



DEPARTMENT OF THE ARMY
OFFICE OF THE PROVOST MARSHAL GENERAL
2800 ARMY PENTAGON
WASHINGTON, DC 20310-2800

DAPM-MPD-PS

NOV 19 2007

MEMORANDUM FOR COMMANDER, UNITED STATES ARMY CORPS OF ENGINEERS (USACE) (CECG), GOVERNMENT ACCOUNTABILITY BUILDING, 441 G STREET NW, WASHINGTON DC 20314-1000

SUBJECT: Review of the Army System Specifications for Automated Installation Entry (AIE)

1. References:

- a. DOD Directive 5200.8R, Security of DoD Installations and Resources, April 2007.
- b. DOD Directive 1000.25, Personal Identity Protection Program, July 2004.
- c. Standard Design for U.S Army Installation Access Control Points, December 2004.
- d. MIL-STD-1472F (1999) DoD Design Criteria Standard-Human Engineering.

2. I have reviewed the Army System Specifications for AIE dated November 2007; concur with the specifications as written and request that USACE publish as an appropriate Army specifications document.

3. These specifications are considered minimum baseline requirements that all future Army AIE systems must meet. Respectfully request that the Office of the Provost Marshal General (OPMG) retain the option to review and comment on any supplementation and or modification of the specifications and approve all waivers and exceptions to these requirements.

4. I sincerely appreciate the arduous and professional efforts of the USACE Electronic Security Systems Center working hand-in-hand with my staff. These standards will ensure our Soldiers, civilians and family members living and working on Army installations remain safe.

5. Points of contact for this action are Mr. Richard Miller, COMM (703) 695-4210 or Mr. Bret Vincent, COMM (703) 692-5541.


RODNEY L. JOHNSON
Brigadier General, USA
Provost Marshal General

Army Standard for Automated Installation Entry

October 26, 2007

Part I

TABLE OF CONTENTS

1 INTRODUCTION	3
1.1 PURPOSE AND SCOPE.....	3
1.2 APPLICABILITY	3
1.3 REFERENCES.....	3
2 DEFINITIONS	3
3 REQUIREMENTS	4
3.1 IDENTITY MANAGEMENT	4
3.2 VETTING CREDENTIALS.....	4
3.3 PERMANENT PARTY ENROLLMENT	5
3.4 VISITOR ENROLLMENT	6
3.5 LANE EQUIPMENT.....	6
3.6 PEDESTRIAN PROCESSING.....	6
3.7 SYSTEM THROUGHPUT	6
3.8 SYSTEM FUNCTIONS.....	7
Appendix A	9

1 INTRODUCTION

1.1 PURPOSE AND SCOPE. This document provides standards for Army Automated Installation Entry (AIE).

1.2 APPLICABILITY. This Standard applies to all Army active installations and reserve components prime installations where government or contractors plan for, construct, and maintain Army AIE.

1.3 REFERENCES. See Appendix A.

2 DEFINITIONS

2.1 Access Control Operational Status Reporting Process: The monitoring of Access Control Point (ACP) status by ACP Operations Personnel which shall be accomplished at a computer terminal within the Department of Emergency Services (DES) to permit control of lane and turnstile activities based on traffic count, traffic events shown on video, and reports by guards with respect to equipment maintenance and law enforcement actions required through the Police Dispatcher in DES.

2.2 Access Control Point: An Access Control Point is a corridor at the Installation entrance through which all vehicles and pedestrians must pass when entering or exiting the Installation. The perimeter of the ACP consists of both passive and active barriers arranged to form a contiguous barrier to pedestrians and vehicles. ACP guards control the active barriers to deny or permit entry into the Installation.

2.3 Authentication: The process of verifying the validity of a person's identity.

2.4 Enrollment Equipment: Equipment capable of collecting data from an individual in order to establish and subsequently preparing, encrypting, managing, and storing reference data representing that person's identity.

2.5 Entry Control Devices: Equipment which provides a user the means to input identifier data into an entry control system for verification.

2.6 Identifier: A credential, personal identification number, biometric, or any other unique information entered into the entry control database for the purpose of verifying the identity of an individual.

2.7 Identity Verification: The process of confirming or refuting a claimed identity by comparing the credentials (something you know, something you have, or something you are) of a person requesting access with those previously enrolled.

2.8 Passage: Ingress and/or egress through an entry control device, or through a portal.

2.9 Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., Photograph, cryptographic keys and digitized fingerprint representation) so the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

2.10 Post Maintenance Test: Test procedures performed after maintenance and repair activities to verify proper component and system operations have been completed.

2.11 System Throughput: Rate for verified/authorized vehicles and drivers in automated vehicle/pedestrian lanes.

2.12 Validation: The process of demonstrating that a system, credential or individual meets in all respects, the specifications for authenticity.

2.13 Vetting: The examination and evaluation of an individual's information against multiple data sources to determine suitability for access to an installation.

3 REQUIREMENTS

3.1 IDENTITY MANAGEMENT

3.1.1 AIE system must accept and use Personnel Identification Record (PIR) data from Department of Defense (DOD) issued ID cards, including the Common Access Card (CAC), the DD Form 2 (retiree ID card), the DD Form 1173 (dependent ID card) and other authorized ID cards issued through the Defense Manpower Data Center (DMDC).

3.1.2 AIE system must provide a capability to record and read a FIPS PUB 201-1 compliant credential for personnel access control.

3.2 VETTING CREDENTIALS

3.2.1 AIE system must interface with and communicate electronically with the Enterprise Defense Biometric Identification System (EBIDS) or the Defense Biometric Identification System (DBIDS) for vetting of DOD credentials in continental United States (CONUS). Interface through the Biometric Identification System (BIDS) will be required for applications in

Korea and through the Installation Access Control System (IACS) in United States Army, European Command (USAREUR).

3.2.2 AIE system enrollment process must include the capability to electronically scan an individual's passport, driver's license or state issued identification card and display information embedded on the credential (i.e., barcode or magnetic stripe data) for the enrollment operator to visually compare and confirm against the data printed on the card. Information presented on the enrollment system monitor must be electronically captured for the establishment of a database entry and issue of a visitor pass.

3.2.3 AIE system must provide a capability to issue, record, and read a credential (for example, a Radio Frequency Identification (RFID) tag) for each vehicle enrolled and registered in the database and have the capability to enroll, read and accept RFID tags from other AIE installations and Air Force Smart Gate. Data received from this credential must be linked to the PIR data of the registered owner and authorized drivers.

3.2.4 AIE system must be computer based and designed to autonomously read and compare personnel and vehicle identification (ID) credentials.

3.3 PERMANENT PARTY ENROLLMENT

3.3.1 AIE system enrollment process must provide a capability to electronically scan/process an authorized individual's CAC or other DOD approved ID card to initiate a validation and verification process through DBIDS or other third party systems (e.g., Defense National Visitor Center (DNVC) to Defense Enrollment Eligibility Reporting System (DEERS)). Information obtained will be displayed along with a digital image of the credential holder for verification by the enrollment operator.

3.3.2 AIE system enrollment process must provide a modular, scalable, secure capability to create, store, update and delete PIR and vehicle registration data at the installation for all registrants. The system must have the capability to distribute this data to each ACP, each automated entrance lane, and the Visitors Control Center (VCC).

3.3.3 AIE system enrollment process must accept and use approved ID credentials (passport, state driver's license, state issued ID or other valid installation issued ID) authorized by appropriate installation access control officials for commercial vendors making deliveries or providing services.

3.4 VISITOR ENROLLMENT

3.4.1 AIE system must provide the ability to process visitor requests and issue temporary passes.

3.4.2 AIE system must provide an interface to accept computer based automated visitor pass data from DBIDS_(e.g., DNVC).

3.4.3 AIE system must provide equipment for visitors to electronically scan a passport, driver's license or state issued ID and display information embedded on the credential to the enrollment operator.

3.4.4 Information displayed must be electronically captured to populate fields in the visitor pass and credential that will be prepared for issuance. The system must provide the capability to manually enter personal and vehicular ID information.

3.4.5 AIE system enrollment process must provide the capability to electronically capture the signature of an individual for visual comparison with the signature on the individual's driver's license and retain as evidence of their voluntary acknowledgement and understanding of conditions for entrance onto a military installation.

3.5 LANE EQUIPMENT

3.5.1 AIE systems components must be designed such that they are interoperable, non-proprietary, modular, scalable, Commercial Off-The-Shelf (COTS) products that can be tailored to accommodate future hardware and software upgrades.

3.6 PEDESTRIAN PROCESSING

3.6.1 For pedestrian entry portals, an AIE system must read and display pedestrian photo and finger print identification data to the gate control person on all entry and exit sequences, as appropriate.

3.6.2 AIE system must provide for the simultaneous operation of pedestrian portals/turnstiles and vehicle lanes to maximize throughput of pedestrian and vehicular traffic.

3.7 SYSTEM THROUGHPUT

3.7.1 The AIE system must provide a minimum throughput rate for verified/authorized vehicles and driver in automated vehicle lanes of 6 vehicles per minute per lane (threshold) with an objective of 30 vehicles per minute per lane. The AIE system must provide a throughput rate of 3

(threshold) to 10 (objective) authorized personnel per minute via pedestrian portals/turnstiles.

3.8 SYSTEM FUNCTIONS

3.8.1 AIE system must provide a capability to operate using local commercial power, emergency power, and battery back-up.

3.8.2 AIE system hardware and software must be configured for use as a distributed control system using a local server and intelligent controllers at each access control point ensuring entry control processing continues when loss of data connectivity from the network or central server is experienced.

3.8.3 AIE system must use standard communication protocols and communication links of local installations. Processors and peripherals supporting the computer resources must be standard interface connectors and will not require proprietary links, connectors, or cables.

3.8.4 AIE system computers must be state-of-the-art with processor speeds and memory capacities to process the data efficiently.

3.8.5 AIE system must recognize and deny entry attempts by unauthorized personnel. Entry denials must include steps to positively prevent access while maintaining a safe environment for other persons transiting the gate area.

3.8.6 AIE system must be capable of being rapidly configured (electronically) to adapt to immediate changes in the threat conditions and apply restrictive entrance criteria consistent with the Force Protection Condition (FPCON).

3.8.7 AIE system must read and display personnel and vehicle identification data to the gate control person on all entry sequences.

3.8.8 AIE system must provide alarm notification when non-routine conditions occur such as tampering and equipment or electrical power failures.

3.8.9 AIE system must provide continuous video surveillance and video recording of all access control transactions that occur in each vehicle and pedestrian lane.

3.8.10 AIE system must enable recording, reporting and screen printing of all system events to include pedestrian and vehicle throughput data on electronic media.

3.8.11 AIE system must be capable of utilizing handheld readers at vehicle inspection points to validate credentials and read a finger print of enrolled personnel.

Appendix A

DEPARTMENT OF DEFENSE (DOD)

DOD Directive 8190.3, Smart Card Technology,

DOD Directive 8500.1, Information Assurance, October 24, 2002

DOD Directive 8000.1, Management of DOD Information Resources and Information Technology, February 27, 2002

DOD Directive 5400.11, DOD Privacy Program, November 16, 2004

DOD Directive 5200.8, Security of DoD Installations and Resources, April 25, 1991

DOD Directive 5000.1, The Defense Acquisition System, May 12, 2003

DOD Directive 1000.25, Personal Identity Protection Program, July 19, 2004

DOD Memorandum Subject Interim DoD Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance (ref. DIACAP) dated July 6, 2006

MIL-STD-1472F (1999) DoD Design Criteria Standard-Human Engineering

DEPARTMENT OF THE ARMY

Army Access Control Points Standard Definitive Design, December 2004

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

EIA ANSI/EIA-310-D (1992) Racks, Panels, and Associated Equipment

EIA ANSI/EIA/TIA-232-F (2002) Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

EIA TIA/EIA-568-B.1 (2001; Addendum 2001) Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements (ANSI/TIA/EIA-568-B.1)

EIA TIA/EIA-568-B.2 (2001) Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components (ANSI/TIA/EIA-568-B.2)

EIA TIA/EIA-568-B.2-1 (2002) Transmission Performance Specifications for 4-Pair 100 Ohm Category 6 Cabling (ANSI/TIA/EIA-568-B.2-1)

EIA TIA/EIA-568-B.3 (2000; Addendum 2002) Optical Fiber Cabling Components Standard (ANSI/TIA/EIA-568-B.3)

FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION (FIPS PUB)

FIPS PUB 140-2 (2001) Security Requirements for Cryptographic Modules

FIPS PUB 197 (2001) Advanced Encryption Standard

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

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2 (2002) National Electrical Safety Code

IEEE C62.41 (1991) Recommended Practice for Surge Voltages in Low-Voltage AC Power Circuits

IEEE STD 142 (1991, change 08/16/96) Recommended Practice for Grounding of Industrial and Commercial Power Systems - Green Book

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

(ISO)/International Electro-technical Commission (IEC)

ISO/IEC 14443-1, Parts 1-4 (2006) Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards

ISO/IEC 7810 (2003) Identification Cards—Physical Characteristics

ISO/IEC 7816 (2004) Identification Cards—Integrated Circuits with Contacts, Parts 1-6

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250 (2003) Enclosures for Electrical Equipment (1000 Volts Maximum)

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70 (2005) National Electrical Code

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Special Publication 800-73-1 (2006) Interfaces for Personal Identity Verification

Special Publication 800-76-1 (2006) Biometric Data Specification for Personal Identity Verification

Special Publication 800-78 (2005) Cryptographic Algorithms and Key Sizes for Personal Identity Verification

UNDERWRITERS LABORATORIES (UL)

UL 60950 (2003) Safety of Information Technology Equipment

UL 294 (1999; Rev thru Oct 2001) Access Control System Units

UL 796 (1999; Rev thru Dec 2003) Printed-Wiring Boards

Army Automated Installation Entry

System Specifications

October 26, 2007

Part II

TABLE OF CONTENTS

PART 1 GENERAL	4
1.1 REFERENCES	4
1.2 SYSTEM DESCRIPTION	6
1.2.1 System Level Functional and Performance Requirements	6
1.2.2 Scope of Work.....	12
1.2.3 System Definitions	12
1.2.4 Electrical Requirements	15
1.2.5 System Reaction	15
1.2.6 System Capacity	16
1.3 SUBMITTALS	16
1.3.1 Group I Technical Data Package	16
1.3.2 Group II Technical Data Package	18
1.3.3 Group III Technical Data Package	18
1.3.4 Group IV Technical Data Package	18
1.3.5 Group V Technical Data Package	21
1.4 TESTING	22
1.4.1 General	22
1.4.2 Test Procedures and Reports	22
1.5 TRAINING	23
1.5.1 General	23
1.5.2 Operator's Training.....	23
1.5.3 System Administrator Training	24
1.5.4 Maintenance Personnel Training.....	24
1.6 MAINTENANCE AND SERVICE	25
1.6.1 Warranty.....	25
1.6.2 Description of Work.....	25
1.6.3 Personnel	25
1.6.4 Schedule of Work.....	25
1.6.5 Emergency Service	26
1.6.6 Operation	26
1.6.7 Records and Logs	26
1.6.8 Work Requests.....	26
1.6.9 System Modifications	27
1.6.10 Software	27
1.7 DATA TRANSMISSION SYSTEM (DTS).....	27
1.7.1 Data Transmission System (DTS) Line Supervision	27
1.7.2 Data Encryption.....	27
1.8 INFORMATION ASSURANCE	28
1.9 DATA CURRENCY AND INTEGRITY	28
PART 2 PRODUCTS	28
2.1 MATERIALS	28
2.1.1 Commercial Off-The-Shelf (COTS) and Non-Developmental Items (NDI)	28
2.1.2 Materials and Equipment	28
2.1.3 Field Enclosures.....	29

2.1.4 Nameplates	29
2.1.5 Fungus Treatment.....	29
2.1.6 Tamper Switches	30
2.1.7 Locks and Key-Lock Switches.....	30
2.2 SYSTEM COMPONENTS	31
2.2.1 Modularity.....	31
2.2.2 Maintainability	31
2.2.3 System Overall Reliability Requirement	31
2.2.4 Interchangeability	32
2.2.5 Product Safety.....	32
2.2.6 Wire and Cable	32
2.2.7 Power Line Surge Protection.....	33
2.2.8 Device Wiring and Communications Line Surge Protection	33
2.2.9 Power Line Conditioners	33
2.2.10 Uninterruptible Power Supplies (UPS)	34
2.2.11 Environmental Conditions	34
2.2.12 AIE System Devices and Equipment.....	36
2.2.13 Actuated Traffic Arms.....	41
2.2.14 Closed Circuit Television (CCTV) System.....	42
PART 3 EXECUTION.....	43
3.1 GENERAL REQUIREMENTS.....	43
3.1.1 Installation	43
3.1.2 Enclosure Penetrations	43
3.1.3 Cold Galvanizing	44
3.1.4 Current Site Conditions	44
3.1.5 Existing Equipment	44
3.1.6 Installation of Software	44
3.2 SYSTEM STARTUP	45
3.3 SUPPLEMENTAL CONTRACTOR QUALITY CONTROL	45
3.4 TESTING	45
3.4.1 General Requirements for Testing	45
3.4.2 Pre-delivery Testing	46
3.4.3 Contractor's Field Testing	47
3.4.4 Performance Verification Test.....	47
3.4.5 Endurance Test.....	47
3.4.6 Commissioning Report.....	49

This specification covers the requirements for U.S. Army Automated Installation Entry (AIE) Systems.

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

DEPARTMENT OF DEFENSE

DoD Directive 8190.3, Smart Card Technology, August 31, 2002
DoD Directive 8500.1, Information Assurance, October 24, 2002
DoD Directive 8000.1, Management of DoD Information Resources and Information Technology, February 27, 2002
DoD Directive 5400.11, DoD Privacy Program, November 16, 2004
DoD Directive 5200.8R, Security of DoD Installations and Resources, April 9 , 2007
DoD Directive 5000.1, The Defense Acquisition System, May 12, 2003
DoD Directive 1000.25, Personal Identity Protection Program, July 19, 2004
DoD Memorandum Subject Interim DoD Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance (ref. DIACAP) dated July 6, 2006

MIL-STD-1472F (1999) DoD Design Criteria Standard-Human Engineering

ELECTRONIC INDUSTRIES ALLIANCE (EIA)

EIA ANSI/EIA-310-D (1992) Racks, Panels, and Associated Equipment

EIA ANSI/EIA/TIA-232-F (2002) Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

EIA TIA/EIA-568-B.1 (2001; Addendum 2001) Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements (ANSI/TIA/EIA-568-B.1)

EIA TIA/EIA-568-B.2 (2001) Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components (ANSI/TIA/EIA-568-B.2)

EIA TIA/EIA-568-B.2-1 (2002) Transmission Performance Specifications for 4-Pair 100 Ohm Category 6 Cabling (ANSI/TIA/EIA-568-B.2-1)

EIA TIA/EIA-568-B.3 (2000; Addendum 2002) Optical Fiber Cabling Components Standard (ANSI/TIA/EIA-568-B.3)

FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION (FIPS PUB)

FIPS PUB 140-2 (2001) Security Requirements for Cryptographic Modules

FIPS PUB 197 (2001) Advanced Encryption Standard

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

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE C2 (2002) National Electrical Safety Code

IEEE C62.41 (1991) Recommended Practice for Surge Voltages in Low-Voltage AC Power Circuits

IEEE STD 142 (1991, change 08/16/96) Recommended Practice for Grounding of Industrial and Commercial Power Systems - Green Book

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)/International Electro-technical Commission (IEC)

ISO/IEC 14443-1, Parts 1-4 (2006) Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards

ISO/IEC 7810 (2003) Identification Cards—Physical Characteristics

ISO/IEC 7816 (2004) Identification Cards—Integrated Circuits with Contacts, Parts 1-6

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250 (2003) Enclosures for Electrical Equipment (1000 Volts Maximum)

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70 (2005) National Electrical Code

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Special Publication 800-73-1 (2006) Interfaces for Personal Identity Verification

Special Publication 800-76-1 (2006) Biometric Data Specification for Personal Identity Verification

Special Publication 800-78 (2005) Cryptographic Algorithms and Key Sizes for Personal Identity Verification

UNDERWRITERS LABORATORIES (UL)

UL 60950 (2003) Safety of Information Technology Equipment

UL 294 (1999; Rev thru Oct 2001) Access Control System Units

UL 796 (1999; Rev thru Dec 2003) Printed-Wiring Boards

1.2 SYSTEM DESCRIPTION

An Automated Installation Entry (AIE) System shall be provided as described and shown including the installation of any Government Furnished Equipment. All computing devices, as defined in 47 CFR 15, shall be certified to comply with the requirements for Class A computing devices and labeled as set forth in 47 CFR 15. Electronic equipment shall comply with 47 CFR 15. The system shall include connectors, adapters, and terminators necessary to interconnect equipment. Supply cabling will be necessary to interconnect the equipment installed at the access control zone, in the Visitor Control Center, in the Access Control Point (ACP) gatehouse; in the ACP guard booths, and interconnect equipment installed at remote control/monitoring stations.

1.2.1 System Level Functional and Performance Requirements

1.2.1.1 The AIE System shall be installed at ACP's to provide automated access control onto an installation for personnel/vehicles that have been enrolled in the system and are authorized access in accordance with the Installation Commander's policy.

1.2.1.2 The AIE System shall recognize and deny entry attempts by unauthorized personnel. Entry denials shall include steps to positively prevent access while maintaining a safe environment for other persons transiting the gate area.

1.2.1.3 The AIE System shall be computer based and designed to autonomously read and compare personnel and vehicle identification (ID) credentials.

1.2.1.4 The AIE System shall provide a capability to record and read a FIPS PUB 201-1 compliant credential for personnel access control.

1.2.1.5 The AIE System shall provide a modular, scalable, secure capability to create, store, update and delete PIR and vehicle registration data at the installation for all registrants. The system shall have the capability to distribute this data to each ACP, each automated entrance lane, and the Visitors Control Center (VCC).

1.2.1.6 The AIE System shall provide accessibility to enrollment records by authorized individuals and electronic entry control equipment for all entry sequences.

1.2.1.7 The AIE System shall interface with and communicate electronically with the Enterprise Defense Biometric Identification System (EBIDS) or the Defense Biometric Identification System (DBIDS) for the vetting of DoD credentials. Interface through the Biometric Identification System (BIDS) will be required for applications in Korea and through the Installation Access Control System (IACS) in USAREUR.

1.2.1.8 The AIE System shall provide the capability to communicate with the Army's Centralized Operations Police Suites (COPS)/ Vehicle Registration System (VRS) and DBIDS/EBIDS to capture vehicle information pertaining to personnel authorized for enrollment in the system. Vehicle information obtained through COPS/VRS shall be confirmed by the registrant and electronically linked to the individual's record established in the local AIE database system.

1.2.1.9 Enrollment.

1.2.1.9.1 Permanent Party and Installation Employee Enrollment

1.2.1.9.1.1 The AIE System shall provide a capability to electronically scan/process an authorized individual's CAC, or other DoD approved ID card, to initiate a validation and verification process through DBIDS. Information obtained will be displayed along with a digital image of the credential holder for verification by the enrollment operator. Results of a successful validation will establish the baseline entry in the DBIDS or other database that is locally available to support an automated vehicle entry process. Specific items of information to be gathered during the registration process are: Name, Social Security number (SSN) (for overseas applications the requirement will include a national ID value in lieu of the SSN), signature, date of birth (DOB), residential address, expiration date of credential, FPCON access code, and unit of assignment. Prior coordination with overseas Army legal advisors is required prior to collecting and storing privacy information on local nationals. All personal identity information collected and stored shall be protected in accordance with applicable US privacy laws.

1.2.1.9.1.2 The AIE System shall accept and use personnel identification record (PIR) data from DoD issued ID cards.

1.2.1.9.1.3 The AIE System enrollment process shall establish a local database of personnel information that can be automatically correlated, validated, and updated against PIR data that has been previously vetted through DBIDS/EBIDS to the Defense National Visitor Center (DNVC) or Defense Enrollment Eligibility Requirements System (DEERS). The system shall also have the capability for the validation of PIR data to include records under the Contractor Verification System (CVS) with the DEERS.

1.2.1.9.1.4 The AIE System must provide a capability to issue, record, and read an identification device (for example, a Radio Frequency ID (RFID) tag) for each vehicle enrolled and registered in the database. Data received from this credential shall be linked to the PIR data of the registered owner and authorized drivers.

1.2.1.9.2 Visitor Enrollment

1.2.1.9.2.1 The AIE System shall provide the ability to process visitor requests, issue temporary passes for visitors and their vehicles, and enroll authorized personnel. AIE system shall allow for the pre-enrollment of approved visitors.

1.2.1.9.2.2 The AIE System shall provide an interface to accept computer based automated visitor pass data from DBIDS and other third party systems (e.g., DNVC)

1.2.1.9.2.3 The AIE System enrollment process shall include the capability to electronically scan an individual's passport, US driver's license or state issued identification card and display information embedded in the credential (i.e. bar code or mag stripe data) for the enrollment operator to visually compare and confirm against the data printed on the card. Information presented on the enrollment system monitor shall be electronically captured for the establishment of a database entry and issue of pass documentation.

1.2.1.9.2.4 The system shall provide equipment for visitors to electronically scan their US driver license and display information embedded in the credential (barcode, magnetic stripe, integrated circuit chip or other media) to the enrollment operator. The system shall provide the capability for a visitor to manually enter personal and vehicular ID information. Specific items of information to be gathered during the registration process are: name, SSN, signature, US driver's license number, date of birth, passport number, address, phone number, year, make, and model of the vehicle driven. FPCON and other status limitations, such as days, hours, and multiple or individual access area limitations. Status limitations will be entered by a system operator at the time of registration.

1.2.1.9.2.5 The AIE system will include an Optical Character Reader (OCR) to scan the license/ID card/passport presented and match the document against the government template to ensure validity.

1.2.1.9.2.6 The AIE System shall provide a capability to compare a visitor's US driver license or state issued identification card against the issuing state's records to confirm the status of the card. (This should be viewed as an objective capability that will be obtained as a spiral development at those locations where the capability can be obtained from the license issuing state.)

1.2.1.9.2.7 The AIE System shall use the information derived from the visitor's credential for comparison with public records and the National Crime Information Center to determine if an individual has outstanding Wants and Warrants or is listed on national terrorist watch lists.

1.2.1.9.2.8 The AIE System shall provide the capability to capture the electronic signature of an individual for visual comparison with the signature on the individual's US driver license and retention as evidence of their voluntary acknowledgement and understanding of the conditions for entrance on a military installation.

1.2.1.9.2.9 Information displayed shall be electronically captured for population of fields in the visitor pass and credential that will be prepared for issuance. Source data (operator name, vehicle description, license number, signature, license date of issue and expiration date) shall be stored in the local database for transaction record and comparison to installation records for suspension and barment actions.

1.2.1.9.3 Commercial Vendor Enrollment. The AIE System shall accept and use approved ID credentials (US drivers license or other valid government issued ID) authorized by appropriate installation access control officials for commercial vendors making deliveries or providing services (e.g. commercial deliveries of food, petroleum, household goods,).

1.2.1.10 The AIE System shall provide the capability to capture and recall templates of 2 fingerprints of each individual enrolled in the database. The fingerprint collection system shall conform with the Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000 and be certified interoperable with the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS). Fingerprint comparison may be required during higher FPCON threat levels or Random Antiterrorism Measures (RAM) measures.

1.2.1.11 The AIE System shall have the capability to be configurable (electronically) to adapt to immediate changes in threat conditions and apply restrictive entrance criteria consistent with the Force Protection Condition (FPCON) levels, designated RAM procedures, and an individual's status code that was entered for each individual during the enrollment process. The AIE System must be configurable as a minimum to prioritize the following configurations for gaining access to the installation

- Combination of ID Card & RFID - linking the two
- Combination of ID Card & RFID with no link
- Using the ID Card only
- Using the RFID only

NOTE: PIN capability may be utilized with any/all of the above configuration(s)

1.2.1.12 The AIE System shall read and display personnel and vehicle identification data to the lane control person on all entry sequences. The split screen display shall include real-time image of the vehicle operator as the credential is presented and an image of the rear of the vehicle to include the vehicle license plate. A stored image of the operator will be simultaneously presented on the monitor for comparison. A positive data match will be presented with a green background indicating the individual may proceed. A mismatch of the data will be presented with a red background and a diagonal bar with the word "DENIAL" indicating no access. The AIE System shall automatically display information to the lane operator and the guard house for all events where the vehicle operator or vehicle do not match or are invalid and the guard is prompted to manually check or stop the vehicle.

1.2.1.13 The AIE system shall provide the capability for an integrated traffic hold for all lanes of traffic at an ACP for turn-around and search exceptions.

1.2.1.14 The AIE System shall provide a capability for the lane control person or gate supervisor to switch to manual control of pedestrian and vehicular lane operations during emergency situations, equipment failures or malfunctions and for training purposes.

1.2.1.15 The AIE System shall provide video surveillance and recording of all access control transactions that occur in each vehicle and pedestrian lane. For vehicle lanes, the data recorded shall include vehicle driver's face with correlated vehicle data. For pedestrian lanes, the data shall include the pedestrian's face.

1.2.1.16 For pedestrian entry portals, the AIE System shall read and display pedestrian photo and finger print identification data to the gate control person on all entry and exit sequences, as appropriate and provide live video of the person processing through for comparison. AIE system must also provide two way intercom system to render assistance and directions when required as well as a remote "manual override" feature for use if or when an authorized user requires assistance processing through a portal.

1.2.1.17 The AIE System shall provide for the simultaneous operation of pedestrian portals/turnstiles and vehicle lanes to maximize throughput of pedestrian and vehicular traffic. Pedestrians desiring entry onto the installation will be required to present an approved credential in order to gain entrance to the portal/turnstile. This action coupled with the presentation of a biometric feature will successfully complete the entrance process.

1.2.1.18 The AIE System will incorporate the capability to use wireless mobile hand-held scanners to perform card and finger print read functions at vehicle inspection and pedestrian lanes.

1.2.1.19 The AIE System shall enable recording, reporting and screen printing of all system events to include pedestrian and vehicle throughput data on electronic media. Access control events records shall include date, time, location, and identity of person granted or denied access. The system shall provide user-defined and user-configurable formatting for all reports. The AIE System shall provide the capability to record and store up to 180 days of events. AIE system must have a Be On the Look Out (BOLO) capability to alert access control guards that intervention is required. AIE system must have ability to export photos for the purposes of law enforcement, generate and/or query system reports on all transactions, as well as ad hoc queries.

1.2.1.20 The AIE System components shall be designed such that they are interoperable, non-proprietary, modular, scalable Commercial-Off-The-Shelf (COTS) that can be tailored to accommodate future hardware and software upgrades.

1.2.1.21 The AIE System shall provide a capability to operate using local commercial power, emergency power, and battery back-up. Provide capability to automatically operate on emergency electric power should normal electric power fail.

1.2.1.22 The AIE System shall provide alarm notification to system monitors when non-routine conditions occur such as tampering and equipment, electrical power failures or communication failures.

1.2.1.23 The AIE System shall be operable by personnel with no more than 16 hours of initial or refresher training.

1.2.1.24 The AIE System shall be safe to operate and maintain. All components will be protected against the effects of lightning, power surges and stray electrical charges or emissions. Personnel shall be protected against the effects of electrical shock.

1.2.1.25 AIE System enrollment stations and registration components shall be safe to operate and maintain with no ergonomic hazards. All components shall be protected against the effects of lightning, power surges and stray electrical charges or emissions.

1.2.1.26 The AIE System hardware and software shall be configured for use as a distributed control system using intelligent controllers at each lane or at a single lane access control point to ensure entry control processing continues when loss of data connectivity from the network or central server is experienced.

1.2.1.27 The AIE System shall use standard communication protocols and communication links of local installations. Processors and peripherals supporting the computer resources shall be standard interface connectors and will not require proprietary links, connectors, or cables.

1.2.1.28 AIE System computers shall be state-of-the-art with processor speeds and memory sized to process the data efficiently. System shall be sustainable with minimal additional costs through the estimated life-cycle with maintenance and hardware/software upgrades.

1.2.2 Scope of Work

The design of an AIE system must be fully engineered to ensure compliance with U.S. Army regulations and standards, FIPS PUB 201-1 and all other applicable regulations and criteria. Using the standards and criteria cited in this document, the designer must prepare an AIE system specific design including the drawings, as indicated herein. The project specific drawings along with this edited performance specification must be included in the procurement documents for the AIE system. Drawings must identify the following: communications signal flow diagrams, power supply flow diagrams, entry control device locations, video camera locations, command and control workstations, central server locations, actuated gate arm locations, and incidental construction.

1.2.3 System Definitions

1.2.3.1 Access Control Activity

The centralized location for the monitoring of all access control points, traffic lanes and pedestrian portals/turnstiles with the capability of initiating law enforcement elements to respond to incidents.

1.2.3.2 Authentication

The process of establishing confidence in the validity of a person's identity.

1.2.3.3 Duress Alarm

A normally covert alarm condition which results from a set of pre-established conditions such as entering a special code into a keypad or by activating a switch indicating immediate personal danger. This alarm category shall take precedence over other alarm categories.

1.2.3.4 Entry Control Alarm

An alarm resulting from improper use of entry control procedures or equipment.

1.2.3.5 Entry Control Devices

Any equipment which gives a user the means to input identifier data into the entry control system for verification.

1.2.3.6 Environmental Alarm

A nuisance alarm resulting from environmental factors.

1.2.3.7 Error and Throughput Rates

Error and throughput rates shall be single portal performance rates obtained when processing individuals one at a time.

1.2.3.7.1 Type I Error Rate

Type I error rate is defined as an error where the system denies entry to an authorized, enrolled identifier or individual. The rate shall be less than 1 percent with a probability of correct acceptance and correct rejection of 95% at the 90% confidence level (threshold) and 99% at the 90% confidence level (objective).

1.2.3.7.2 Type II Error Rate

Type II error rate is defined as an error where the system grants entry to an unauthorized identifier or individual. The entry control Type II error rate shall be less than 0.1 percent.

1.2.3.8 Facility Interface Device

A facility interface device shall be any type of mechanism which is controlled in response to passage requests and allows passage through a portal.

1.2.3.9 False Alarm

An alarm when there is no alarm stimulus.

1.2.3.10 Fail-Safe Alarm

An alarm resulting from detection of diminished functional capabilities.

1.2.3.11 Identifier

A card credential, keypad personal identification number or code, biometric characteristic or any other unique identification entered as data into the entry control database for the purpose of verifying the identity of an individual. Identifiers shall be used by the AIE System for the purpose of validating passage requests for areas equipped with entry control equipment.

1.2.3.12 Identity Verification:

The process of confirming or refuting that a claimed identity is correct by comparing the credentials (something you know, something you have, or something you are) of a person requesting access with those previously proven and stored data in the PIV card of system that can be positively associated with the identity being claimed.

1.2.3.13 Intrusion Alarm

An alarm resulting from the detection of a specified target, attempting to intrude into the protected area or when entry into an entry-controlled area is attempted without successfully using entry control procedures.

1.2.3.14 Nuisance Alarm

An alarm resulting from the detection of an appropriate alarm stimulus, or failure to use established entry control procedures, but which does not represent an attempt to intrude into the protected area.

1.2.3.15 Passage

Ingress and/or egress past an entry control device, or through a portal. Entry control procedures and equipment shall be implemented for passage through each portal as shown.

1.2.3.16 Personal Identity Verification (PIV) Card

A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., Photograph, cryptographic keys and digitized fingerprint representation) so that the claimed identity of the card holder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable)

1.2.3.17 Portal

Specific control point, such as a door or a gate, providing entry or access from one security level to another.

1.2.3.18 Power Loss Alarm

An alarm resulting from a loss of primary power.

1.2.3.19 System Throughput

a. Traffic Lane. The AIE System shall provide a minimum throughput rate for verified/authorized vehicles and driver in automated vehicle lanes of 6 vehicles per minute per lane (threshold) with an objective of 30 vehicles per minute per lane.

b. Pedestrian Portal/turnstile. The AIE System shall provide a throughput rate of 3 (threshold) to 10 (objective) authorized personnel per minute.

1.2.3.20 Validation

The Process of demonstrating that a system, credential or individual meets in all respects, the specifications for authenticity.

1.2.3.21 Vetting

The examination and evaluation of an individual's information against multiple data sources to determine suitability for access to an installation.

1.2.4 Electrical Requirements

Electrically powered AIE equipment shall operate on 50/60 Hz AC and shall be capable or operating at a voltage of 105 to 130, 205-240, or 24 Volts. Equipment shall be able to tolerate variations in the voltage source of plus or minus 10 percent, and variations in the line frequency of plus or minus 2 percent with no degradation of performance.

1.2.5 System Reaction

1.2.5.1 System Response

Alarms shall be annunciated at the central station within 3 or less seconds of the alarm occurring at a local processor or device controlled by a local processor.

1.2.5.2 System Heavy Load Definition

For the purpose of system heavy load definition, the system shall consist of central station equipment, communication controllers and all local processors. System heavy load conditions are defined as the occurrence of entry control transactions at the rate of 6 transactions per minute per portal distributed evenly among all local processors in the system.

1.2.6 System Capacity

The system shall be comprised of scalable central servers, regional servers, monitoring stations, administrative stations, and badging stations as shown. The system shall also monitor and control the inputs and outputs shown. The system shall discriminate to the individual sensors, switches, and entry control devices and report status at the appropriate workstations as shown. This will include a minimum expansion capability of 25 percent (threshold) to 66 percent (objective) through additional software capacity, hardware capacity at the local panel level, or hardware capacity at the input module level.

1.3 SUBMITTALS

All items of computer software and technical data (including technical data which relates to computer software), which is specifically identified in this specification shall be delivered in accordance with the CONTRACT CLAUSES, SPECIAL CONTRACT REQUIREMENTS, and in accordance with the Contract Data Requirements List (CDRL), DD FORM 1423, which is attached to and thereby made a part of this contract. All data delivered shall be identified by reference to the particular specification paragraph against which it is furnished.

1.3.1 Group I Technical Data Package

The data package shall include the following as required:

1.3.1.1 System Drawings

- a. Functional System block diagram, identifying communications protocols, wire type and quantity, and approximate distances.
- b. Security Console installation, including block and wiring diagrams and equipment layout.
- c. Local processor installation, including typical block and wiring diagrams.
- d. Field equipment enclosure with local processor installation and schematics.
- e. Device wiring and installation drawings.
- f. Details of connections to power sources, including power supplies and grounding.
- g. Details of surge protection device installation.

- h. Entry control system block diagram and layout.
- i. Closed Circuit Television (CCTV) block diagram and layout.
- j. Details of interconnections with Intercom system.
- k. Details of interconnections with Security Lighting system.

1.3.1.2 Manufacturer's Data

The data package shall include manufacturer's data for all materials and equipment, including terminal devices, local processors and central station equipment provided under this specification.

1.3.1.3 System Description and Analyses

The data package shall include system descriptions, analyses, and calculations used in sizing equipment specified. Descriptions and calculations shall show how the equipment will operate as a system to meet the performance of this specification. The data package shall include the following:

- a. On-board Random Access Memory (RAM).
- b. Communication speeds and protocol descriptions.
- c. Hard disk size and configuration.
- d. CD-ROM/CD-RW/DVD/DVD-RW drive speed and protocol descriptions.
- e. Alarm response time calculations.
- f. Command response time calculations.
- g. Start-up operations including system and database backup operations.
- h. Expansion capability and method of implementation.
- i. Sample copy of each report specified.
- j. Color output of typical graphics.
- k. System throughput calculation.

The data package shall also include a table comparing the above information for the equipment supplied and the minimum required by the software manufacturer.

1.3.1.4 Software Data

The software data package shall consist of descriptions of the operation and capability of system, and application software as specified.

1.3.1.5 Overall System Reliability Calculations

The overall system reliability calculations data package shall include all manufacturer's reliability data and calculations required to show compliance with the specified reliability in accordance with paragraph, OVERALL SYSTEM RELIABILITY REQUIREMENTS.

1.3.1.6 Certifications

Specified manufacturer's certifications shall be included with the data package certification.

1.3.2 Group II Technical Data Package

A "Current Site Conditions" report shall be prepared and submitted to the Government documenting site conditions that significantly differ from the design drawings or conditions that affect performance of the system to be installed. Specification sheets, or written functional requirements to support the findings shall be provided, and a cost estimate to correct those site changes or conditions. Deficiencies shall not be corrected without written permission from the Government.

1.3.3 Group III Technical Data Package

Test procedures and reports shall be prepared for the pre-delivery test. Pre-delivery test procedures shall be based on the material contained in UFGS 28 20 01.00 10, Electronic Security System.

1.3.4 Group IV Technical Data Package

Test procedures and reports shall be prepared for the performance verification test and the endurance test. The test procedures will be based on the material contained in UFGS 28 20 01.00 10, Electronic Security System. The performance verification test and endurance test procedures will be delivered to the Government for approval.

1.3.4.1 Operation and Maintenance Manuals

Draft copies of the operator's, software, hardware, functional design, and maintenance manuals, as specified below, shall be delivered to the Government prior to beginning the performance verification test for use during the test period.

1.3.4.2 Operator's Manuals

The operator's manual shall fully explain all procedures and instructions for the operation of the system, including:

- a. Computers and peripherals.
- b. User enrollment.
- c. System start-up and shutdown procedures.
- d. Use of system and application software.
- e. Recovery and restart procedures.
- f. Graphic alarm presentation.
- g. Use of report generator and generation of reports.
- h. Data entry.
- i. Operator commands to include system operator and administrator as well as system maintenance.
- j. Alarm and system messages and printing formats.
- k. System entry requirements.

1.3.4.3 Software Manual

The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

- a. Definition of terms and functions.
- b. Use of system and application software.
- c. Procedures for system initialization, start-up and shutdown.
- d. Reports generation.
- e. Database format and data entry requirements.
- f. Directory of all disk files.

g. Description of all communication protocols, including data formats, command characters, and a sample of each type of data transfer.

h. Interface definition.

1.3.4.4 Hardware Manual: A manual describing all equipment furnished including:

a. General description and specifications.

b. Installation and checkout procedures.

c. Equipment electrical schematics and layout drawings.

d. System schematics and layout drawings.

e. Alignment and calibration procedures.

f. Manufacturer's repair parts list indicating sources of supply.

g. Interface definition.

1.3.4.5 Functional Design Manual

The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes.

1.3.4.6 Maintenance Manual

The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic prevention maintenance, fault diagnosis, and repair or replacement of defective components.

1.3.4.7 Training Documentation

Lesson plans and training manuals for the training phases, including type of training to be provided, and a list of reference material, shall be delivered for Government approval.

1.3.4.8 Data Entry

All data will be entered to make the system operational. Data will be delivered to the Government on data entry forms, utilizing data from the contract documents, field surveys, and other pertinent information required for complete installation of the database. Any additional data needed to provide a complete and operational AIE

System shall be identified and requested from the Government. The completed forms shall be delivered to the Government for review and approvals at least 30 days prior to the scheduled need date. When the AIE System database is to be populated in whole or in part from an existing or Government furnished electronic database, the field mapping scheme shall be demonstrated to correctly input the data.

1.3.4.9 Graphics

Where graphics are required and are to be delivered with the system, it will be necessary to create and install the graphics needed to make the system operational. Data shall be utilized from the contract documents, field surveys, and other pertinent information to complete the graphics. Any additional data needed to provide a complete graphics package shall be identified and requested from the Government. Graphics shall have sufficient level of detail for the system operator to assess the alarm. Hard copy, color examples at least 200 x 250 mm (8 x 10 inches) in size, of each type of graphic to be used for the completed system shall be supplied. The graphics examples shall be delivered to the Government for review and approval at least 30 days prior to the scheduled need date.

1.3.5 Group V Technical Data Package

Final copies of the manuals as specified, bound in hardback, loose-leaf binders, shall be delivered to the Government within 30 days after completing the endurance test. The draft copy used during site testing shall be updated with any changes required prior to final delivery of the manuals. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each subcontractor installing equipment and systems, and nearest service representative for each item of equipment. The manuals shall have a table of contents and tab sheets. Tab sheets shall be placed at the beginning of each chapter or section and at the beginning of each appendix. The final copies delivered after completion of the endurance test shall include modifications made during installation, checkout, and acceptance. The number of copies of each manual to be delivered shall be as specified on DDFORM 1423.

1.3.5.1 Operator's Manual

A copy of the final and approved Operator's Manual shall be provided.

1.3.5.2 Software Manual

A copy of the final and approved Software Manual shall be provided.

1.3.5.3 Hardware Manual

A copy of the final and approved Hardware Manual shall be provided.

1.3.5.4 Functional Design Manual

A copy of the final and approved Functional Design Manual shall be provided.

1.3.5.5 Maintenance Manual

A copy of the final and approved Maintenance Manual shall be provided.

1.3.5.6 Final System Drawings

A separate set of drawings, elementary diagrams and wiring diagrams of the system shall be maintained to be used for final system drawings. This set shall be accurately kept up-to-date with all changes and additions to the AIE System and shall be delivered to the Government with the final endurance test report. In addition to being complete and accurate, this set of drawings shall be kept neat and shall not be used for installation purposes. Final drawings submitted with the endurance test report shall be finished drawings on CD-ROM in [Microstation Version 8] [AutoCAD 2002 or later] format.

1.4 TESTING

1.4.1 General

Pre-delivery testing, site performance verification testing, endurance testing and adjustment of the completed AIE System shall be performed. Personnel, equipment, instrumentation, and supplies necessary to perform testing shall be provided. Written notification of planned testing shall be given to the Government at least 14 days prior to the test; notice shall not be given until has received written approval of the specific test procedures.

1.4.2 Test Procedures and Reports

Test procedures shall explain in detail, step-by-step actions and expected results, demonstrating compliance with the requirements specified. Test reports shall be used to document results of the tests. Reports shall be delivered to the Government within 7 days after completion of each test.

1.5 TRAINING

1.5.1 General

Training courses shall be conducted for designated personnel in the maintenance and operation of the system as specified. The training shall be oriented to the specific system being installed. Training manuals shall be delivered for each trainee with 2 additional copies delivered for archiving at the project site. The manuals shall include an agenda, defined objectives for each lesson, and a detailed description of the subject matter for each lesson. Audio-visual equipment and other training materials and supplies shall be furnished. Portions of the course by which audio-visual material is used, copies of the audio-visual material shall be delivered to the Government either as a part of the printed training manuals or on the same media as that used during the training sessions. A training day is defined as 8 hours of classroom instruction, including 2 15-minute breaks and excluding lunchtime, Monday through Friday, during the daytime shift in effect at the training facility. For guidance in planning the required instruction, it will be assumed that all attendees will have a high school education or equivalent, and are familiar with AIE System. Approval of the planned training schedule shall be obtained from the Government at least 30 days prior to the training.

1.5.2 Operator's Training

The first course shall be taught at the project site for a minimum period of two consecutive training days at least 1 month prior to the scheduled performance verification test. A maximum of 12 personnel shall attend this course. Upon completion of this course, each student, using appropriate documentation, shall be able to perform elementary operations with guidance and describe the general hardware architecture and functionality of the system. This course shall include:

- a. General System hardware architecture
- b. Functional operation of the system
- c. Operator commands
- d. Data base entry
- e. Reports generation
- f. Alarm reporting
- g. Diagnostics

1.5.3 System Administrator Training

All system managers shall be trained for at least 3 consecutive days. The system manager training shall consist of the operator's training and the following:

- a. Enrollment/deactivation
- b. Assignments of identifier data
- c. Assign operator password/levels
- d. Change database configuration
- e. System network configuration and management
- f. Modify graphics
- g. Print special or custom reports
- h. System backup
- i. Any other functions necessary to manage the system

1.5.4 Maintenance Personnel Training

The system maintenance course shall be taught at the project site during or after the field testing, but before commencing the performance verification test for a period of 5 training days. A maximum of 5 personnel, designated by the Government, will attend the course. Upon completion of this course, the students shall be fully proficient in the maintenance of the system. The training shall include:

- a. Physical layout of each piece of hardware
- b. Troubleshooting and diagnostics procedures
- c. Component repair and/or replacement procedures
- d. Maintenance procedures and schedules to include system testing after repair
- e. Calibration procedures
- f. Review of site-specific drawing package, device location, communication, topology, and flow

1.6 MAINTENANCE AND SERVICE

1.6.1 Warranty

All labor, equipment, and materials required to maintain the entire system in an operational state as specified shall be provided, for a period of one year after formal written acceptance of the system to include scheduled and nonscheduled adjustments.

1.6.2 Description of Work

The adjustment and repair of the system includes all computer equipment, software updates, communications transmission equipment and data transmission system (DTS), local processors, sensors and entry control, facility interface, and support equipment. Responsibility shall be limited to Contractor installed equipment. Repair, calibration, and other work shall be provided and performed in accordance with the manufacturer's documentation and instruction.

1.6.3 Personnel

Service personnel shall be certified in the maintenance and repair of the specific type of equipment installed and qualified to accomplish work promptly and satisfactorily. The Government shall be advised in writing of the name of the designated service representative, and of any change in personnel.

1.6.4 Schedule of Work

Two minor inspections at 6 month intervals shall be performed (or more often if required by the manufacturer), and two major inspections offset equally between the minor inspections to effect quarterly inspection of alternating magnitude.

1.6.4.1 Minor Inspections

Minor inspections shall include visual checks and operational tests of console equipment, peripheral equipment, local processors, sensors, and electrical and mechanical controls. Minor inspections shall also include mechanical adjustment of laser printers.

1.6.4.2 Major Inspections

Major inspections shall include work described under paragraph 1.6.4.1, Minor Inspections, and the following work:

- a. Clean interior and exterior surfaces of all system equipment and local processors, including workstation monitors, keyboards, and console equipment

- b. Perform diagnostics on all equipment
- c. Run all system software diagnostics and correct all diagnosed problems
- d. Resolve any previous outstanding problems
- e. Purge and compress data bases
- f. Review network configuration

1.6.4.3 Scheduled Work

Scheduled work shall be performed during regular working hours, Monday through Friday, excluding federal holidays.

1.6.5 Emergency Service

The Government will initiate service calls when the system is not functioning properly. Qualified personnel shall be available to provide service to the complete system. The Government shall be furnished with a telephone number where the service supervisor can be reached at all times. Service personnel shall be at site within 4 hours after receiving a request for service. The system shall be restored to proper operating condition within 8 hours after service personnel arrive onsite and obtain access to the system.

1.6.6 Operation

Performance verification test procedures shall be used after all scheduled maintenance and repair activities to verify proper component and system operation.

1.6.7 Records and Logs

Records and logs of each task shall be kept, shall chronologically organize cumulative records for each component and for the complete system resulting in a continuous log to be maintained for all devices. The log shall contain all initial settings. Complete logs shall be kept and shall be available for inspection onsite, demonstrating that planned and systematic adjustments and repairs have been accomplished for the system.

1.6.8 Work Requests

Each service call request shall be separately recorded, as received. The form shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing what has to be done, the amount and nature of the material to be used, the time and date work started, and the time and

date of completion. A record of the work performed within 5 days after work is accomplished shall be delivered.

1.6.9 System Modifications

Any recommendations for system modification shall be made in writing to the Government. System modifications shall not be made without prior approval of the Government. Any modifications made to the system shall result in the updating of the operation and maintenance manuals as well as any other documentation affected.

1.6.10 Software

A description of all software updates to the Government shall be provided, who will then decide whether or not they are appropriate for implementation. After notification by the Government, the designated software updates shall be implemented and then verified operational in the system. These updates shall be accomplished in a timely manner, fully coordinated with system operators, and shall be incorporated into the operation and maintenance manuals, and software documentation. A system image file shall be made so the system can be restored to its original state if the software update adversely affects system performance.

1.7 DATA TRANSMISSION SYSTEM (DTS)

1.7.1 Data Transmission System (DTS) Line Supervision

All signal and DTS lines shall be supervised by the system. The system shall supervise the signal lines by monitoring the circuit for changes or disturbances in the signal and for conditions as described in UL 1076 for line security equipment. The system shall initiate an alarm in response to a current change of 5 percent or greater. The system shall also initiate an alarm in response to opening, closing, shorting, or grounding of the signal and DTS lines.

1.7.2 Data Encryption

The system shall incorporate data encryption equipment on data transmission circuits.. The algorithm used for encryption shall be the Advanced Encryption Standard (AES) algorithm described in FIPS PUB 197.

1.8 INFORMATION ASSURANCE

The AIE System shall provide for user authentication security, including strong authentication, non-repudiation, and personal identification, in accordance with Section 4 of DoDI 8500.1. Verification, administration and critical system setup and configuration functions in the system shall be protected from tampering by unauthorized users. If the system processes or stores information protected under the Privacy Act of 1974, the system shall conform to the notification and other requirements in accordance with the provisions of DoD Directive 5400.11. The system shall provide for protection of all Privacy Act protected data during transmission over any network and storage in any server and database. In addition, the system shall provide for protection of all Privacy Act protected data during transmission over any network and storage in any server and database.

1.9 DATA CURRENCY AND INTEGRITY

The AIE System shall maintain currency of data among the system components across a physical installation to the extent possible with available network connectivity. All data shall be checked for consistency prior to being stored to eliminate duplicate or contradictory information and all stored data shall be capable of verification using checksum or other consistency methods. Critical system setup and configuration functions in the software shall be protected from tampering by unauthorized users.

PART 2 PRODUCTS

2.1 MATERIALS

2.1.1 Commercial Off-The-Shelf (COTS) and Non-Developmental Items (NDI)

To the extent possible, the components for this system will be COTS equipment or NDI.

2.1.2 Materials and Equipment

Units of equipment that perform identical, specified functions shall be products of a single manufacturer. All material and equipment shall be new and currently in production. Each major component of equipment shall have the manufacturer's

model and serial number in a conspicuous place. System equipment shall conform to UL 294.

2.1.3 Field Enclosures

2.1.3.1 Interior Devices

Devices to be used in an interior environment shall have a housing that provides protection against dust, falling dirt, and dripping non-corrosive liquids.

2.1.3.2 Exterior Devices

Devices to be used in an exterior environment shall have a housing that provides protection against windblown dust, rain and splashing water, and hose directed water. Devices shall be undamaged by the formation of ice on the enclosure.

2.1.3.3 Interior Electronics

Systems electronics to be used in an interior environment will be housed in enclosures which meet the requirements of NEMA 250 Type 12.

2.1.3.4 Exterior Electronics

Systems electronics to be used in an exterior environment shall be housed in enclosures which meet the requirements of NEMA 250 Type 4X.

2.1.3.5 Corrosion Resistant

System electronics to be used in a corrosive environment as defined in NEMA 250 shall be housed in non-metallic non-corrosive enclosures which meet the requirements of NEMA 250 Type 4X.

2.1.4 Nameplates

Nameplates shall be provided for major components of the system. Nameplates shall have the manufacturer's name, address, type or style, model or serial number, and catalog number on a corrosion resistant plate secured to the item of equipment. Nameplates will not be required for devices smaller than 25 x 75 mm 1 x 3 inches.

2.1.5 Fungus Treatment

System components located in fungus growth inductive environments shall be completely treated for fungus resistance. Treating materials containing a mercury bearing fungicide shall not be used. Treating materials shall not increase the flammability of the material or surface being treated. Treating materials shall cause no skin irritation or other injury to personnel handling it during fabrication,

transportation, operation, or maintenance of the equipment, or during use of the finished items when used for the purpose intended.

2.1.6 Tamper Switches

Equipment enclosures for the AVBCS, ESS, and the active vehicle barrier shall have hinged doors or removable covers. The doors or covers shall be provided with cover operated, corrosion-resistant tamper switches, arranged to initiate an alarm signal when the door or cover is moved. Tamper switches shall be three-position push-pull type. The enclosure and the tamper switch shall function together and shall not allow direct line of sight to any internal components before the switch activates. Tamper switches shall be 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; be connected to circuits which are under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating; shall be spring-loaded and held in the closed position by the door or cover; and shall be wired so that the circuit is broken when the door or cover is disturbed.

2.1.7 Locks and Key-Lock Switches

2.1.7.1 Locks

Locks shall be provided on system enclosures for maintenance purposes. Locks shall be UL listed, [round-key type with 3 dual, 1 mushroom, 3 plain pin tumblers] [or] [conventional key type lock having a combination of 5 cylinder pin and 5-point 3 position side bar]. Keys shall be stamped "U.S. GOVT. DO NOT DUP." The locks shall be arranged so that the key can only be withdrawn when in the locked position. Maintenance locks shall be keyed alike and only 2 keys shall be furnished for all of these locks. These keys shall be controlled in accordance with the key control plan as specified in paragraph Key Control Plan.

2.1.7.2 Key-Lock-Operated Switches

Key-lock-operated switches required to be installed on system components shall be UL listed, [round-key type, with 3 dual, 1 mushroom, and 3 plain pin tumblers] [or] [conventional key type lock having a combination of 5 cylinder pin and 5-point 3 position side bar]. Keys shall be stamped "U.S. GOVT. DO NOT DUP." Key-lock-operated switches shall be two positions, with the key removable in either position. All key-lock-operated switches shall be keyed differently and only 2 keys shall be furnished for each key-lock-operated-switch. Keys shall be removable in the positions described in these specifications or as shown on the drawings. Keys shall be controlled in accordance with the key control plan as specified in paragraph Key Control Plan.

2.1.7.3 Construction Locks

A set of temporary locks shall be used during installation and construction. The final set of locks installed and delivered to the Government shall not include any of the temporary locks.

2.2 SYSTEM COMPONENTS

System components shall be designed for continuous operation. Electronic components shall be solid state type, mounted on printed circuit boards conforming to UL 796. Printed circuit board connectors shall be plug-in, quick-disconnect type. Power dissipating components shall incorporate safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current carrying capacity. Control relays and similar switching devices shall be solid state type or sealed electro-mechanical.

2.2.1 Modularity

Equipment shall be designed for increase of system capability by installation of modular components. System components shall be designed to facilitate maintenance through replacement of modular subassemblies and parts.

2.2.2 Maintainability

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. There shall be no degradation in tamper protection, structural integrity, EMI/RFI attenuation, or line supervision after maintenance when it is performed in accordance with manufacturer's instructions.

2.2.3 System Overall Reliability Requirement

2.2.3.1 Mean Time Between Failure

The system, including components and appurtenances, shall be configured and installed to yield a mean time between failure (MTBF) of at least 1,440 hours.

2.2.3.2 Mean Time Between Critical Failure

AIE System modules, gates and portals shall operate continuously and yield a minimum mean time between critical failures (MTBCF) of 10,000 hours. A critical failure is defined as a failure that renders a vehicle lane or pedestrian portal unusable.

2.2.3.3 Operational Availability

Operational availability (Ao) is the probability that a system or equipment, when used under stated conditions in an actual operational environment, will operate satisfactorily when called upon. The AIE system shall have a minimum Ao of 97% per module, gate and portal allowing time for preventive maintenance and training, and potential power outages with an objective Ao of 99% per module, gate and portal. Ao is expressed as mean time between downing events (MTBDE) divided by the sum of MTBDE and mean down time (MDT). MTBDE is the average time between events that bring the system down, including critical or non-critical failures, preventive maintenance, and training. MDT is the average total elapsed time to fully restore the system/subsystem to an operational state as a result of a downing event. It includes active maintenance time, logistics delay time, and administrative delay time.

$$Ao = \text{MTBDE} \div (\text{MTBDE} + \text{MDT})$$

2.2.4 Interchangeability

The system shall be constructed with off-the-shelf components which are physically, electrically and functionally interchangeable with equivalent components as complete items. Replacement of equivalent components shall not require modification of either the new component or of other components with which the replacement items are used. Custom designed or one-of-a-kind items shall not be used without explicit approval from the Contracting Officer. Interchangeable components or modules shall not require trial and error matching in order to meet integrated system requirements, system accuracy, or restore complete system functionality.

2.2.5 Product Safety

System components shall conform to applicable rules and requirements of NFPA 70. System components shall be equipped with instruction plates including warnings and cautions describing physical safety and any special or important procedures to be followed in operating and servicing system equipment.

2.2.6 Wire and Cable

All wire and cable not indicated as Government furnished equipment shall be provided. Wiring shall meet NFPA 70 standards. All cable components shall withstand the environment in which the cable is installed for a minimum of 20 years.

2.2.7 Power Line Surge Protection

Equipment connected to AC power shall be protected from surges. Equipment protection shall withstand surge test waveforms described in IEEE C62.41. Fuses shall not be used for surge protection.

2.2.8 Device Wiring and Communications Line Surge Protection

Cables and conductors, except fiber optic cables, which serve as communication, control, or signal lines shall be protected against surges and shall have surge protection provided at each end. Protection shall be provided at the equipment and additional triple electrode gas surge protectors rated for the application on each wireline circuit shall be installed within 1m (3 feet) of the building cable entrance. Fuses shall not be used for surge protection. The inputs and outputs shall be tested in both normal mode and common mode using the following waveforms:

2.2.8.1 A 10 microsecond rise time by 1000 microsecond pulse width waveform with a peak voltage of 1500 volts and a peak current of 60 amperes.

2.2.8.2 An 8 microsecond rise time by 20 microsecond pulse width waveform with a peak voltage of 1000 volts and a peak current of 500 amperes.

2.2.9 Power Line Conditioners

A power line conditioner shall be provided for the security console equipment. The power line conditioner used for the equipment shall be the same one as provided for in UFGS 28 20 01.00 10, Electronic Security System. The power line conditioner shall be of the Ferro resonant design, with no moving parts and no tap switching, while electrically isolating the secondary from the power line side. The power line conditioner shall be sized for 125 percent of the actual connected kVA load.

Characteristics of the power line conditioner shall be as follows:

2.2.9.1 At 85 percent load, the output voltage shall not deviate by more than plus or minus 1 percent of nominal when the input voltage fluctuates between minus 20 percent to plus 10 percent of nominal.

2.2.9.2 During load changes of zero to full load, the output voltage shall not deviate by more than plus or minus 3 percent of nominal. Full correction of load switching disturbances shall be accomplished within 5 cycles, and 95 percent correction shall be accomplished within 2 cycles of the onset of the disturbance.

2.2.9.3 Total harmonic distortion shall not exceed 3-1/2 percent at full load.

2.2.10 Uninterruptible Power Supplies (UPS)

2.2.10.1 Provide an UPS to supply power to the AIE System in the event of a loss of normal electrical power. Upon loss of normal power, the UPS shall be capable of carrying designated loads for the duration of time required for the Emergency Power Back-up source (e.g., Diesel Generator) to start, come on line, and pick-up 100% of its load. The UPS shall provide critical components with a minimum of six hours of operating power. Critical components include:

- a. Host Servers
- b. Client Servers
- c. Local processors
- d. Credential readers
- e. Video cameras
- f. Traffic control arms
- g. Guard booth equipment

2.2.10.3 Calculations for all proposed UPS systems shall be submitted identifying all connected loads plus 50% spare capacity and submit in accordance with Section 1.3.1 Group I – Technical Data Package.

2.2.11 Environmental Conditions

2.2.11.1 Nuclear, Biological, Chemical Environment

The AIE System is not expected to survive a nuclear attack or the effects resulting from Electromagnetic Pulse (EMP) events. All exterior components shall be resistant to the effects of chemicals and vapors sometimes present in the conduct of base operations (e.g., gasoline, engine oil, diesel fuel, hydraulic fluid, ammonia, paint thinner and other potentially corrosive agents) and to the effects of chemicals used in winter road maintenance (e.g., salt and other deicer chemicals).

2.2.11.2 Interior, Controlled Environment

System components, except the console equipment installed in interior locations having controlled environments, shall be rated for continuous operation under ambient environmental conditions of 2 to 50 degrees C 36 to 122 degrees F dry bulb and 20 to 90 percent relative humidity, non-condensing.

2.2.11.3 Console

Console equipment, unless designated otherwise, shall be rated for continuous operation under ambient environmental conditions of 2 to 50 degrees C (36 to 122 degrees F) and a relative humidity of 20 to 80 percent.

2.2.11.4 Interior, Uncontrolled Environment

System components installed in interior locations having uncontrolled environments shall be rated for continuous operation under ambient environmental conditions of -18 to plus 50 degrees C 0 to 122 degrees F dry bulb and 10 to 95 percent relative humidity, non-condensing.

2.2.11.5 Exterior Environment

System components that are installed in locations exposed to weather shall be rated for continuous operation under ambient environmental conditions of -34 to plus 50 degrees C (-30 to plus 122 degrees F) dry bulb and 10 to 95 percent relative humidity, condensing. Components shall be rated for continuous operation when exposed to rain as specified in NEMA 250, winds up to 137 km/hr (85 mph) and snow cover up to 610 mm (2 feet thick), measured vertically.

2.2.11.6 Precipitation

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

2.2.11.7 Icing

All components shall be operable in icing conditions.

2.2.11.8 Sunlight

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

2.2.11.9 Ruggedness

Systems 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.

2.2.12 AIE System Devices and Equipment

2.2.12.1 Enrollment and Badging Equipment

Enrollment stations shall be provided and located to enroll personnel into, and remove personnel from the system database. The enrollment equipment shall only be accessible to authorized personnel. Credential cards/RFID tags shall be provided to enroll all personnel and vehicles at the site plus an additional amount equal to three months usage based on COPS/VRS data. The enrollment equipment shall include subsystem configuration controls and electronic diagnostic aids for subsystem set-up and troubleshooting with the central station.

The enrollment and badging function shall:

- a. Register authorized personnel and vehicles (permanent party, installation employees, visitors and commercial vendors).
- b. Enable the unique enrollment of at least 40,000 (scalable up to 250,000) personal information records.
- c. Capture, retrieve and store a digital picture and signature of the personnel being registered.
- d. Provide a capability for base affiliated personnel to initiate a self-entering sequence of their personal information and vehicular information. All data input will be independently verified by a system operator during the completion of the enrollment process.
- e. Allow base-affiliated personnel to sponsor visitors. In a stand-alone configuration, this is a manual process. If an enterprise configuration is deployed, this is accomplished from a sponsor's workstation.
- f. Print and issue both paper vehicle passes that contain the visitor's name, photograph, sponsor's name, sponsor's phone number and bar code and plastic ID visitor badges that contain the vehicle operator's name, photograph, sponsor's name, sponsor's phone number and bar code.
- g. Provide both manual and automated verification that the issued credentials function properly and the database entries are correct.
- h. Issue credentials and RFID tags for vehicles of authorized, base-affiliated personnel.

2.2.12.2 Credentials

Credentials shall be FIPS PUB 201-1 compliant. The AIE System shall, as a minimum, interface with and use the CAC, the DD Form 2 (retiree ID card), the DD Form 1173 (dependent ID card) and FIPS PUB 201-1 Compliant Personal Identification Verification (PIV) Cards.

2.2.12.3 Credential Readers

Credential readers shall be combination credential reader and keypad device. Keypad shall accept input of individual PINs associated with the CAC for authentication. Although normally anticipated usage will be during high FPCON levels, the keypad devices shall be configured such that their use can be implemented on a random basis as directed by the Installation Commander or his designated representative.

Credential readers shall, at a minimum, read all credentials produced by the AIE System enrollment and badging equipment, the CAC, the DD Form 2 (retiree ID card), the DD Form 1173 (dependent ID card) and the FIPS PUB 201-1 Compliant PIV Cards.

Readers shall incorporate built-in heaters or other cold weather equipment to extend the operating temperature range as needed for operation at the site.

Communications protocol shall be compatible with the local processor.

Credential readers shall be capable of separate maintenance, upgrade and augmentation without major modification to the AIE System.

Readers shall minimize processing and recognition time and provide maximum flexibility in presentation angle and orientation so as not reduce traffic throughput rates.

The AIE System shall include credential reading equipment for vehicle lanes, pedestrian lane and separately positioned hand-held devices for use by security personnel.

a. Vehicle Lane Reader

Vehicle lane reading stations shall be positioned to provide adequate clearance for standard passenger, commercial and military vehicles and their drivers to be verified prior to reaching security personnel. Vehicle lane reading stations shall not read vehicle credentials in adjacent lanes.

b. Wireless hand-held Reader

Wireless readers shall be provided for use by security personnel, external to the gatehouse and guard booths. Readers shall be capable, at a minimum, of reading a finger print and all credentials recognized by the system including paper vehicle passes. Readers shall operate in all weather conditions, provide controls that are simple to use and provide a clear and legible display to operators in all lighting levels. Readers shall be rechargeable and operate for a minimum of 12-hours following a single charge. Readers shall provide the capability for operating and recharging from vehicle 12VDC and 24VDC power supplies.

c. Reader Display

All credential readers shall provide a visual and auditory feedback when credential reading equipment has successfully read personal and vehicle credentials. Readers shall include an LED or other type of visual indicator display and provide visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the display or reader enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus 5 degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

d. Reader Power

Readers shall be powered from the source as shown and shall not dissipate more than 5 Watts.

e. Reader Mounting Method

Readers shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.

f. Duress Codes

Readers shall provide a means for users to indicate a duress situation by entering a special code.

2.2.12.4 Fingerprint Reader

The AIE System shall include means to collect individuals' fingerprints (2 (threshold) to 10 (objective)). Features will be extracted from each of these individual prints to form its corresponding template. This template shall be part of the enrollees PIR.

The stored template shall be used as a basis for comparison to a live fingerprint collected by the fingerprint reader to identify authorized or enrolled personnel and to either allow or prohibit access to installations. The design of this device shall incorporate positive measures to establish that the hand being scanned is live and the proper fingerprint format is being collected. The fingerprint reader shall automatically initiate the collection process upon proper positioning of the hand. Each fingerprint template shall not require more than 1250 bytes of storage media space. Fingerprint readers shall include an LED or other type of visual display to provide visual and audible status indications, user prompts, match or no-match status, and power on/off status. Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000 and be certified interoperable with the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS).

a. Template Update and Acceptance Tolerances. Fingerprint readers shall not automatically update a user's profile. Significant changes in an individual's fingerprints shall require re-enrollment. The fingerprint readers shall provide an adjustable acceptance tolerance or template match criteria under system administrator or operator control. The fingerprint reader shall determine when multiple attempts are needed for fingerprint verification, and shall automatically prompt the enrollee for additional attempts up to a maximum of 3. Three failed attempts shall generate an entry control alarm.

b. Average Verification Time. The fingerprint reader shall respond to passage requests by generating signals to the local processor. The verification time shall be 2.0 seconds or less from the moment the fingerprint reader initiates the scan process until the fingerprint reader generates a response signal.

c. Modes. The fingerprint reader shall provide an enrollment mode, recognition mode, and code/credential verification mode. The enrollment mode shall create a fingerprint template for new personnel and enter the template into the system database file created for that person. Template information shall be compatible with the system application software. The operating mode shall be selectable by the system administrator from the central server. When operating in recognition mode, the fingerprint reader shall allow passage when the fingerprint data from the verification attempt matches a fingerprint template stored in the database files. When operating in code/credential verification mode, the fingerprint reader shall allow passage when the fingerprint data from the verification attempt matches the fingerprint template associated with the identification code entered into a keypad or matches the fingerprint template associated with credential data read by a card reader.

d. Mounting Method. Fingerprint analysis scanners shall be suitable for surface, flush, or pedestal mounting as required.

e. Communications Protocol. The communications protocol between the fingerprint reader and its associated local processor shall be compatible.

2.12.5 Entry Control Local Processor

The entry control local processor shall respond to interrogations from the field device network, recognize and store status inputs until they are transmitted to the central server and change outputs based on commands received from the central server. The local processor shall also be capable of automatically restoring communication within 10 seconds after an interruption with the field device network that is internal to the AIE and is a result of an event other than a failure and provide line supervision on each of its inputs.

The entry control local processor shall provide local entry control functions including communicating with field devices such as card readers, keypads, biometric personal identity verification devices, and gate arm operators. Processors shall accept data from entry control field devices as well as database downloads and updates from the central server that include enrollment and privilege information. Processors shall send indications of success or failure of attempts to use entry control field devices and make comparisons of presented information with stored identification information.

The processor shall grant or deny entry by sending control signals to portal control devices and mask intrusion alarm annunciation from sensors stimulated by authorized entries. The local processor shall maintain a date-time and location stamped record of each transaction and transmit transaction records to the central server. The processor shall operate as a stand-alone portal controller using the downloaded database during periods of communication loss between the local processor and the central server. The processor shall store a minimum 4000 transactions during periods of communication loss between the local processor and the central server for subsequent upload to the central server upon restoration of communication.

a. Inputs. Local processor inputs shall monitor dry contacts for changes of state that reflect alarm conditions. The local processor shall have at least 8 alarm inputs which allow wiring as normally open or normally closed contacts for alarm conditions. It shall also provide line supervision for each input by monitoring each input for abnormal open, grounded, or shorted conditions using DC current change measurements. The local processor shall report line supervision alarms to the central station. Alarms shall be reported for any condition that remains off normal at an input for longer than 500 milliseconds. The entry control local processor shall include the necessary software drivers to communicate with entry control field devices. Information generated by the entry control field devices shall be accepted by the local processor and automatically processed to determine valid identification of the individual present at the portal. Upon authentication of the credentials or information presented, the local processor shall automatically check privileges of the

identified individual, allowing only those actions granted as privileges. Privileges shall include, but not be limited to, time of day control, day of week control, FPCON level access, group control, and visitor escort control. The local processor shall maintain a date-time and location stamped record of each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

b. Outputs. Local processor outputs shall reflect the state of commands issued by the central server. The outputs shall be a form C contact and shall include normally open and normally closed contacts. The local processor shall have at least 4 addressable outputs. The entry control local processor shall also provide control outputs to portal control devices.

c. Communications. The local processor shall be able to communicate with the central server via RS485 or TCP/IP as a minimum. The time for downloading information for panel configurations and cardholder data when using IP connectivity shall be minimized.

2.2.13 Actuated Traffic Arms

Traffic arms in the ID Check Area shall be controlled by control switches in the Guard Booths. Lowering of the traffic arm shall take no more than one (1) second in all required environmental conditions. Raising of the traffic arm shall take no more than three (3) seconds in all required environmental conditions. If a vehicle crashes into the traffic arm when it is in the down position, the AIE System shall generate a signal (contact open/close) capable of indicating alarm conditions to remote workstations.

2.2.13.1 Traffic Arm Assembly

The housing for the traffic arm controller shall be weather proof and constructed of stainless steel not less than 14 gauge, carbon steel not less than 3 mm 1/8 inch thick, or cast steel not less than 6 mm 1/4 inch thick. All seams, joints, and supports shall be electric bead welded. Access to the motor compartment shall be provided with a removable cover secured in a weather proof manner with a lock. 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. The assembly shall be capable of a minimum of 500 duty cycles per hour. A motor of at least 1/3 HP shall be used to power the system. The traffic arm assembly shall consist of a hollow aluminum assembly, wood, steel or fiberglass material with a length of nine (9) feet. Provide a spare arm for each traffic arm assembly. The traffic arm shall be covered with retro reflective red and white sheeting. See FHWA SA-89-006 for proper orientation of sheeting. Each traffic arm shall be equipped with an obstruction detector that will automatically reverse the traffic arm motor when an obstruction is detected. The assembly shall be capable of manual override

operation in the event of a malfunction due to mechanical failure, main power outage, and/or backup power supply failure.

2.2.14 Closed Circuit Television (CCTV) System

The CCTV system shall provide video assessment and surveillance for presentation of critical video images to ACP guards and for storage of video data for incident reporting and future evaluation by security personnel. The CCTV equipment shall provide continuous color video imagery showing personnel and vehicles entering and exiting the ACP. The CCTV system shall make video data available for remote monitoring and recording. Video from the CCTV system shall be stored in a manner that allows it to be admissible as evidence in a court of law and shall be downloadable to backup storage media. The CCTV system shall meet the requirements listed in Section 28 23 23.00 10 CLOSED CIRCUIT TELEVISION SYSTEMS, and the following:

a. The CCTV system shall provide at least one camera in each vehicle lane mounted and focused to enable the reading of rear-mounted, vehicle license plates.

b. The CCTV system shall provide at least one camera in each vehicle lane and at each pedestrian entry portal mounted and focused to provide identification level resolution video of each individual processing through the AIE System onto the installation. Identification resolution is defined as producing images that allow a system operator to identify a person by distinguishing specific individual features on that person such as the detailed shape of the eyes, ears, nose, mouth, and chin.

c. The CCTV system shall provide surveillance of the ACP areas shown on the drawings. For surveillance, the cameras and CCTV system shall operate full time to monitor the required ACP areas

d. The CCTV system shall provide video assessment of entry control, tamper, and duress alarms. For assessment, the appropriate camera or cameras shall automatically focus on the alarmed area and the CCTV system shall automatically display the camera image to the operator's monitor when an alarm is activated.

e. CCTV monitoring and controls shall be included in the gatehouse control console to provide monitoring and display control of live CCTV images from any ACP camera. The CCTV subsystem shall also provide controls to display and view recorded video imagery.

f. The CCTV system shall provide digital video recording of all ACP video imagery cameras 24 hours per day, seven (7) days per week and retain all images for 7 days. The CCTV system shall be capable of storing up to 180 days of video information related to events that required the intervention of the gate guard and/or response by law enforcement personnel.

g. The camera located on the pedestal in the entry control lane that contains the ID presentation devices will record images of the vehicle operator at a rate of 5 frames per second for two seconds as the ID credential is presented to the credential reader.

g. Provide an interface with the installation central monitoring stations to allow the central station to monitor live CCTV images from any ACP camera or recorded images.

PART 3 EXECUTION

3.1 GENERAL REQUIREMENTS

All system components shall be installed, including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions, IEEE C2 and as shown. Interconnections, services, and adjustments required for a complete and operable system shall be furnished as specified and shown. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.

3.1.1 Installation

The system shall be installed in accordance with the standards for safety, NFPA 70, UL 681, UL 1037 and UL 1076, and the appropriate installation manual for each equipment type. Components within the system shall be configured with appropriate service points to pinpoint system trouble in less than 20 minutes. Conduit shall be rigid galvanized steel or as shown and a minimum of 15 mm 1/2 inch in diameter. DTS shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring. Flexible cords or cord connections shall not be used to supply power to any components of the system, except where specifically noted.

3.1.2 Enclosure Penetrations

Enclosure penetrations shall be from the bottom unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer, and in a manner that does not damage the cable.

3.1.3 Cold Galvanizing

Field welds and/or brazing on factory galvanized boxes, enclosures, conduits, etc., shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

3.1.4 Current Site Conditions

All site conditions shall be verified in agreement with the design package. Any changes in the site, or conditions that will affect performance of the system shall be reported to the Government in a report as defined in paragraph Group II Technical Data Package. No corrective action shall be taken without written permission from the Government.

3.1.5 Existing Equipment

Existing equipment, DTS, and other such devices as shown shall be connected to and utilized. System equipment and DTS that are usable in their original configuration without modification may be reused with Government approval. A field survey shall be performed, including testing and inspection of all existing system equipment and DTS intended to be incorporated into the system, and furnish a report to the Government as part of the site survey report as defined in paragraph Group II Technical Data Package. For those items considered nonfunctioning, the report shall include specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the scheduled need date shall be included for connection to all existing equipment. Written requests shall be made and approval obtained prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Government approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the failure shall be diagnosed and any necessary corrections shall be performed to his equipment and work. The Government is responsible for maintenance and the repair of Government equipment. Responsibility for repair costs due to negligence or abuse of Government equipment shall be put on the Contractor.

3.1.6 Installation of Software

Software shall be loaded as specified and required for an operational system, including data bases and specified programs. Upon successful completion of the endurance test, any original and backup copies on CD-ROM of all accepted software shall be provided, including diagnostics.

3.2 SYSTEM STARTUP

Satisfaction of the requirements below does not relieve the Contractor of responsibility for incorrect installations, defective equipment items, or collateral damage as a result of Contractor work/equipment. Power to the system shall not be applied until after:

a. System equipment items and DTS have been set up in accordance with manufacturer's instructions.

b. A visual inspection of the system has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.

c. System wiring has been tested and verified as correctly connected.

d. System grounding and transient protection systems have been verified as properly installed.

e. Power supplies to be connected to the system have been verified as the correct voltage, phasing, and frequency.

3.3 SUPPLEMENTAL CONTRACTOR QUALITY CONTROL

Technical representatives who are familiar with all components and installation procedures of the installed system shall provide the necessary support services; and are approved by the Contracting Officer. These representatives shall be present on the job site during the preparatory and initial phases of quality control to provide technical assistance. These representatives shall also be available on an as needed basis to provide assistance with follow-up phases of quality control. These technical representatives shall participate in the testing and validation of the system and shall provide certification that their respective system portions meet the contractual requirements.

3.4 TESTING

3.4.1 General Requirements for Testing

Personnel, equipment, instrumentation, and supplies necessary to perform site testing shall be provided. The Government will witness all performance verification and endurance testing. Written permission shall be obtained from the Government before proceeding with the next phase of testing. Original copies of all data

produced during pre-delivery, performance verification and endurance testing shall be turned over to the Government at the conclusion of each phase of testing, prior to Government approval of the test.

3.4.2 Pre-delivery Testing

3.4.2.1 The test system shall be assembled as specified, and perform tests to demonstrate that performance of the system complies with specified requirements in accordance with the approved pre-delivery test procedures. The tests shall take place during regular daytime working hours on weekdays. Model numbers of equipment tested shall be identical to those to be delivered to the site. Original copies of all data produced during pre-delivery testing, including results of each test procedure, shall be delivered to the Government at the conclusion of pre-delivery testing, prior to Government approval of the test. The test report shall be arranged so that all commands, stimuli, and responses are correlated to allow logical interpretation.

3.4.2.2 Test Setup: The pre-delivery test setup shall include the following:

- a. All gatehouse, guard booth and visitor control center equipment.
- b. At least 1 of each type DTS link, but not less than 2 links, and associated equipment to provide a fully integrated system.
- c. The number of local processors shall equal the amount required by the site design.
- d. At least 1 of each type entry control device used.
- e. Sufficient simulators to provide alarm signal inputs to the system equal to the number of entry control devices required by the design. The alarm signals shall be manually or software generated.
- f. At least 1 of each type of portal configuration with all facility interface devices as specified or shown.
- g. Equipment as specified in Section 28 23 23.00 10 CLOSED CIRCUIT TELEVISION SYSTEMS, when required.
- h. Test procedures and reports shall be prepared for the pre-delivery test, and shall deliver the pre-delivery test procedures to the Government for approval. The final pre-delivery test report shall be delivered after completion of the pre-delivery test.

3.4.3 Contractor's Field Testing

All equipment shall be calibrated and tested, DTS operations verified, the integrated system placed in service, and the integrated system tested. All Ground rods installed shall be tested as specified in IEEE STD 142. A report describing results of functional tests, diagnostics, and calibrations, including written certification to the Government that the installed complete system has been calibrated, tested, and is ready to begin performance verification testing shall be delivered. It is recommended that the Contractor use the approved performance verification test as a guideline when the field test is conducted.

3.4.4 Performance Verification Test

The completed system shall be demonstrated so that it complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown. The performance verification test, as specified, shall not be started until after receipt by the Contractor of written permission from the Government, based on the Contractor's written report. The report shall include certification of successful completion of testing as specified in paragraph 3.4.3, Contractor's Field Testing, and upon successful completion of training as specified. The Government may terminate testing at any time when the system fails to perform as specified. Upon termination of testing by the Government or by the Contractor, an assessment period will commence as described for Endurance Testing Phase II. Upon successful completion of the performance verification tests all test reports and other documentation as specified to the Government prior to commencing the endurance test shall be delivered.

3.4.5 Endurance Test

3.4.5.1 System reliability and operability shall be demonstrated at the specified throughput rates for each portal, and the Type I and Type II error rates specified for the completed system. False alarm rates shall be calculated and the system shall yield false alarm rates within the specified maximums at the specified probability of detection. The endurance test shall be conducted in phases as specified. The endurance test shall not be started until the Government notifies the Contractor, in writing, that the performance verification test is satisfactorily completed, training as specified has been completed, and correction of all outstanding deficiencies has been satisfactorily completed. One operator shall be provided to operate the system 24 hours per day, including weekends and holidays, during Phase I and Phase III endurance testing, in addition to any Government personnel that may be made available. The Government may terminate testing at any time the system fails to perform as specified. Upon termination of testing by the Government or by the Contractor, an assessment period shall be commenced as described for Phase II. The operation of each terminal device shall be verified during the last day of the test.

Upon successful completion of the endurance test, test reports and other documentation shall be delivered as specified to the Government prior to acceptance of the system.

3.4.5.2 Phase I Testing. The test shall be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system shall operate as specified. No repairs shall be made during this phase of testing unless authorized by the Government in writing. If the system experiences no failures during Phase I testing, the Contractor may proceed directly to Phase III testing after receipt by the Contractor of written permission from the Government.

3.4.5.3 Phase II Assessment. After the conclusion of Phase I, all failures, determine causes of all failures, repair all failures shall be identified, and a written report delivered to the Government. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and shall recommend the point at which testing should be resumed. After delivering the written report a test review meeting shall be convened at the jobsite to present the results and recommendations to the Government. The meeting shall not be scheduled earlier than 5 business days after receipt of the report by the Government. As a part of this test review meeting all failures shall have been corrected by performing appropriate portions of the performance verification test. Based on the Contractor's report and the test review meeting, the Government will determine the restart date, or may require that Phase I be repeated. If the retest is completed without any failures, the Contractor may proceed directly to Phase III testing after receipt by the Contractor of written permission from the Government.

3.4.5.4 Phase III Testing. The test shall be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system shall operate as specified. No repairs shall be made during this phase of testing unless authorized by the Government in writing.

3.4.5.5 Phase IV Assessment. After the conclusion of Phase III, all failures, determine causes of failures, repair failures shall be identified and delivered in a written report to the Government. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and shall recommend the point at which testing should be resumed. After delivering the written report, a test review meeting shall be convened at the jobsite to present the results and recommendations to the Government. The meeting shall not be scheduled earlier than 5 business days after receipt of the report by the Government. As a part of this test review meeting, it shall be demonstrated that all failures have been corrected by repeating appropriate portions of the performance verification test. Based on the Contractor's report and the test review meeting, the Government will determine the restart date, and may require that Phase III be repeated. Any required retesting shall not be commenced until after receipt of written notification by Government. After the conclusion of any retesting which the

Government may require, the Phase IV assessment shall be repeated as if Phase III had just been completed.

3.4.5.6 Exclusions. The Contractor will not be held responsible for failures in system performance resulting from the following:

a. An outage of the main power in excess of the capability of any backup power source, provided that the automatic initiation of all backup sources was accomplished and that automatic shutdown and restart of the AIE System performed as specified.

b. Failure of a Government furnished communications circuit, provided that the failure was not due to Contractor furnished equipment, installation, or software.

c. Failure of existing Government owned equipment, provided that the failure was not due to Contractor furnished equipment, installation, or software.

3.4.6 Commissioning Report

Upon successful completion of the Endurance Test, the Contractor's Commissioning Team Leader shall prepare a Commissioning Report documenting that the Contractor has successfully completed the PVT and Endurance Test and recommending that the completed system be accepted. The Commissioning Report shall include signatures of the Commissioning Team.