following table lists the parameters of the Identity Management Middleware interface that is exposed to the IMM-AutoReg (in-lane registration).

ICD Parameter	Description	Data Type
Plugin	Defines the Authoritative Service to use for credential validation	Text (4) {IoLS, LEV, …}
credentialTypeCode	Type of credential submitted.	1 – PIV (other federal) 2 – DoD ID Card (CAC/Teslin) 3 – PIV-I (other non-federal) 4 – TWIC 5 – DBIDS Local PACS 6 – AIE Local PACS 7 – NACMS Local PACS 8 – USMC Local PACS 9 – Component PACS
tokenTypeCode	Type of token submitted.	02 – Bar Code (DoD, PACS, and FiXs PIV-I) 04 – FASC-N (DoD and PIV) 20 – GUID (PIV-I)

tokenString	The token data.	Text (50)
valid	0 for not valid, or 1 for valid	{0, 1}
validSpecified	0 for “valid” not specified, or 1 for “valid” specified in response	{0, 1}
credentialStatusCode	Validity response from authoritative source	Text (4). See Reference 3 below for enumeration
credentialStatusDate	Last update of credential status. See Reference 3 below.	Date
credentialStatusDateSpecified	1 if credentialStatusDate has been specified, otherwise 0.	{0, 1}
_IMM_Success	1 if the request was completed successfully, otherwise 0.	{0, 1}
_IMM_ErrorString	If an error occurred, contains the error string, otherwise <null>	Text (50)
PN_SYS_ID	Person System Identifier.	Text (10)
PN_SYS_ID_TYP_CD	Person System Identifier Type Code.	Text (1) D – DoD EDI PI L – Local Population EDI PI
PN_ID	Person Identifier.	Text (9)
PN_ID_TYP_CD	Person Identifier Type Code.	Text (1): S – SSN – Social Security Number F – Special 9-digit DoD code created for foreign military and nationals I – ITIN – Tax Identification Number T – Test ID used only for Test purposes
PN_LST_NM	Person Last Name.	Text (26)
PN_1ST_NM	Person First Name.	Text (20)
PN_SEX_CD	Person Gender.	Text (1): F – Female M – Male Z – Unknown
PN_BRTH_DT	Person Birth Date.	Date
PN_BRTH_DTSpecified	1 if the PN_BRTH_DT was specified, otherwise 0	{0, 1}
US_CTZP_STAT_CD	Code indicating US Citizen Status.	Text (1): N – No Y – Yes Z – Unknown
PHT_IMG	Photo Image	Hex/Binary in JPG format
MA_LN1_TX	Mailing Address Line 1 text	Text (40)
MA_CITY_NM	Mailing Address City Name	Text (20)
MA_ST_CD	Mailing Address State Code.	Text (2)
MA_CTRY_CD	Mailing Address Country Code.	Text (2). See Reference 3 below for enumeration.
MA_PR_ZIP_CD	Mailing Address Postal Region Code (i.e., ZIP code).	Text (5)
MA_PR_ZIPX_CD	Mailing Address Postal Region Extended Code.	Text (4)
CRD_EXP_DT	Card Expiration Date.	Date

CRD_EXP_DTSpecified	1 if the CRD_EXP_DT was specified, otherwise 0	{0, 1}
NAC_STAT_CD	National Agency Check Status Code. See Reference 3 below for enumeration.	Text (1). See Reference 3 below for enumeration.
NAC_LST_DT	National Agency Check Last Performed Date.	Date
NAC_LST_DTSpecified	1 if the NAC_LST_DT was specified, otherwise 0	{0, 1}
TKN_TYP_CD	Token Type Code.	02 – Bar Code (DoD, PACS, and FiXs PIV-I) 04 – FASC-N (DoD and PIV) 20 – GUID (PIV-I)
TKN_ID	Token Identifier data.	Text (50)
TKN_END_DT	The TKN_END_DT will always be equal to CRD_EXP_DT	Date
TKN_END_DTSpecified	1 if the TKN_END_DT was specified, otherwise 0	{0, 1}

Figure 56: Identity Management Middleware Interface Physical Schema

CC.1.2. IMM Client Interface to External Resource, IoLS

The Interoperability Layer Services (IoLS) is a cloud service offered by DMDC and provides credential and identity validation services as well as continuous information management engine (CIME) for identity related security alerts. The IoLS interface is defined by DMDC and is documented as indicated in the reference section below.

CC.1.3. IMM Client Interface to External Resource, LE Vetting Service

The Law Enforcement (LE) Vetting Service is a cloud service offered by Iberon. The interface is described in the document as indicated in the reference section below

CC.1.4. Symmetry Interfaces

The Symmetry Security Management System by AMAG Technology acts as the management resource for personal information record (PIR) data. There are two interfaces defined by AMAG Technology that are used in the AIE-3/4 System. The Data Connect interface is used to store PIR data in the database after a successful registration and during the PIR synchronization process, and to retrieve PIR data for

operational use. The XML Open Integration Module is used to control devices like the gate arm and traffic light from the Handheld.

CC.2. OPMG Dashboard Reports

Data is collected from the Symmetry databases across the installations to support the OPMG Dashboard reports to include Existing Credentials, Credentials Added, Credentials Denied, Access Granted and Access Denied.

CC.2.1 Dashboard Table

Dashboard table collects data from Symmetry that is ready to be displayed in the OPMG AIE Dashboard report. It shows counts of cards issued.

Parameter	Description	Data Type	Comment
DashboardID	Unique Identifier	bigint	Primary Key
DashBoardDate	When date was collected	datetime	
SiteID	OPMG ID for site	bigint	Foreign Key
RegisteredPersons	Count of persons registered	bigint	
DODCredentials	Count of active DOD Credentials	bigint	
VisitorCredentials	Count of active Visitor Credentials	bigint	
VHICCredentials	Count of active Veterans Health Insurance Cards	bigint	
ForeignMilitary	Count of cards issued to Foreign Military	bigint	
RFIDCredentials	Count of RFID tags issues.	bigint	

Figure 57: Dashboard Table Physical Schema

CC.2.2 DimSet Table

The DimSet table is a crosswalk between a basic datetime representation of a point in time, ‘2021-12-31’, and various attributes of the date, such as day of the week (Friday), day of the month(31), etc.

Parameter	Description	Data Type	Comment
DateKey	Unique identifier	int	Primary Key
Date	YYYY-MM-DD 00:00:00	datetime	
FullDateUK	UK Date: DD-MM-YYYY	char(10)	
FullDateUSA	USA Date: YYYY-MM-DD	char(10)	
DayOfMonth	Day of Month 1-31	varchar(2)	
DaySuffix	Th,nd,st	varchar(4)	
DayName	Name of Day	varchar(9)	
DayOfWeekUSA	Number of Day, 1-7	char(1)	
DayOfWeekUK	Number of Day, USA - 1	char(1)	
DayOfWeekInMonth	Day 1 is the first Sunday of the month.	varchar(2)	
DayOfWeekInYear	Day 1 is the first Sunday of the CY.	varchar(2)	
DayOfQuarter	Day 1 is the first Sunday of the FY.	varchar(3)	
DayOfYear	Day of Julian Calendar, 1-366	varchar(3)	
WeekOfMonth	5APR2020 => 2,start SUN	varchar(1)	
WeekOfQuarter	First week begins sun after 1st mon Oct/Jan/Apr/Aug	varchar(2)	
WeekOfYear	First week begins sun after 1st mon of Jan	varchar(2)	
Month	1-12	varchar(2)	
MonthName	Name of month	varchar(9)	
MonthOfQuarter	1-3	varchar(2)	
Quarter	1-4	char(1)	
QuarterName	First…	varchar(9)	
Year	yyyy	char(4)	
YearName	CY YYYY	char(7)	
MonthYear	Yyyy-mm-01	char(10)	
MMYYYY	MMYYYY	char(6)	
FirstDayOfMonth	YYYY-mm-01	date	
LastDayOfMonth	YYYY-mm-(28-31)	date	
FirstDayOfQuarter	YYYY-mm-01	date	

Parameter	Description	Data Type	Comment
LastDayOfQuarter	YYYY-mm-(30-31)	date	
FirstDayOfYear	YYYY-01-01	date	
LastDayOfYear	Yyyy-12-31	date	
IsHolidayUSA	0=NO,1=True	bit	
IsWeekday	0=NO,1=True	bit	
HolidayUSA	Name of Holiday	varchar(50)	
IsHolidayUK	0=NO,1=True	bit	
HolidayUK	Name of Holiday	varchar(50)	
FiscalDayOfYear	1-366	varchar(3)	
FiscalWeekOfYear	1-52	varchar(3)	
FiscalMonth	1-12	varchar(2)	
FiscalQuarter	1-4	char(1)	
FiscalQuarterName	First,Second,Third,Fourth	varchar(9)	
FiscalYear	YYYY	char(4)	
FiscalYearName	FY YYYY	char(7)	
FiscalMonthYear	FYYY-MM-01	char(10)	
FiscalMMYYYY	MMFYYY	char(6)	
FiscalFirstDayOfMonth	1/1/2020 => 12/8/2019??1st Sun after 1st Sat	date	
FiscalLastDayOfMonth	1/1/2020 => 1/4/2020?? Sat prior to next FiscalFirstDayOfMonth	date	
FiscalFirstDayOfQuarter	1st Sun after 1st Sat	date	
FiscalLastDayOfQuarter	Sat prior to next FiscalFirstDayOfQuarter	date	
FiscalFirstDayOfYear	First Sunday of CY after first Sat	date	
FiscalLastDayOfYear	Saturday prior to next FiscalFirstDayOfYear	date	

Figure 58: DimSet Table Physical Schema

CC.2.3 Exceptions Table

When operations malfunction, details of that activity are stored in the Exceptions Table.

Each installation's instance of OPMG has capacity to capture malfunctions in data gathering from Symmetry and/or transfer to the common OPMG database.

Parameter	Description	Data Type	Comment
ExceptionID	Unique Identifier	bigint	Primary Key
Comment1	Text explaining conditions	nchar(230)	
Comment2	Text explaining conditions	nchar(230)	
ExceptionText	SQL generated text	nchar(1030)	
TimeOfException	Time Exception occurred.	datetime	

Figure 59: Exceptions Table Physical Schema

CC.2.4 LaneHoursCounts Table

LaneHourCounts provides a summation of hourly counts of scans for a given day for a given site. When joined with the SiteACPID it allows a report to readily present a site's hourly counts with meaningful names for the site and ACPs.

Parameter	Description	Data Type	Comment
LaneHourCountsID	Unique identifier	bigint	Primary Key
LaneHourCountsDate	Day of counts,yyyy-mm-dd	datetime	
SiteID	SiteID of installation	bigint	Foreign Key
ACPID	Abbreviation found in Symmetry for a given Access Control Point	nchar(10)	
Lane	Abbreviation found in Symmetry for a given Lane	nchar(10)	
h0	Counts for scans from 0001 to 0100 hours	bigint	
h1	Counts for scans from 0101 to 0200 hours	bigint	
h2	Counts for scans from 0201 to 0300 hours	bigint	
h3	Counts for scans from 0301 to 0400 hours	bigint	
h4	Counts for scans from 0401 to 0500 hours	bigint	
h5	Counts for scans from 0501 to 0600 hours	bigint	
h6	Counts for scans from 0601 to 0700 hours	bigint	

Parameter	Description	Data Type	Comment
h7	Counts for scans from 0701 to 0800 hours	bigint	
h8	Counts for scans from 0801 to 0900 hours	bigint	
h9	Counts for scans from 0901 to 1000 hours	bigint	
h10	Counts for scans from 1001 to 1100 hours	bigint	
h11	Counts for scans from 1101 to 1200 hours	bigint	
h12	Counts for scans from 1201 to 1300 hours	bigint	
h13	Counts for scans from 1301 to 01400 hours	bigint	
h14	Counts for scans from 1401 to 1500 hours	bigint	
h15	Counts for scans from 1501 to 1600 hours	bigint	
h16	Counts for scans from 1601 to 1700 hours	bigint	
h17	Counts for scans from 1701 to 1800 hours	bigint	
h18	Counts for scans from 1801 to 1900 hours	bigint	
h19	Counts for scans from 1901 to 2000 hours	bigint	
h20	Counts for scans from 2001 to 2100 hours	bigint	
h21	Counts for scans from 2101 to 2200 hours	bigint	
h22	Counts for scans from 2201 to 2300 hours	bigint	
h23	Counts for scans from 2301 to 2400 hours	bigint	
AllHours	Counts for scans from 0001 to 2400 hours	bigint	
TransType	Type of Transaction e.g., ‘Scan’	nchar(30)	Primary Key

Figure 60: LaneHoursCount Table Physical Schema

CC.2.5 Site Table

The Site Table stores the distinctive characteristics of an installation, allowing it to be distinguished from other sites, and for the parsing of Symmetry transactions.

Parameter	Description	Data Type	Comment
SiteID	SiteID of installation	bigint	Primary Key
Site	Name of Site	nchar(30)	

ServerID	Name of server hosting Symmetry for installation	nchar(30)
SiteGroup	Group that contains this site	nchar(30)
ServerType	Category that contains this site	nchar(30)
CompanyID	CompanyID in Symmetry for this Site	smallint
SiteAbbr	Site Abbreviation in Symmetry for this Site	nchar(3)
LastUpdated	<deprecated> reserved to identify last date a site's data has been updated. Not in use.	datetime
RFIDprefix	<deprecated> three-digit code in RFID codes distinct for the site. Not in Use.	nchar(3)
AIEPrefix	<deprecated> three-digit code in AIE card codes distinct for the site. Not in Use.	nchar(3)
Logo	Graphical logo for the site	varbinary(MAX)

Figure 61:Site Table Physical Schema

CC.2.6 SiteACPID Table

The SiteACPID Table contains names for the ACPIDs found in Symmetry

Parameter	Description	Data Type	Comment
SiteID	SiteID of installation	bigint	Primary Key
Site	Name of Site that appears in report	nvarchar(30)	
ACPID	ACPID of Access Control Point found in Symmetry	nvarchar(10)	
ACPNAME	Name of ACP that appears in report	nvarchar(50)	
IsFiltered	No if included in report, yes if not included in report	nvarchar(1)	

Figure 62:SiteACPID Table Physical Schema

CC.2.7 TransTimeData Table

The TransTimeData Table stores hourly and daily counts of all types of transactions queried from the Symmetry databases at different sites. Counts are further broken down by type of card, type of person, and ACP/VCC and Lane/WorkStation.

Parameter	Description	Data Type	Comment
TransTimeID	Unique Identifier	bigint	Primary Key
TransID	**<deprecated> reserved for storing the Symmetry Transaction ID, not in use.**	nchar(30)	
TransType	Top level categorization of transaction (i.e., Scan,Denial)	nchar(30)	See TransType Values CC.2.7.1
TransDate	**Yyyy-mm-dd of transactions**	datetime	
TransSubType	Second level categorization of transaction	nchar(255)	
SiteID		bigint	Foreign Key
ACPID	ID of Access Control Point or VCC in Symmetry	nchar(10)	
Lane	**ID of Lane or WorkStation in Symmetry**	nchar(10)	
TimeToCompleteSecs	<deprecated> reserved to capture time it takes to complete a given transaction. Not in use.	float	
subTotal	**The count of similar transactions for the given identifiers in this record**	float	
TransSubType2	Third level categorization of transaction	nchar(30)	See TransSub Type2 Values Table CC.2.7.2, CC.2.7.3
TransSubType3	Fourth level categorization of transaction	nchar(30)	See TransSubType3 Values Table CC.2.7.4
TransDateHr	Hour of day when transactions occurred, 00-23	nchar(2)	
TransTimeIDLocal	**The TransTimeID of the transaction stored in the local instance of OPMG, stored in the Central instance of OPMG**	bigint	

Figure 63: TransTimeData Table Physical Schema

CC.2.7.1 TransType Values

This table shows valid values for the TransType

Value	Description
Denial	Denial during initial vetting
Denial3	Denial during continuous vetting
NonAccessScan	Scan for something other than access

Value	Description
OtherAccess	Scan for abnormal access, not used for scan counts
scan	Normal scan, used for scan counts

Figure 64: TransType Values

CC.2.7.2 TransSubType2 Values for Scans

This table shows valid values for the TransSubType2 when the TransType=Scan

Value	Description
AIE	AIE card issued
AIECTR	AIE card issued to Contractor
AIEFamily	AIE card issued to Family member
AIEForeign	AIE card issued to foreigner
CTR	Contractor CAC
DOD	DOD CAC
DOJ	DOJ CAC
Family	Family CAC
ForEmp	Foreign Employee CAC
ForMil	Foreign Military CAC
Other	unknown card type
Retiree	Retiree CAC
RFID	RFID
TESDisabled	Teslin issued to Disabled servicemember
TESFormer	Teslin issued to former servicemember
TESMOH	Teslin issued to MOH
TESRetiree	Teslin issued to Retiree
TESRetireeC	Teslin issued to Retiree
TESSurvivor	Teslin issued to Survivor of servicemember

Value	Description
VHIC	Veterans' Health Insurance Card

Figure 65: TransSubType2 Type for Scans Values

CC.2.7.3 TransSubType2 Values for Continuous Denials

This table shows valid values for the TransSubType2 when the TransType=Denial3

Value	Description
Ambiguous	Ambiguous
AWOL	Absent WithOut Leave
BA	Debarred
BL	Blacklisted
Debar	Debarred
DEERS	Issue with DEERS
DrivingIssue	DrivingIssue
Felony	Felony
FTA_Child	Failure to appear
FTA_Credit	Failure to appear
FTA_Other	Failure to appear
FTA_Traffic	Failure to appear
FTA_Vehicle	Failure to appear
IdentityIssue	Failure to identify
iii	"iii" in rejection message
InvalidCard	InvalidCard
IOLS	IOLS flag
NCIC	NCIC flag
NL	"NL" in rejection message
QUARANTINE	QUARANTINE
RE	"RE" in rejection message

Sexual	Sexual offense
STOP	"STOP" in rejection message
SU	"SU" in rejection message
TSDB	Terrorist
Violent	Violent Offender
WAI	Warrant for arrest

Figure 66: TransSubType2 for Continuous Denials Values

CC.2.7.4 TransSubType3 Values for Continuous Denials

This table shows valid values for the TransSubType3 when the TransType=Denial3

Value	Description
AIE	AIE card issued
AIECTR	AIE card issued to Contractor
AIEFamily	AIE card issued to Family member
AIEForeign	AIE card issued to foreigner
CTR	Contractor CAC
DOD	DOD CAC
DOJ	DOJ CAC
DPlus	<Extraneous scan, filtered out>
Family	Family CAC
ForEmp	Foreign Employee CAC
ForMil	Foreign Military CAC
Other	unknown card type
Retiree	Retiree CAC
RFID	RFID
TESDisabled	Teslin issued to Disabled servicemember
TESFormer	Teslin issued to former servicemember
TESMOH	Teslin issued to MOH

Value	Description
TESRetiree	Teslin issued to Retiree
TESRetireeC	Teslin issued to Retiree
TESSurvivor	Teslin issued to Survivor of servicemember
VHIC	AIE card issued

Figure 67: TransSubType3 for Continuous Denials Values

CC.2.8 UserSite Table

The UserSite table cotains the of users with access to OPMG reports and determines which site(s) they may view. Multiple entries can exist for a user, with the union of all sites indicated made visible to this user.

Parameter	Description	Data Type	Comment
UserSiteID	Unique Identifier	bigint	Primary Key
UserID	The userid found in the AIE Active Directory.	nchar(30)	
SiteID	SiteID of installation	bigint	Foreign Key
SiteGroup	Group that contains this site	nchar(30)	
ServerType	Category that contains this site	nchar(30)	
SiteAbbr	Site Abbreviation in Symmetry for this Site	nchar(3)	

Figure 68: UserSite Table Physical Schema

CC.3 References

1. *Symmetry Homeland Security Edition Data Connect Manual 9.3.0v1 (9600-0459) G4S TECHNOLOGY, 13 February 2020*

2. *Symmetry XML Open Integration Module User Guide 9.3.0v1 (9600-0469) G4S TECHNOLOGY, 13 February 2020*

3. *Interoperability Layer Services Software Development Guide v2.1.1, Defense Manpower Data Center, February 2015*

4. *Identity Matching Engine for Security and Analysis (IMESA) Interface Control Document (ICD) 1.3 v, February 2020*

5. *Iberon NCITE Vetting Service Interface Control Document*

APPENDIX DD

TV-1 Technical Standards Profile

APPENDIX DD
TV-1 Technical Standards Profile

DODAF V2.02 reclassifies Technical Viewpoint 1 (TV-1), Technical Standards Profile in the new category, Standards Viewpoint 1 (StdV-1). The title is simply, Standards Profile. The intent of the change is to allow inclusion of not just technical standards, but also business standards, guidance and policy that apply to the solution.

DD.1 Government Documents

The following documents contribute to this architecture to the extent that they reflect topics and content which relate to the AIE-3/4 requirements and architecture. Unless otherwise specified, the latest revision of the referenced document is in effect. Documents not specifically identified in the body of this architecture are for reference only.

DD.1.1 DoD Documents (in alphabetical order)

a. Army Regulation (AR) 25-1, *Army Information Technology*, 15 July 2019.
b. AR 25-2, *Army Cybersecurity, 4 April 2019*
c. AR 70-1, *Army Acquisition Policy,* 10 August 2018.
d. AR 190-13, *Army Physical Security Program*, 27 June 2019
e. AR 525-13 *Antiterrorism* December 2019
f. AR 525-28 *Personnel Recovery* 3 May 2010
g. AR 530-1 *Operations Security (OPSEC)* 16 September 2014
h. AR 700-127, *Integrated Product Support*, 22 October 2018
i. Army Access Control Points Standard Definitive Design, 13 April 2019
j. Chairman of the Joint Chief of Staff Instruction (CJCSI) 3170.01I *Joint Capabilities Integration and Development System (JCIDS)*, 23 January 2015.

k. CJCSI 5123.01G, *Charter of the PEO CBD Requirements Oversight Council,* 30 October 2021

l. Department of the Army (DoA), Office of the Chief Information Officer, *Army Information Architecture (AIA) v4.1*, 5 June 2013.

m. *DoD Architecture Framework (DoDAF) v2.02*, Change 1, Volumes I, II, III, & IV, January 2015.

n. DoD Direction (DoDD) 1000.25 *DoD Personnel Identity Protection (PIP) Program* 2 March 2016

o. DoDD 5101.07, *DoD Executive Agent for Information Technology Standards*, 21 May 2004.

p. DoDD 5400.11 DoD Privacy Program Change 1, Effective: 8 December 2020

q. DoD 5400.11-R Department of Defense Privacy Program Change 1, Effective: 8 December 2020

r. DoD, Office of the Chief Information Officer, *DoD Information Enterprise Architecture (IEA) v2.0*, Volume I, August 2012

s. DoD, Office of the Chief Information Officer, *DoD Information Enterprise Architecture (IEA) v2.0*, Volume II, August 2012

t. *DoD Information Technology Standards Repository (DISR),* (See DoDD 5101.07, May 2004).

w. DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, May 19, 2010, Incorporating Change 3, Effective: 20 November 2015.

u. DoD 5200.08R, *Physical Security Program*, April 9, 2007, Incorporating Change 2, 19 October 2020

x. DoDI 8500.01, *Cybersecurity*, 14 March 2014, Incorporating Change 1, Effective: 7 October 2019.

v. DoDI 8510.01, *Risk Management Framework for DoD Information Technology*, 29 December 2020

w. DoDD 8570.01 *Information Assurance Training, Certification, and Workforce Management* 15 August 2004

x. DoD 8570.01-M *Information Assurance Workforce Improvement Program* 19 December 2005

y. DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 July 2004.

z. Military Standard (MIL-STD) 130N *Identification Marking of U S Military Property* 16 November 2012

aa. MIL-STD 810, *Environmental Engineering Considerations and Laboratory Tests*, latest revision (G or later), with Change 1, Effective 15 April 2014

bb. Security Equipment Integration Working Group (SEIWG) Interface Control Document (ICD) 0101B, *Force Protection Systems Sensor Information Interchange Information Interchange using XML*, June 2011.

y. Unified Capabilities Requirements (UCR) 2013, *Unified Capabilities Requirements 2013,* January 2013, Change 2, Effective 2 September 2017.

DD.1.2 Other Government Documents

a. Criminal Justice Information Services, *Electronic Fingerprint Transmission Specification (EFTS)*, July 2013

b. Criminal Justice Information Services, *Electronic Biometric Transmission Specification (EBTS)*, 14 December 2012

c. Criminal Justice Information Services 6510.01F Information Assurance (IA) and Computer Network Defense (CND) 9 June 2015

d. Department of Labor (DOL), *Americans with Disabilities Act: Accessibility Guidelines for Buildings and Facilities (ADAAG),* Latest Revision/Update.

e. Federal Highway Administration (FHWA), Installation of Traffic Control Devices, FHWA-SA-89-006, March 1988.

h. *FIPS 140-3: Security Requirements for Cryptographic Modules.* National Institute for Standards and Technology (NIST) Computer Security Resource Center (CSRC). 22 March 2019

i. *FIPS 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors.* NIST CSRC. January 2022

f. NIST SP 800-53 *Security Controls for Federal Information Systems and Organizations,* April 2013

g. NIST SP 800-53A *Assessing the Security and Privacy Controls in Federal Information Systems and Organizations* July 2014

DD.1.3 Code of Federal Regulations (CFR)

a. 36 CFR Part 1194, *Electronic and Information Technology Accessibility Standards.*

DD.1.4. AIE-3/4 Program Documents

a. AIE Standards and Specifications November 19, 2007.

b. AIE-3 Statement of Work

c. System Performance Specification for AIE-3, 22 October 2014.

d. AIE-3 Concept of Operations (CONOPS), 8 September 2014.

DD.2 Non-Government Documents

a. American National Standards Institute/National Institute of Standards and Technology- ITL 1-2011, update 2015

b. American National Standards Institute/National Institute of Standards and Technology- ITL 1-2011, updated 2013

c. National Fire Protection Association (NFPA) 72, *National Fire Alarm Code®,* 2013 (or latest revision). (Current with verbiage – 2022 is latest.)

DD.3 Order of Precedence: The contractor applies precedence in accordance with the SOW, the System Architecture (this document), the System Performance Specification and the Concept of Operations, respectively. The various Specification documents detail the technical requirements of the system and/or component. However, nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

APPENDIX EE

TV-2 Technical Standards Forecast

APPENDIX EE
TV-2 Technical Standards Forecast

DODAF V2.02 reclassifies Technical Viewpoint 2 (TV-2), Technical Standards Forecast in the new category, Standards Viewpoint 2 (StdV-2). The title is simply, Standards Forecast. The intent of the change is to allow inclusion of not just technical standards, but also business standards, guidance and policy that apply to the solution.

EE.1 Government Standards and Guidance

The National Institute of Standards and Technology (NIST) evaluates standards and guidance on a periodic basis. While Federal Information Processing Standards (FIPS) are reviewed on a five (5) year cycle, Special Publications (SP) and NIST Interagency Reports (NISTIR) are reviewed on an as-needed basis. Several documents related to the AIE-3/4 mission and the cybersecurity vulnerability assessment and mitigation requirements that AIE-3/4 systems are subject to are in a Draft status at NIST. While the Draft status is not a guarantee that the product will be released, it is an indication that the material is under review by NIST. The following are in Draft status:

- SP 800-63-3 Digital Authentication Guideline, 2 March 2022
- SP 800-116, Rev 1 Recommendations for Use of PIV Credentials in PACS, 29 June 2018
- SP 800-125A, Rev 1 Security Recommendations for Hypervisor Deployment, 28 January 2018
- SP 800-126, Rev 3 Security Content Automation Protocol (SCAP) v1.3, 14 February 2018
- SP 800-184 Guide for Cybersecurity Event Recovery, 22 December 2016
- FIPS 201-3 Personal Identity Verification, 24 January 2022

EE.2 Commercial Standards and Guidance

None identified.