INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM-VI (ICIDS-VI)

SYSTEM PERFORMANCE SPECIFICATION

08 Dec 2021

Version 1

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

Intentionally Left Blank

PREPARED BY

GOEHRING.RICHARD.HAI.1200149951 Digitally signed by GOEHRING.RICHARD.HAI.1200149951 Date: 2022.06.17 14:52:40 -04'00'

Richard H. Goehring — Date
Assistant Product Manager/COR
Product Manager, Force Protection Systems
Integrated Commercial Intrusion Detection System

CONCURRENCE

BROOKER.CURTIS.ELLIOT.1255076767 Digitally signed by BROOKER.CURTIS.ELLIOT.1255076767 Date: 2022.06.30 08:48:51 -04'00'

Curtis Brooker — Date
LTC
Product Manager, Force Protection Systems

Table of Contents

1. SCOPE

1.1 Scope. This System Performance Specification (SPS) provides requirements for Integrated Commercial Intrusion Detection System (ICIDS)-VI. It establishes performance, interface and test requirements for ICIDS-VI system and subsystems. The SPS lists general requirements and performance specifications contained in the Unified Facilities Guide Specifications (UFGS) Section 28 10 05 and National Fire Protection Association (NFPA) 731, Standard for the Installation of Premises Security Systems. When requirements for sub-systems and components not included in this document, refer to the current version of UFGS Section 28 10 05. Detailed interface, system specific configuration requirements will be published in the Configuration Management Plan. Detailed testing requirements will be published in the Test Plan.

2. APPLICABLE DOCUMENTS

2.1 General. Documents are shown in Appendix A. If a document is referenced without indicating any specific paragraphs as applicable, entire document applies.

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

3. DEFINITIONS See Appendix B

4. GENERAL REQUIREMENTS

4.1 General. ICIDS-VI shall provide the capability to detect intrusion, control access to restricted areas, detect and deny unauthorized entries within specific areas, generate reports, produce photo identification badges, provide surveillance, and annunciate alarms. It shall be designed to provide operational flexibility, survivability, and reliable performance. ICIDS VI shall be modular, allowing for future incremental expansion or modification of inputs, outputs, and remote-control stations. It shall be compatible with fielded ICIDS systems. Integrated system capabilities shall include but not be limited to Command-and-Control System, Intrusion Detection, Physical Access Control, Intercommunications, Close Circuit Television (CCTV) and Redundant Power.

4.2 Systems of Systems. ICIDS VI is a System of Systems of complementary physical security capabilities fielded at Army installation provides regional command and control center for multiple Army/Joint installations.

4.2.1 Central Monitoring Station (CMS) System. Shall provide the continuous display and primary situational awareness data management of all connected Installations, facilities, zones, and partitions. The Central Monitoring Station Subsystem shall also interface with enterprise-level records management systems and provide interoperability with systems that support policing and incident management functions. CMS provides regional monitoring of Local Control Stations that may use disparate Intrusion Detection Systems (IDS) (Figure 1).

4.2.2 Local Control Station (LCS) System. Shall provide continuous display and command and control of a specific Installation and facility-based zones and partitions to include the ability to manage user access to a restricted area which is controlled by an intrusion system. The Local Station Control System must provide the ability to interface with physical access control systems (PACS) and closed-circuit television (CCTV) systems that support the physical security function (Figure 2). Multiple LCS are monitored by specific CMS within a defined geographic region.

4.3 Integrated Functional Requirements.

4.3.1 Security Command Center System. Shall be UL certified Burglar Alarm Units, UL 1610, the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, or the Standard for Digital Alarm Communication System Units, UL 1635. The system shall be able to monitor multiple Installations or zones for the CMS and LCS respectively. The SCC includes alarm reporting and display subsystem. Software, hardware and devices to control, process, integrate, and annunciate ICIDS data that allow for operator monitoring and intervention. It includes the Local or Regional Station Control Console, SQL server(s), and media server(s). Additionally, Application Programming Interfaces (APIs) shall be required for unified content at the CMS and interoperability between the CMS and the hosted LMS using disparate physical security applications and devices.

4.3.2 Intrusion Detection System (IDS). The system shall be able to detect and report intrusion attempts and provide means to indicate a duress condition. It consists of sensors, premise control units (PCU) and software modules.

4.3.3 Physical Access Control System (PACS). PACS and its components shall be listed as approved on the FIPS 201 Approved Products List (APL). The PACS shall detect intrusion attempts, monitor and control personnel movement through normal access routes in and out of the facility and between protected areas within the facility. It consists of electronic devices, access control units (ACU), sensors and software modules. The PACS shall be capable of performing all required authentication methods outlined in FIPS 201 and shall perform the required level of authentication designated by the system owner at each door or layer of security in depth.

4.3.4 Close Circuit Television (CCTV) System. The system shall interface with ICIDS for control of camera call up to monitor, Pan-Tilt-Zoom (PTZ) control, Video recording based on alarm event triggers. Integration shall provide the means to associate ICIDS archived alarm events with recorded video at two separate locations. It consists of electronic devices required to provide visual assessment of ICIDS alarms and recording.

4.3.5 Communication System. The system shall provide redundant communications links from the Local Control Station and the Central Monitoring Station. It consists of elements required to ensure that pertinent data is transferred from point of origin to point where appropriate actions can be taken.

4.3.6 Back-up Power System. The system shall enable continuous operation of the entire ICIDS-VI and back-up systems to ensure continuous operation of certain components as determined by Army and/or pertinent regulations when primary power is interrupted.

4.4 Growth Capability. ICIDS-VI shall provide capability for modular ICIDS expansion with minimal equipment modification. ICIDS-VI shall be able to integrate products from multiple manufacturers and shall not be limited growth capability to products of a single manufacturer.

4.5 Hazardous Locations. When located in areas where fire or explosion hazards exist, ICIDS shall provide system components rated and installed according to Chapter 5 of NFPA 70. Additionally, the system shall conform to DA PAM 385-64 Chapter 17 – HERO requirements – as applicable.

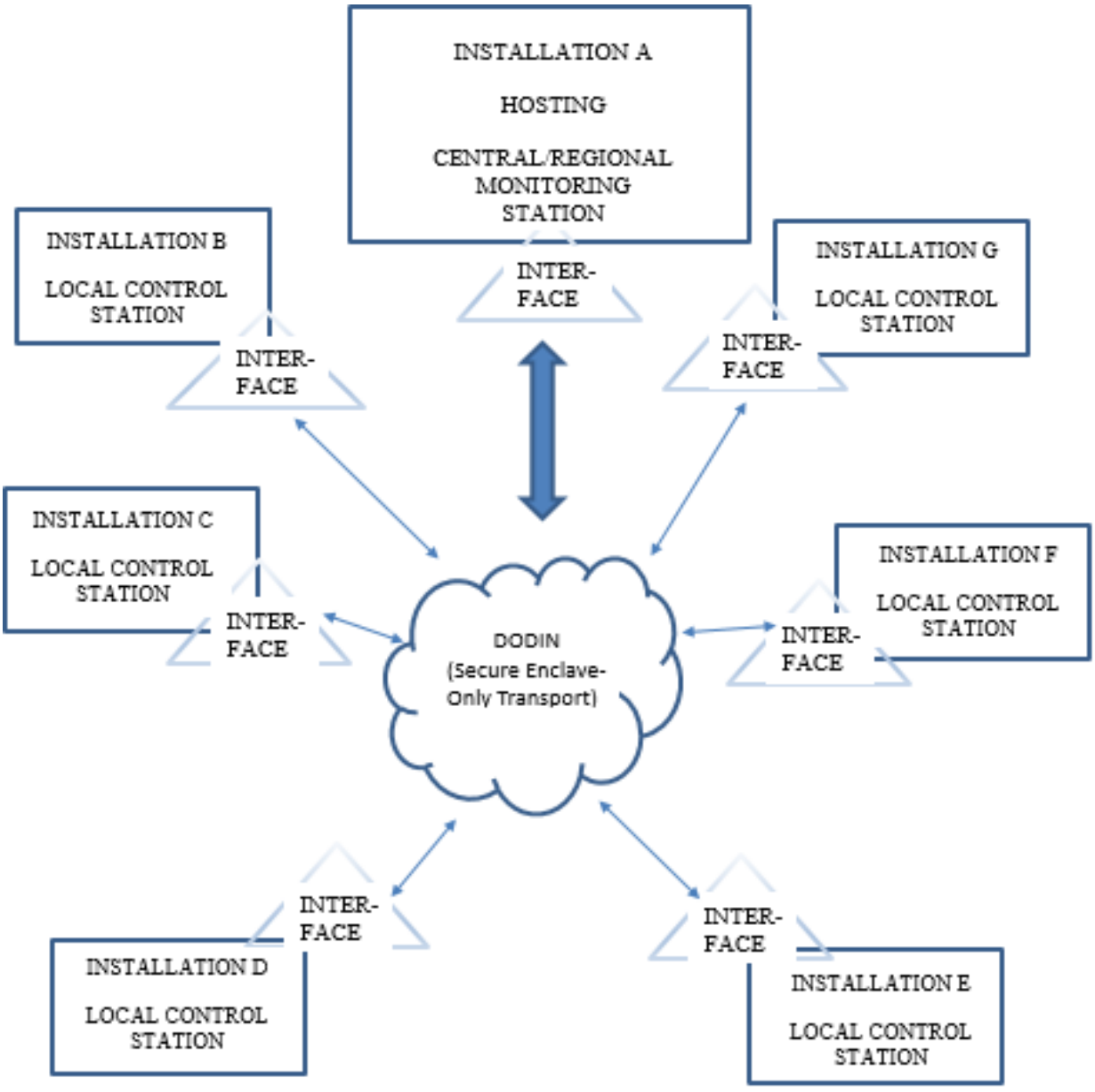

Figure 1. ICIDS-VI Functional Architecture Central/Regional Monitoring Station.

NOTES:

1. Diagram describes functional requirements and is not a design constraint.
2. INTERFACE – interoperability and encryption capabilities between installation system and central monitoring system.

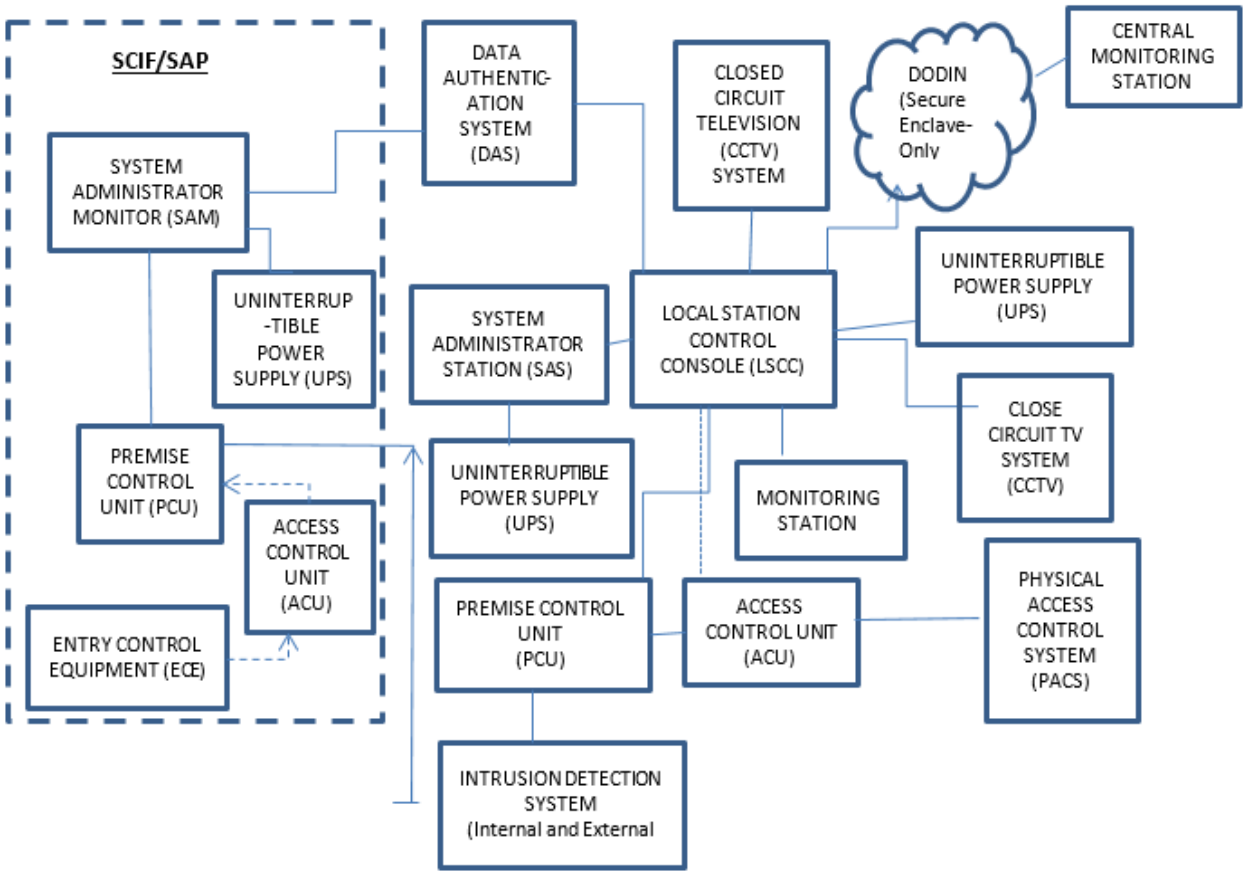

Figure 2. ICIDS-VI Functional Architecture Local Control Station (LCS) at Installation.

NOTES:

1. Diagram describes functional requirements and is not a design constraint.
2. Quantities and types of components will vary with each installation.

4.6 System Configuration. ICIDS VI shall be set up as an Information System Secure Enclave. ICIDS VI Life Cycle operations, sustainment and maintenance support are provided by PM FPS. ICIDS VI fiber/network architecture/topology infrastructure shall be designed for CONUS-OCONUS installations by logical separation to maintain Information System secure enclave posture and gain necessary network and Cyber approvals from the U.S Army Network Enterprise Technology Command (NETCOM) and other DoD managed networks to integrate the ICIDS VI fiber/network architecture/topology infrastructure into each designated Army/Joint Bases CONUS-OCONUS Installation site facility by logical separation to maintain Information System enclave posture. ICIDS-VI enterprise network access to the DODIN will be available via the network Top-Level Architecture (TLA)/Joint Regional Security Stack (JRSS) managed by NETCOM and/or Joint Department of Defense entities (National Guard/US Army Corp of Engineers/ Joint Army-Air Force-Navy-Defense Information Systems Agency and any Non-Standard sites) to include computer network defense (CND) protection for ICIDS VI. The system shall provide a network architecture compliant with Joint Regional Security Stack (JRSS) Installation Area Network (ICAN) modernization guidance. The System shall use any feasible way to establish system enclave utilizing Installation Network infrastructure only for transport purposes. The System shall be designed to integrate with existing infrastructure and networks. The System components shall be interoperable, modular, scalable, and compatible that can be tailored to accommodate future hardware and software upgrades.

4.7 System Installation. ICIDS-VI installation shall meet Unified Facilities Criteria (UFC) 4-021-02, Electronic Security Systems with Change 1, 11 September 2019, Unified Facilities Guide Specifications (UFGS) Section 28 10 05 or current revision as specified by Army Regulation (AR) 190-13, Physical Security Program. Additionally, it shall meet applicable codes and standards within NFPA 731, and applicable regulations.

4.8 Performance Requirements. Integrate the installed and operating subsystems into the overall ICIDS system to detect intrusion, control access, provide CCTV surveillance, provide visual verification, and perform as an entity, as specified below. Provide electronic equipment that complies with 47 CFR 15, Radio Frequency devices, and are suitable for the environment where they will be installed.

4.8.1 Reliability. Mean Time Between Operational Mission Failure for the display subsystem shall be 4,100 hours or greater. Mean Time Between Failure (MTBF) for any single transmission line of 21,400 hours or greater. MTBF for PCU of 11,100 hours or greater. MTBF for any sensor of 18,100 hours or greater.

4.8.2 Availability. Provide components rated for continuous operation. Provide solid-state electronic components mounted on printed circuit boards, conforming to UL 796. Provide boards that are plug-in, quick-disconnect type. Do not impede maintenance with densely packed circuitry. Provide power-dissipating components with safety margins of not less than 25 percent with respect to dissipation ratings, maximum voltages, and current-carrying capacity. Provide solid-state type or hermetically sealed electromechanical type light duty relays and similar switching devices.

4.8.2.1 Operational Availability. ICIDS-VI shall have system Operational Availability of 0.997 or greater. ICIDS VI shall have a Mean Time to Repair (MTTR) of 0.5 hours or less. ICIDS VI shall have a Maximum Time to Repair of 1.0 hours or less.

4.8.3 Maintainability. Provide components that can be maintained using commercially available tools and equipment. Arrange and assemble components to be readily accessible to maintenance personnel without compromising system defeat resistance and with no degradation in tamper protection, structural integrity, EMI or RFI attenuation, or line supervision after maintenance when it is performed in accordance with manufacturer's instructions.

4.8.4 Fail Safe Capability. Provide fail-safe capability in critical elements of the ICIDS including, but not be limited to, the capability to monitor communication link integrity and to provide self-test. Provide fault annunciation when diminished functional capabilities are detected. Annunciate fail-safe alarms to clearly distinguish from other types of alarms.

4.8.5 Preventive Maintenance. System components shall require minimal preventive maintenance. Provisions shall allow preventive maintenance while system is operational.

4.8.6 Line Supervision. Provide the same geographic resolution for fault isolation at the systems level as provided for intrusion detection. Provide either a static or dynamic system with active mode for line supervision of communication links of the ICIDS-VI system.

a. The static system must represent "no-alarm" always by the same signal, which is different than the originally transmitted signal.

b. The dynamic system must represent "no-alarm" with a signal which continually changes with time.

4.8.7 Power Loss Detection. Detect AC and DC power loss and generate an alarm when a critical component of the system experiences temporary or permanent loss of power. Annunciate the alarm in PCU and LCS to clearly identify the component experiencing power loss.

4.8.8 Controls and Designation. Provide controls and designations as specified in NEMA ICS 1, Industrial Control and Systems General Requirements.

4.8.9 Interchangeability. Use off-the-shelf components which are physically, electrically, and functionally interchangeable with equivalent components as complete items. Equivalent, replacement components must not require new or other component modification. Shall not use custom designed or one-of-a-kind items. Interchangeable components or modules must not require trial and error matching to meet integrated system requirements, system accuracy, or restore complete system functionality.

5. SUBSYSTEM REQUIREMENTS

5.1 Performance Characteristics. The ICIDS-VI performance characteristics shall conform to the UFGS 28 10 05 or current revision per Army Regulation (AR) 190-13 and all applicable regulations and standards as referenced in Para 2 of this document and in Appendix A. This document provides an overview.

5.1.1 Security Command Center (SCC) System. As a general overarching requirement to meet Secure Equipment Act of 2021 for all Electronic Security Systems components, SCC must integrate all subsystems and communications, and provide operator control interface to the ICIDS-VI system. Additionally, the CMS shall be able to operate with the different physical security applications and equipment used by hosted Installations. The components are as follows:

a. ICIDS Software Suite
b. Monitoring Display Software
c. Graphical Map Software
d. Printers
e. Control and Display Integration
f. Enrollment Center Equipment and Software
g. Data Storage
h. Application Interface and Encryption
i. Computer Aided Dispatch Systems

5.1.1.1 ICIDS Software. ICIDS software requirements shall be IAW be UFGS 28 10 05 para 2.6.1 and sub para as applicable. Other requirements listed conform to capabilities of fielded ICIDS systems.

a. Provide commercial off-the-shelf software that utilizes a single database for the subsystem integrations provided under a single operating environment. The system is to archive all events in a database stored either on a local hard drive or a networked database server. The software must support configuration and simultaneous monitoring of all subsystems.

b. Allow the networked PC servers and workstation configurations connected via TCP/IP network utilizing DoD approved secure protocols. Administrative tasks including configuration, monitoring, schedules, report generation and graphic display are provided from any PC server and workstation on the network. All system programming data must be instantly accessible to every PC Workstation connected to the network and limited only by USER PRIVILEGES. The system is to utilize a non-proprietary SQL-based, ODBC-compliant database, managed by Sybase Adaptive Server Anywhere, Microsoft SQL Server, or Oracle.

c. Utilize a preemptive multi-tasking operating system, such as the latest Microsoft Windows environment, that is multitasking without any internal and external interference.

d. Provide capabilities to define visual exclusion areas.

e. Provide de-warping software for panoramic cameras as applicable.

5.1.1.2 Alarm Call Up. Support responses to alarms entering the system with each alarm capable of initiating one or more of the actions listed in UFGS 28 10 05 para 2.6.1.1.

5.1.1.3 System Timing. Shall be able to report five simultaneous alarms transmitted, processed, and annunciated within three seconds when the alarm occurs.

5.1.1.4 Programming. Provide the capability of, but not limited to, the following programming and functionality listed in UFGS 28 10 05 para 2.6.1.2.

5.1.1.5 ICIDS Monitor Display Software. All monitor display software requirements shall be IAW be UFGS 28 10 05 para 2.6.2 and sub paragraphs as applicable.

5.1.1.6 Graphical Map Software. All ICIDS graphical map software requirements shall be IAW be UFGS 28 10 05 para 2.6.2 and sub paragraphs as applicable.

5.1.1.7 Printers. All ICIDS printer requirements shall be IAW be UFGS 28 10 05 para 2.6.2 and sub paragraphs as applicable.

5.1.1.8 Control and Display Integration. Integrate human engineer SCC controls so the entire SCC can be operated by a single or multiple operators. Integrate switching and monitoring components of the assessment subsystem with the SCC so that SCC operator(s) can effectively monitor, assess alarms, and control the ICIDS. Method of system integration must be as a single console. Provide chassis, and modules required for console SCC configuration.

5.1.1.9 Enrollment Center Equipment and Software.

5.1.1.9.1 Enrollment Center Equipment. All ICIDS-VI enrollment center equipment requirements shall be IAW be UFGS 28 10 05 para 2.6.6 and sub paragraphs as applicable. Provide enrollment stations to enroll personnel into, and dis-enroll personnel from, the system database. The enrollment equipment is to only be accessible to authorized entry control enrollment personnel.

5.1.1.9.2 Enrollment Center Software. All ICIDS enrollment center equipment requirements shall be IAW be UFGS 28 10 05 para 2.6.6.3.

5.1.1.9.3 Data Storage. The system shall use an operating system that satisfies the requirements of Information Assurance, have sufficient storage capacity and processing speed to meet system storage requirements.

a. System shall continuously and automatically store configuration, operator actions, maintenance periods and alarm data with corresponding date and time into nonvolatile storage.

b. Operator shall have no control of data storage.

c. Shall be at a minimum configured as hot swappable RAID 5 with redundant power supplies on all application and storage servers.

d. Provisions shall allow for one month storage of archive data for an installation with 1,280 remote areas before being downloaded to permanent storage.

e. System shall generate status display message before capacity of data storage is reached:

(1) Message shall be generated when data storage is at 75% of capacity in time to replace the storage media or backup stored data before overwriting occurs without disrupting operator functions.

(2) User shall have ability to select an alert, so message is not lost until data storage is reduced or replaced.

5.1.1.9.4 Application Interface and Encryption. The CMS shall be able to interface with the LMS that use disparate physical security applications while using secure enclave transport systems.

5.1.2 Intrusion Detection System (IDS). The IDS primary function is to detect intrusion into secured areas. The IDS shall utilize a single database for all IDS programming data that seamlessly integrates with the ICIDS system under a single operating environment. The IDS events must be viewable as separate or as a combined list of all ICIDS events. Control the IDS alarm monitoring through software control from the ICIDS system. IDS shall be consistent with the requirements in UL 1076. Additionally, IDS in Sensitive Compartmentalized Information Facilities (SCIFs) and Special Access Programs (SAPs) shall comply with UL 2050 Extent 3 standards for installation.

a. Provide both supervised and non-supervised alarm point monitoring.

b. Secure or access alarm points both manually and automatically by time of day, day of week or by operator command.

5.1.2.1 IDS Components.

a. Premise Control Units (PCU)
b. Detection Sensors
c. Tamper Switches
d. Duress Switches (as required by zone)

5.1.2.2 Detection Sensitivity. The sensitivity shall allow for the following:

a. Locating intrusions within 100 meters or 300 feet zones along a line or perimeter to one side of the facility building.

b. Locating intrusions at individually protected assets or at an individual portal.

c. Locating intrusions within the coverage on a single volumetric sensor.

d. Locating failures or tampering at individual sensors.

5.1.2.3 Detection Alarm and Reporting Capacity.

a. Collect, communicate, and display up to a minimum of 256 sensor zone alarms and to enable control of two card reader or card reader with integral keypad for arming and disarming secure and access inside of the protected area with a delayed alarm and outside of the protected area with instant alarm.

b. Identify individual sensors in alarm if the sensor zone is a multiple alarm source combination. Annunciate a single alarm within 2 seconds maximum, after sensor transducer or other detection device activation except that alarms transmitted by radio frequency signaling must communicate in less than 3 seconds.

c. Arm/Disarm keypads shall have LED display with capability to display alarm status and event history and identify alarms by device, input, zone, and partition, etc.

5.1.2.4 Probability of Detection. The ICIDS-VI system shall have the following probability of detection goals by asset risk level:

a. Risk I: 0.90 (T), 0.95 (O).
b. Risk Level II: 0.95 (T), 0.99 (O); and
c. Risk Level III; 0.95 (T), 0.99 (O).

5.1.2.5 False Alarm Rate. The false alarm rate for each interior IDS zone must not exceed one false alarm per 30-day period. The false alarm rate for each exterior IDS zone must not exceed one false alarm per 24-hour period.

5.1.2.6 Nuisance Alarm Rate. The nuisance alarm rate for each interior IDS zone must not exceed three nuisance alarms per 30-day period. The nuisance alarm rate for each exterior IDS zone must not exceed three nuisance alarms per 24-hour period.

5.1.2.7 Premise Control Unit (PCU). Install the PCU command processor in a tamper resistant enclosure that is specified in paragraph "Component Enclosure". Package the following with the PCU:

a. Power transformer
b. Battery(s)
c. Network connection cable and/or appropriate communication medium
d. Keypad(s)
e. Keypad connection cable(s)
f. Additional components as required for full functionality

5.1.2.7.1 Overcurrent Protection Indication. When overcurrent more than it is rated for is detected by the PCU, the communication bus(es) and keypad(s) shall shut down and an overcurrent notification LED lit to indicate the situation.

5.1.2.7.2 Manual and Self-Test. All testing from any alphanumeric keypad include testing for: standby battery, alarm bell or siren, and communication to the Security Command Center (SCC) of the Installation and the Central Monitoring Station. Shall include provisions for an automatic, daily, weekly, 30 days, or up to 60-day communication link test from the PCU installation site to the SCC. Include a provision for displaying the internal system power and wiring conditions.

5.1.2.7.3 Backup Battery Capacity Calculations. Backup battery capacity shall exceed sensor(s) operation, communications supervision, and alarm annunciation power requirements for proposed equipment plus 25 percent spare capacity. Backup time HRS= Battery capacity (amps/hr.) x Input Voltage/ Total load in Watts.

5.1.2.7.4 Backup Battery Monitoring and Detection. PCU shall monitor backup battery power for low battery condition or loss of backup battery power. Monitoring shall be continuous regardless of if primary power is present or not. The system shall generate an alarm whenever low battery condition or loss of backup battery power is detected. Annunciate the alarm at the LCS and the CMS, to clearly identify the PCU experiencing the condition.

5.1.2.7.5 Multi-state Alarm Inputs. PCUs shall accept multi-state alarm inputs and/or addressable alarm sensors to reduce the number of home run signal cables, alarm inputs required, and simplifies programming.

5.1.2.7.6 Expandability. The PCU shall provide modular solution which will allow for present zone security requirements while also having the capability for adding sensors and status points. PCU shall allow for array configuration should the zone requirements exceed the capacity of the PCU.

5.1.2.8 Detection Sensors.

a. Sensors are to detect facility perimeter or protected zone penetrations by unauthorized personnel or intruders and transmit an alarm signal to the alarm annunciation system upon change detection. Accomplish this with a probability of detection (PD) of 0.9 with a 95 percent confidence level and conforming to UL 639 where applicable.

b. Required sensor power is 12 VDC unless otherwise specified.

c. Shall provide line supervision for all sensors with an end-of-line resistor at the sensor or within a tampered junction box with conduit from the junction box to the sensor.

d. Shall provide sensors and components rated for operation in the installed environment. The sensors must transmit an alarm signal to the alarm annunciation system upon change detection. Provide all sensors with a tamper switch and elements housed in a tamper-

alarmed enclosure in accordance with paragraph "Component Enclosure" in UFGS 28 10 05.

5.1.2.8.1 High Security Switch (HSS). Shall conform to UL 639. Shall conform to additional requirements by zone type as required by all applicable regulations.

5.1.2.8.2 Passive Infra-Red Sensors (Interior and Exterior). Shall conform to UL 639. Shall conform to additional requirements by zone type as required all applicable regulations.

5.1.2.8.3 Microwave Sensors. Shall conform to UL 639. Shall conform to additional requirements by zone type as required by all applicable regulations.

5.1.2.8.4 Dual Technology Sensors. Shall conform to UL 639. Shall conform to additional requirements by zone type as required by all applicable regulations.

5.1.2.8.5 Fence Mounted Sensors. Sensors are fiber optic or strain-sensitive cable sensors as indicated which initiate an alarm when an intruder attempts to scale, cut through, lift the fabric of, or lean climbing devices on to the entire length of a standard chain link fence or physical barrier. Shall provide sensors that are either tamper alarmed or self-protecting. House exterior components in rugged, corrosion-resistant enclosures, as specified in paragraph “Component Enclosures” in UFGS 28 10 05.

5.1.2.8.6 Duress Alarms. Shall comply with ANSI/SIA CP-01, Control Panel Standard – Features for False Alarm Reduction, Para 4.2.4. Shall conform to NFPA 731.20 and other additional requirements by zone type as required by all applicable regulations.

5.1.3 Physical Access Control System (PACS).

5.1.3.1 Functional Requirements. The following are some functional requirements of the PACS. A complete and detailed list is in UFGS Para 20 28 10 05. PACS and its components shall be listed as approved on the FIPS 201 Approved Products List (APL). Additionally requirements dictated by zone type shall be governed by pertinent Army Regulations.

a. The PACS card credentials are required to be Common Access Cards (CAC), and CAC cards are being provided by the Government. Interface system with and provide alarm and other status to the overall ICIDS.

b. System is to grant or deny access or exit based upon (as applicable):

(1) Keypad identification data
(2) CAC or PIV card identification data
(3) Biometric reader identification data
(4) Smart card identification data
(5) Identification technologies combination
(6) Input through the access control devices compared to data stored within the system

c. Decision to grant or deny access or exit is to be based upon authorization for such

data to be input at a specific location for the current time period. Access decisions for high security areas are to be based upon two identification technology combinations: card and keypad or card and biometric.

d. Shall provide ACS that supports the configuration and simultaneous monitoring of multiple access control devices when TCP/IP communication interfaces are used between the ICIDS system and the Primary Access Control Unit (ACU). The events of the ACS are to be viewable as separate or as a combined list of all ICIDS events. Provide overall control of the ACS, alarm monitoring, and photo identification through software control of the ICIDS system.

e. Shall provide both supervised and non-supervised alarm point monitoring.

5.1.3.2 PACS Badging Requirements.

a. Shall include fully integrated badging capabilities, including image capture, image editing, badge design, and badge printing. Allow for each cardholder to be assigned to both a badge design formatted for badge printing and a dossier design formatted for standard paper printing.

b. Shall provide for interfacing with external badge programs, in which stored photo images are displayed in a cardholder information window, but other badge features are supported by the external program. Include one or more networked PC workstations with the photo imaging components at which all the required image capture equipment has been installed.

c. Shall provide a minimum 100 blank visitor card stock that is listed on the FICAM APL, https://www.idmanagement.gov/approved-products-list-piv/.

5.1.3.3 PACS Programming. Software shall be capable of, but not limited to, the following programming requirements as stated in UFGS 28 10 05 para 2.4.2.

5.1.3.4 Error and Throughput Rates. Rates must be portal to portal performance averages obtained when processing individuals one at a time. Shall have a minimum of throughput of six authorized entries per minute.

5.1.3.5 Enrollment Equipment. Shall provide enrollment equipment as required in paragraph Enrollment Center Equipment of UFGS 28 10 05 para 2.6.6.

5.1.3.6 Access Control Unit (ACU). Shall be micro-processor based ACU with all access and input and output decisions to be made by the individual ACU(s). Provide modular solution which will allow for present security requirements and the capability to expand. Configure all field ACU panels to intercommunicate via RS-422/485 or RS-232 hardwired, TCP/IP or fiber-optic communication. Equip all field ACU(s) with a tamper contact. ACUs shall accept multi-state alarm inputs and/or addressable alarm sensors to reduce the number of home run signal cables, alarm inputs required, and simplifies programming. Shall conform to UL 294.

5.1.3.7 Access Control Devices. The card, card reader, and panels shall meet encryption requirements that are specified in paragraph Data Encryption. Devices are to be tamper alarmed, tamper and vandal resistant, and solid state, containing no electronics which could compromise the access control subsystem should the subsystem be attacked. ACU shall monitor backup battery power for low battery condition or loss of backup battery power. Monitoring shall be continuous regardless of primary power is present or not. The system shall generate an alarm whenever low battery condition or loss of backup battery power is detected. annunciate the alarm at the LCS and the CMS, to clearly identify the ACU experiencing the condition. Shall conform to UL 294.

5.1.3.8 Access Control Keypads. Entry control keypads shall use unique alphanumeric and other symbol combinations as an identifier. Keypads shall contain an integral alphanumeric and special symbols keyboard with symbols arranged in ascending ASCII code ordinal sequence or random scrambled order. Communications protocol is to be compatible with the local processor.

5.1.3.8.1 Keypad Display. Keypads are to include an LED or other type of visual indicator display and provide visual (T) Visual and Audible (O) status indications for power ON and OFF and whether user passage requests have been accepted or rejected.

5.1.3.8.2 Keypad Response Time. The keypad is to respond to passage requests by generating a signal to the local processor.

5.1.3.8.3 Keypad Power. The keypad must not dissipate more than 5 watts.

5.1.3.8.4 Keypad Mounting Method. Provide keypads suitable for variable weatherproof mounting as required.

5.1.3.8.5 Keypad Duress Codes. Provide a means for users to indicate a duress situation by entering a special code into the keypad.

5.1.3.9 Card Readers with Integral Keypad. Equip contact and contactless card readers with integral keypads as specified in UFGS 28 10 05 paragraph “Keypads”.

5.1.3.10 Access Control Cards. Shall provide cards with the capability of modification and lamination during enrollment process without readability reduction for use as a picture and identification badge. Cards shall contain binary coded data arranged in a scrambled pattern as a unique identification code stored on or within the card and of the type readable by the subsystem card readers. Shall be listed as approved and consistent with the PACS manufacturer's approved solution.

5.1.3.11 Personal Identity Verification Equipment. Entry control personnel identity verification equipment shall use a unique personal characteristic or unique personal physiological measurement to establish the identity of authorized, enrolled personnel. The PACS shall designed based on the FICAM 13.02 Topology – end-to-end systems which integrate the first two components (PACS Infrastructure; Validation System) into a “PACS Validation

Infrastructure," which is then integrated with the third component category (PIV Reader).

5.1.3.12 Portal Control Devices. Portal Control Devices shall be designed in accordance with NFPA 101, Means of Egress. If ICIDS is to be integrated with the Fire Alarm System provide appropriate signage in accordance with NFPA 101. Door hardware shall be UL 1034 Burglary-Resistant Electric Locking Mechanisms. Provide FF-L-2890 locking hardware where required.

5.1.4 Closed-Circuit Television (CCTV) System. System components shall conform to the Open Network Video Interface Forum (ONVIF) specification. Shall be compatible with UL listed CCTV components to provide visual assessment of ICIDS alarms automatically upon alarm or upon operator selection. Otherwise, the subsystem is to continuously display the coverage area. Display alphanumeric camera location ID on all monitors. CCTV will comply with FAR Clause 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

5.1.4.1 Cameras. All Camera and camera component requirements shall be IAW UFGS 28 10 05 para 2.5.1 and sub paragraphs.

5.1.4.2 Video Analytics. Video Analytics requirements shall be IAW UFGS 28 10 05 para 2.5.3 and sub paragraphs.

5.1.4.3 Color Video Monitors. Color video requirements shall be IAW UFGS 28 10 05 para2.5.4 and sub paragraphs.

5.1.4.4 Ancillary Equipment. All ancillary CCTV equipment requirements shall be IAW UFGS 28 10 05 para 2.5.5 and sub paragraphs as applicable. Shall conform to UL 1678, Standard for Safety for Household, Commercial, and Institutional-Use Carts, Stands and Entertainment Centers for Use with Audio and/or Video Equipment.

5.1.4.5 Camera Housing. Camera housings shall meet IP66/67/or 68 rating.

5.1.4.6 Camera Mounting Structures. Camera mounting requirements shall be IAW UFGS 28 10 05 para 2.5.6 and sub paragraphs as applicable. Shall conform to UL 1678.

5.1.5 Communication System (UFGS 28 10 01 para 2.7).

a. Communications are to link together subsystems of the ICIDS and be in accordance with Section 27 10 00 Building Telecommunications Cabling System of UFGS 28 10 05. Interfaces between subsystems cannot be accomplished by use of an electro-mechanical relay assembly. Communications links shall be supervised. Shall provide common communications interface devices throughout the ICIDS. Provide dry contact sensor to control unit interface that is normally OPEN or normally CLOSED, except as specified otherwise.

b. Use digital, asynchronous, or multiplexed data control unit for central alarm reporting and display processor interface. Group individual data bits into word format and

transmit as coded messages. Implement interface with network switches which function as a communications controller, perform data acquisition and distribution, buffering message handling, error checking, and signal regeneration as required to maintain communications.

c. Provide totally automatic status changes communication, commands, field-initiated interrupts, and any other communications required for proper system operation. Do not require system communication operator initiation or response. System communication is to return to normal after any partial or total network interruption including power loss or transient upset. Automatically annunciate communication failures to the operator with communication link identification that has experienced a partial or total failure.

5.1.5.1 Link Supervision. Link supervision requirements shall be IAW UFGS 28 10 05 para 2.5.5 and sub para as applicable.

5.1.5.2 Hardwire. Hardwire shall be IAW UFGS 28 10 05 para 2.7.2 and sub paragraphs as applicable.

5.1.5.3 Radio Frequency Link. Radio frequency link shall be IAW UFGS 28 10 05 para 2.7.3 and sub para as applicable.

5.1.5.4 Data Encryption. Shall incorporate current NIST FIPS encryption standards. System and applicable subcomponents shall comply with the current NIST FIPS encryption standard throughout the warranty period. Reference Technical Specification ICD/ICS 705 for detailed encryption requirements for SCIF and SAP facilities.

5.1.5.5 Network Switch. The small form-factor pluggable (SFP) is to provide full-duplex 1000/100/10-Mbps connectivity between switches over single mode (SM) infrastructures. Provide mounting accessories for a typical field distribution box, cabinet, or rack. Rack requirements as specified in paragraph Equipment Rack of the UFGS 28 10 05.

5.1.5.6 Network Time Server. Shall provide Network Time Server (NTS) to all ICIDS local, central, regional monitoring stations or local station with integrated IDS, ACS, and/ or CCTV. To keep the system in time with each other.

5.1.5.7 Video and ICIDS Transmission. Transmission shall be IAW UFGS 28 10 05 para 2.7.6 and sub paragraphs as applicable.

5.1.5.8 Wire and Cable. Transmission shall be IAW UFGS 28 10 05 para 2.7.7 and sub paragraphs as applicable.

5.1.5.9 Digital Data Interconnection Wiring. Digital data interconnection wiring shall be IAW UFGS 28 10 05 para 2.7.8 and sub paragraphs as applicable.

5.1.5.10 Above Ground and Direct Sensor Wiring. Shall be IAW UFGS 28 10 05 para 2.7.9 and 2.7.10 respectively.

5.1.5.11 Local Area Network (LAN) Cabling. Cabling shall be in accordance with TIA-568-C.2, Category 6. Shall be IAW DoD IT Infrastructure Policy, cabling shall comply with CNSSAM TEMPEST 1-13 Red/Black Installation guidance Tab 1.

5.1.5.12 Cable Construction. Provide all cable components that will withstand the environment in which the cable is installed for a minimum of 20 years.

5.1.6 Back-Up Power System. Requirements as dictated by UFGS 28 10 05 Para 2.11, NFPA 731-20, ICS 705, UL 2050, and other applicable regulations governing the security of the specific zone or asset requiring protection.

a. Intrusion alarms shall not to be generated because of power switching; however, it shall provide a power switching indication and on-line source at the alarm monitor.

b. The system shall automatically switch back to the primary source upon primary power restoration. Detect and report failure of an on-line battery as a fault condition. Power products must be in accordance with UFGS 26 20 00 Interior Distribution System.

c. Shall provide backup power to the primary power by backup batteries in each element or subsystem and/or uninterruptible power supply (UPS). If the facility is supported by a back-up generator, provide UPS adequate to support the transition from primary power loss to power provided by the generator.

d. Shall automatically provide power to the premises security system instantaneously whenever the primary power supply fails to provide the minimum voltage required for operation.

e. Shall provide power for continuous operation of the security system, whenever primary power fails, for duration as specified for each zone type and component.

5.1.6.1 Uninterruptible Power Supply. Shall be IAW UFGS 28 10 05 para 12.11.1 and sub para as applicable.

5.1.6.2 Batteries. Shall be IAW UFGS 28 10 05 para 12.11.2 and sub paragraphs as applicable.

5.1.6.3 Surge Suppression Devices. Shall comply with requirements in UFGS 33 82 00 Telecommunication Outside Plant (OSP). Provide appropriate surge suppression devices. Devices shall be properly sized and installed as prescribed by the equipment manufacturer. The head end equipment rack shall utilize IU rack mounted shielded Ethernet, Power Over Ethernet (POE), and/or optional POE extender circuits surge protection unit that utilize field replaceable modules that do not require removal and disassembly of the unit to replace a surge protector.

5.1.7 Component Enclosures. Alarm enclosures with a tamper switch(es). Refer to paragraph "Tamper Switch" of the UFGS 28 10 05. Enclosures is to be formed and assembled to be sturdy and rigid and for components listed in UFGS 28 10 05 para 2.13.

5.1.7.1 Interior and Exterior Sensors. Shall be IAW UFGS 29 10 05 para 2.13.1 and 2.13.2 respectively.

5.1.7.2 Interior Enclosures. Enclosures to house equipment in an interior environment must meet the requirements of NEMA 12.

5.1.7.3 Exterior Enclosures. Enclosures to house equipment in an outdoor environment or corrosive environments must meet the requirements of NEMA 250 Type 4X.

5.1.7.4 Metal Thickness. Shall be IAW UFGS 28 10 05 para 2.13.7.

5.1.7.5 Doors and Covers. Shall be IAW UFGS 28 10 05 para 2.13.8.

5.1.7.6 Ventilation. Ventilation openings in enclosures and cabinets must conform to requirements of UL 1610.

5.1.7.7 Labels. Label boxes containing connections that they contain ICIDS connections and indicate that the box is part of the ICIDS system.

5.1.7.8 Test Points. Provide readily visible and accessible with minimum disassembly of equipment to test points, controls, and other adjustments inside enclosures. Test points and other maintenance controls must be readily accessible to operator personnel.

5.1.8 Equipment Rack. Provide standard 483 mm 19-inch electronic rack cabinets conforming to UL 50, Safety Enclosures for Electrical Equipment, Non-Environmental Considerations, for the ICIDS system at the SCC and remote control and monitoring sites. Equipment rack must be in accordance with UFGS 27 10 00 Building Telecommunications Cabling System. All other requirements listed in UFGS 28 10 05 para 2.14 as applicable.

6. CYBERSECURITY.

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

b. The System shall implement system security measures sufficient to attain and maintain Authorization to Operate (ATO) IAW Risk Management Framework (RMF) for DoD Information Technology per the DoDI 8510.01, AR 25-2, pamphlets that fall under AR-2 and the Network Enterprise Technology Command (NETCOM) RMF: Assess and Authorize TIP dated 2 June 2016(latest updated Policy, regulation and Instructions apply).

c. The System shall use secure encrypted communications over the network of at least AES-256 (latest updated Policy, regulation, Instructions, DoD required configuration apply).

d. The System shall encrypt data at rest IAW with DoD Policy Memorandum, " Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," dated July 7, 2007, DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," dated April 14, 2004, as supplemented by ASD Nll/DoD CIO memorandum, same subject, dated June 2, 2006, DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," dated April 18, 2006.

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

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

g. The System shall provide Host Based Security System (HBSS), per JTF-GNO CTO 07-12. 3.5.9

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

i. The System shall remain current with the latest Department of the Army and DoD security standards.

j. The System shall provide a secure operating environment IAW Defense Information System Agency (DISA) guidelines and standards. The System shall provide WSUS capabilities across all ICIDS-VI, if integrated with other ICIDS platforms provide same capability all cross the board. The System shall provide capabilities for ongoing Monitoring, monitoring/updating Information System & Environment Changes, performing Corrective Actions, updating Security Controls as needed, conducting periodic Security Control Assessments, conducting Remediation Actions, accomplishing Security Status Reporting and ensuring Risk Determination and Acceptance. The system shall be configured and maintained IAW Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). The system shall utilize highest approved FIPS algorithm in place to encrypt all devices to include System logs. The system shall be configured to use Secure File Transfer protocol. The system shall be configured and implement secure network implementation in accordance with DODI 8531.01 to include but not limited to support Vulnerability assessments and analysis (network discovery, network and host vulnerability scanning, penetration testing). The system shall implement Internal Network scanning and Monitoring/ update tools. The system shall implement threat, vulnerability and attack notification, and take corrective action to mitigate potential vulnerabilities to the system and DODIN (Department of Defense Information Networks) as part of Comprehensive Vulnerability Management consisted with repeatable Vulnerability Management Process. The system shall be configured and implemented IAW NIST SP800-53 Revision 5 Security and

Privacy Controls for Information Systems and Organizations, SP 800-53B Control Baseline for information Systems and Organizations, SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations, SP 800-53 Rev4 Assessing Security and Privacy Controls in Federal Information Systems and Organization, DoDI 8500.01, Cybersecurity, – DoDI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), – DoDI O-8530.2, "Support to Computer Network Defense (CND)", – DoDI 8551.01, Ports, Protocols, and Services (PPSM).

k. The system shall be configured to comply with current Computer Network Defense (CND) directives at the time of installation.

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

m. The system shall be configured to comply with DoD Network and Cyber Security TASKORDs, ARCYBER OPORDS, FRAGOs, CTOs. These orders changes, weekly, monthly basis so it is important that the vendor should understand that this is ongoing as part of system requirements that system is up to date configured IAW DoD and Army configuration requirements.

n. System shall be configured and ready to meet T&E requirement defined in Directive-Type memorandum (DTM) 11-009 systems such as Cooperative Vulnerability and Penetration Assessment (CVPA) The Adversarial Assessment (AA) and Red Team Assessment. A CVPA is an overt and cooperative examination of the system to identify all significant cyber vulnerabilities and the level of capability required to exploit those vulnerabilities. CVPAs are conducted in the intended operational environment with representative system operators, system/network administrators, and local cyber defenders present to assist the test team in their evaluation. The system shall be configured to meet AA's Protect, Detect, React, and Restore requirements. AA evaluate the ability to protect the system/data, detect threat activity, react to threat activity and restore mission capability degraded or lost due to threat activity.

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

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

APPENDIX A – REFERENCES

Army Air Force Exchange System:	
AAFES, EOP Procedures 16-1	Exchanges operating procedures: AAFES Security
AAFES, EOP Procedures 40-11	Special Retail Programs (Controlling Firearms), March 2000
American National Standards Institute:	
ANSI/SIA CP-01	Control Panel Standard –Features for False Alarm Reduction
ANSI/SIA PIR-01	Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity
CEA-330	Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1, December 2004
US Army:	
AR 190-11	Physical Security of Arms, Ammunition, and Explosives
AR 190-12	Military Working Dogs, 23 October 2019
AR 190-13	The Army Physical Security Program
AR 190-17	Biological Select Agents and Toxins Security Program
AR 190–51	Security of Unclassified Army Property
AR 190-51	Security of Unclassified Army Property (Sensitive and Non-sensitive)
AR 190–54	Security of Nuclear Reactors and Special Nuclear Materials
AR 190–56	The Army Civilian Police and Security Guard Program
AR 190–59	Chemical Agent Security Program
AR 215–8	Army and Air Force Exchange Service Operations
AR 25-2,	Information Assurance, 23 March 2009
AR 340–21	The Army Privacy Program
AR 380-381	Special Access Programs (SAPS) and Sensitive Activities, 21 April 2004
AR 380–5	Department of the Army Information Security Program
AR 380–86	Classification Of Former Chemical Warfare, Chemical and Biological Defense, And Nuclear, Biological Chemical Contamination Survivability Information
AR 420–1	Army Facilities Management

AR 525–13	Antiterrorism
AR 530–1	Operations Security (OPSEC)
AR 600–8–14	Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel
AR 870-20	Army Museums, Historical Artifacts and Art, 11 January 1999
AR 25-1	Army Information Technology, 15 July 2019
DA Form 4930	Alarm/Intrusion Detection Record, September 2006
DA Form 2806	Physical Security Survey Report (Prescribed in para 2–14c.)
DA Form 2806–1	Physical Security Inspection Report (Prescribed in para 2–15a.)
DA Form 4261 and DA Form 4261–1	Physical Security Inspector Identification Card (Prescribed in para 3–5.)
AR A12:A36	Military Working Dog Program, 30 September 1993
Army Corps of Engineers:	
STD 872–90–03	Standard Drawing: FE6 Chain-Link Security Fence Details for Non-Sensored Fence
UFGS 27 21 10.00 40,	Fiber Optic Data Transmission System, May 2013
UFGS 28 10 05	Electronic Security Systems May1, 2016
Chairman of The Joint Chiefs of Staff Instruction:	
CJSI 6510.01F	Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011, Current as of 10 October 2013
Committee of National Security Systems:	
CNSSI 1253	Security Categorization and Control Selection for National Safety and Security May 2016
Department of Defense:	
Department of Defense 5220.22-M,	National Industrial Security Program, Operating Manual, March 18, 2011, w/Change 3, December 10, 2021
DODD 1000.25	DOD Personnel Identity Protection (PIP) Program
DODD 8190.3	Smart Card Technology
DODI 3224.03	Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)

DODI 5200.08	Security of DOD Installations and Resources and the DOD Physical Security Review Board, 10 December 2005 w/Change 2, 8 April 2014
DoDI 5200.08-R	Physical Security Program, 9 April 2007 w/Change 1, 27 May 2009
DoDI 8500.01	Cybersecurity, 14 March 14
DoDI 8500.2	Information Assurance (IA) Implementation, 6 February 2003
DoDI 8510.01	Risk Management Framework for DoD Information Systems, July 19, 2022,
DoDI 8580.1	Information Assurance (IA) In the Defense Acquisition System, 9 July 04
DoDI O-8530.02	Support to Computer Network Defense (CND), 9 March 2001
DTM 08-003	Next Generation Common Access Card (CAC) Implementation Guidance, 8 October 2013
Electronic Components Industry Association:	
EIA/ECA-310-E	Racks, Panels and Associated Equipment, December 2005
Federal:	
CFR Data Part 15, Federal Communications Commission (FCC), Subpart C Intentional Radiators	Radio Frequency Devices, 22 May 2014
36CFR79 National Park Service, long-term curatorial services, 10 May 2014.	Part 79 Curation of Federally Owned and Administered Archeological Collections, Section 9 Standards to determine when a repository possesses the capability to provide adequate
44 U.S. Code 3542(b)2, Definitions	
47 CFR 15	Radio Frequency Devices
FED-STD-368A	Quality Control System Requirements, 10 December 1979
FIPS 140-2	Security Requirements for Cryptographic Modules, 25 May 2001
FIPS 197	Advanced Encryption Standard (AES), 26 November 2001
FIPS 201	Federal Information Processing Standards 201 (Available at http://www.itl.nist.gov/fipspubs/)
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013

HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors 44 U.S. Code 3542 (b) 2, 27 August 2004
Intelligence Community:	
Intelligence Community (IC) Directive (ICD) Number 705, 26 May 2010	Sensitive Compartmented Information Facilities
IC Standard Number (ICS) 705-1, 17, September 2010	Physical and Technical Security Standards for Sensitive Compartmented Information Facilities, 17 September 2010
Institute of Electrical and Electronics Engineers:	
IC Tech Spec for ICD/ICS 705 v1.2 23	Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities March 13, 2020
IEEE C62.41-1991	IEEE Recommended Practice for Surge Voltages, 1991
Joint Air Force, Army, and Navy Documents:	
JAFAN 6/9	Joint Air Force-Army-Navy Physical Security Standards for Special Access Program Facilities, 23 March 2004
Military Standards:	
MIL-PRF-32216A	Performance Specification: Evaluation of Commercial Off-The-Shelf (COTS) Manuals and preparation of Supplemental Data
MIL-STD 130M	Identification Marking of U.S. Military Property
MIL–STD–3007F	Department of Defense Standard Practice for Unified Facilities Criteria and Unified Facilities Guide Specifications
Mil-STD-38784	Including Notices, Department of Defense Standard Practice for Manuals, Technical: General Style and Format Requirements
MIL-STD-40051-2	Department of Defense Standard Practice: Preparation of Digital Technical Information for Page Based Technical Manuals
MIL-STD-882	System Safety Program Requirements

National Electrical Manufacturers Association:	
NEMA 250-2003,	Enclosure for Electrical Equipment (1000 v max)
NEMA ICS 1	Industrial Control and Systems General Requirements
National Fire Protection Association10/12/2021	
NFPA 70,	National Electrical Code, 2020
NFPA 101	Life Safety Code,2021
NFPA 110	Standard for Emergency and Standby Power Systems
NFPA 111	Standard on Stored Electrical Energy Emergency and Standby Power Systems,
NFPA 731	Standard for the Installation of Premises Security System
National Institute for Standards and Technology:	
NIST Special Publication 800-37, Rev 1	Guide for applying the Risk Management Framework to Federal Information Systems, February 2010
NIST Special Publication 800-40v2	Creating a Patch and Vulnerability Management Program, November 2005
NIST Special Publication 800-53, Rev 4,	Security and Privacy Controls for Federal Information systems and Organizations, April 2013
NIST Special Publication 800-53A, Rev 1	Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010
NSTISSI N0.7003	Protective Distributive Systems (PDS), 13 December 1996
United Facilities Criteria:	
UFC 4–020–01	Unified Facilities Criteria: DOD Security Engineering Facilities Planning Manual
UFC 4–022–01	Unified Facilities Criteria: Security Engineering: Entry Control Facilities/Access Control Points
UFC 4-510-01	UFC Design: Military Medical Facilities
Underwriters Laboratories (UL) Standards:	
UL 50	Standard for Enclosures for Electrical Equipment, Non-Environmental Considerations

UL 50E	Standard for Enclosures for Electrical Equipment, Environmental Considerations ,2015.
UL 294,	Standard of Safety for Access Control System Units, 8 October 2018
UL 634,	Standard for Safety for Connectors and Switches for Use with Burglar-Alarm Systems
UL 639	Standard for Safety for Intrusion-Detection Units
UL 687	Standard for Safety Burglary Resistant Safes, 18 February 2020
UL 864	Control Units and Accessories for Fire Alarm Systems, 1 December 2014
UL 1076	Standard for Proprietary Burglar Alarm Units and Systems, 16 February 2021
UL 1610	Standard for Central-Station Burglar-Alarm Units 4th Edition 5 July 2016
UL 1635	Standard for Digital Alarm Communication System Units, 13 April 2018
UL 1981	Standards for Central Station Automation Systems, 29 October 2019
UL 2044	Standard for Commercial Closed-Circuit Television Equipment, 2008, revised 2016
UL 62368	Standard for Audio/Video, Information and Communication Technology Equipment 22 October 2021

APPENDIX B – DEFINITIONS

Access	Defines a zone as being in the disarmed or day mode. Alarms are inhibited. The status of all devices in the zone is disarmed.
Access Control	Access Control ensures that resources are only granted to those users who are entitled to them.
Access Control Point	Points at the outermost boundary of the installation (or cantonment area of large installations) where security checks can be performed on personnel, vehicles, and materials before potential threats can gain proximity to Army assets.
Access Control Unit	Synonymous with the Local Controller or Entrostar™
Alarm	Defines a point as being in an active ALARM state. Sensor has been activated in zone according to its detection technology. Needs operator action or response.
Annunciate	Sensor(s) reporting an alarm(s) to the control console via PCU
Anti-Pass back	An attempt was made to gain entry to an area twice with the same card. When configured, the purpose is to prevent a card holder from passing their card back to a second person to enter the same controlled area.
Application Programming Interface	A set of defined rules that explain how computers or applications communicate with one another. APIs sit between an application and the web server, acting as an intermediary layer that processes data transfer between systems
Armed	Defines a zone as being in the armed or secure, night mode, with all alarms active.
Army Standard for Access Control Points	Provides standards for Army access control points (ACPs) (https://www.us.army.mil/suite/doc/8912967).
Asset	Any resource requiring protection.
Biometric Identifier	A set of biological characteristics that are unique to an individual and may be used to positively identify a person. Examples of biometric identifiers are fingerprints, facial characteristics, iris pattern and hand geometry.
Biometric Input Device	An input device which senses the biometric parameters being used as an identifier. Examples are a fingerprint pad, an iris scanner, a hand geometry sensing plate, and other biometric sensors. The input sensor may have processing circuits and associated electronics included within its enclosure (housing). It may operate in a standalone mode directly communicating with the local processor or it may be operated in conjunction with other devices such as a card reader or keypad and communicate with a remotely located database.
Biometrics	Biometrics use physical characteristics of the users to determine access.

Boundary Penetration Sensors	Sensors that detect penetration through perimeter barriers, such as walls, ceilings, duct openings, doors and windows and include balanced magnetic switches, glass break sensors, grid wire sensors, passive ultrasonic sensors and vibration sensors.
Capacity Proximity Detectors	A sensor designed to detect when an intruder approaches or touches a protected item within a protected area.
Card	A type of access token for use with entry control equipment. Made of plastic, it is similar in size and appearance to a credit card.
Central Monitoring Station	Designated hub or Installation that provides regional ICIDS monitoring of multiple Installations.
Closed Circuit Television (CCTV)	Television that serves several different functions, one of which is physical security. As it pertains to the field of physical security, CCTV is used to augment, not replace, existing intrusion detection systems (IDS) or security patrols. It is not used as a primary sensor, but rather as a means of assessing alarms. CCTV also may be used as a surveillance means, but if used in this way, it will augment, not replace, existing IDS.
Common Access Card (CAC)	An identification card displaying the cardholder's name, photo, and organization. The CAC is the DOD implementation of Homeland Security Presidential Directive 12 that requires Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.
Controlled area	A type of restricted area in which access to the public is denied unless certain entry controls are met. This type of area has the least restrictive conditions. Usually, the required controls for entry include a military identification card or proof of identification by another Federal or state government document, and a need for access. Once authorized to enter, movement within the area is not controlled. An example of a controlled area is an Army installation or facility where entry is granted at the IACP. A controlled area may also be a building that is not accessible by the public because entry is controlled by proof of identification that the individual is an active or retired member of the military (for example, commissary, post exchange).
Damage	A deformation, corrosion, loosening of parts, breakage, change of fit of any part, physical change which impairs the mechanical integrity of the component, evidence of delaminating or water penetration into integrated circuits, printed circuit boards or parts resulting in nonconformance of a component to the provisions of the performance specification.

Data Authentication System (DAS)	Encryption of Intrusion Detection System (IDS) data using an algorithm based on the AES, which complies with FIPS 197, for the purpose of ensuring the integrity and validity of transmitted data.
Defer	To place an alarm into a deferred queue for later processing. An available option in the Operator applications alarms queue.
Delay	The use of obstacles to increase the adversary task time. Obstacles can be passive barriers (e.g., locks, fences, and Jersey walls) or active barriers (e.g., engagement by the response force, pop-up vehicle barriers).
DES	Provides secure data communications using NIST validated AES as specified in FIPS-197 and conforming to the requirements of FIPSPUB-140-2, for data communications between Information Systems (IS)within a network (if architecture dictates). The DES may be internal or external. The DAS shall be physically compatible and electrically interoperable with IS equipment, hardwired data links and other system components, including the optional fiber optic communication interface and the optional RF/microwave data link. It shall derive operating power from existing power source(s). The DES shall provide the capability to remotely install or change the Premise Control Unit (PCU) encryption key. The DES shall provide data encryption for the specified communication channels. A DES secure communication channel shall require installation of a DAS device at each end of the communication link. The DAS shall provide sufficient capacity, flexibility, and redundancy to allow any or all eligible communication channels of IS within the network to operate simultaneously in the encryption mode.
Detection	The discovery of an adversary when a sensor detects an abnormal event. The operator assesses the alarm to determine if it is valid (an adversary is detected) or invalid (a nuisance or false alarm)
Device Server	The Device Server is a computer on the network that manages the communications between the PCU and the File Server. The Device Server polls each PCU for information through the Poller Mux cards at regular intervals and relays the information gathered from the PCU to the Application Server.
Digital Input or Output	Having only two states, 1 (on) or 0 (off).
Door Forced	Alerts the operator that a door has been forced open without valid access granted.
Duress	An alarm raised discreetly by a person in a zone with an intruder.
Duress alarm system	A method by which authorized personnel can covertly communicate a situation of duress to a security control center or to other personnel in a position to notify a security control center. (DOD 5100.76–M)

Duress Sensor	A switch designed to be incorporated into IDS to provide individuals located within a protected area, a means of signaling, in a covert manner, that they have been placed under duress. A duress sensor should never be annunciated by a local audible alarm.
EMI	Disruption of the alarm signal caused by electromagnetic disturbance. This can be caused by lightning, power line noise and other electrical devices.
Enabled	Defines a point or zone as being enabled. This is the active or normal state.
Environmental Alarm	Type of nuisance alarm. An environmental alarm is the result of sensor activation caused by natural causes such as wind, lightning, or thunder.
Exclusion area	A type of restricted area that contains a security interest or other material of such vital importance that proximity resulting from entry into the area constitutes access to such security interest or material. Therefore, entry into an exclusion area is more restrictive than into a limited area. An exclusion area is usually located within a limited area. In addition to conditions required for entry into the limited area, further entry into an exclusion area is disqualified from everyone unless they are identified through an entry control roster, electronic access control system, or exchange badge system for the exclusion area and can meet two conditions: (1) The person must be a current member of the Personnel Reliability Program, and (2) the person is a participant in a two-person access requirement within the area. Movement within an exclusion area is controlled by the two-person rule. All other individuals allowed entry into an exclusion area must be escorted by person who can satisfy the previous two conditions. Persons under escort cannot satisfy the two-person requirement and are not considered to have access to the security interest.
Explosives	Any chemical compound, mixture, or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite, trinitrotoluene (TNT), C–4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitroguanidine.
Facility	Any single building, project, or site.
Failed	Communications to a zone has failed. Can also represent a failed sensor or point.

Failure	Failure of the components listed in 3.2.1 is defined as any relevant malfunction that results in loss of the ability of the equipment to perform its intended function. Where functional redundancy exists failure is defined as total loss of that function.
False Alarm	A false alarm is the result of sensor activation for no apparent reason.
False Alarm Rate (FAR)	The number of alarms produced by unknown sources during a given period.
False Rejects	False Rejects are when an authentication system fails to recognize a valid user.
File Server	Database Server
Global information Grid (GIG)	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. The GIG supports the DOD, the National Security Agency, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.
Local Controller	A single/dual door (portal) controller that can be used with an entry device, locking mechanism and an exit device. Monitors and enables users to enter or exit alarmed zones and reports unauthorized entry attempts
High risk personnel	Personnel who, by their grade, assignment, value, location, or specific threat, are more likely to be attractive or accessible terrorist targets.
Independent Power Source	A power source (usually a battery) that is independent of any other source.
Input	A point that receives data from equipment and transmits it on to the system database. Often referred to as a control point.
Insecure	An alarm has caused the zone breach, insecure status.
Installations	Such real properties as reserve centers, depots, arsenals, ammunition plants (both contractor- and Government-operated, hospitals, terminals, and other special mission facilities, as well as those used primarily by troops.

Integrated Commercial Intrusion Detection (ICIDS)	US Army Program of Record for Physical Security Systems that includes but not limited to Intrusion Detection, Access Control and CCTV
Interior Sensor	Sensors that perform one of three detection functions: detection of an intruder penetrating the boundary of a protected area, detection of an intruder's motion within a protected area and detection of an intruder touching or lifting an asset within a protected area.
Intrusion Alarm	An intrusion alarm is the result of sensor activation caused by an actual intrusion or an attempted intrusion into a protected area.
Intrusion Detection System	The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm monitoring station. The IDS will be an approved DOD standardized system, such as the Joint Service Interior Intrusion Detection System or MACOM-approved commercial equipment.
Invalid / Unknown Card	Indicates that a person has attempted entry into a controlled area with an unknown or unregistered card.
IP Address	A unique string of numbers separated by periods that identifies a computer using the Internet Protocol to communicate over a local or domain network.
Left Open	Alerts the operator that a door has been left open after a valid access was granted.
Limited area	A type of restricted area that is more restrictive than a controlled area because in addition to the need for access and proof of positive identification, entry is limited to only those individuals whose names have been previously placed on an entry control roster signed by the controlling authority (installation/activity commander) or who have been enrolled in an electronic access control system or are part of an approved exchange badge system. Entry is granted to those limited individuals listed on the entry control roster, enrolled in the electronic access control system, or members of an exchange badge system after verification at the entry control facility. Movement within a limited area is not controlled for those authorized unescorted entry. A limited area is normally a buffer zone for an exclusion zone because access to the security interest contained within the exclusion area remains prohibited. Commanders may require escorts for un-cleared personnel with a need for entry into the limited area.

Line Replaceable Unit	The LRU is defined as the lowest level component that is normally replaced at the installation level. An example of an LRU might be a printed circuit board rather than a chip or other component mounted on a printed circuit board.
Line Supervision	Line supervision is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the system. The telephone or dedicated lines that transmit the alarm signals from the protected area to the monitoring station must be protected to prevent interruption of the alarm signal. To ensure such integrity, the transmission lines should be electronically supervised. Line supervision refers to the protection various signaling techniques incorporate, such as random tone patterns or data encryption. The signal shall not repeat itself within a minimum six-month period.
Local Station Control Console	Primary server of the ICIDS. Manages the information from the Premise Control Unit. Manages multiple ICIDS Databases. Synonymous with the Primary Monitoring Console (PMC)
Log In	The action of formally entering an application. Log in by entering the proper username and password.
Log Out	The action of signing out of an application. Upon log out, the user is often offered the option of saving any alterations made to the data within the application.
Low Battery	Indicates that the charging circuit on a PCU has detected that the battery voltage is low.
Maintenance	Indicates that a zone/building has been placed into maintenance mode by a maintenance technician or consumer.
Map	A graphical representation in the system (zone, text, etc.). Designed to be used by day-to-day users of the system.
Mission essential and vulnerable areas	Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's State National Guard, or MUSARC mission. This includes areas nonessential to the installation's/facility's operational mission but which, by nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.
Monitoring Station	Process and display alarm data from the remote sensor areas or zones and system status information. Also, used to issue commands or control instructions. Synonymous with the Operator Workstation (OPWS).

Motion Sensor	Sensors designed to detect intruder motion within a protected area. The sensors may be active or passive and include Ultrasonic Motion Sensors, Interior Microwave and Passive Infrared Motion Sensors.
Node Failure	Indicates one or more Premise Control Units or Access Control Units have lost communications.
Nuisance Alarm	A valid detection, but it is an occurrence that has no security implication, such as when a dog leans against a fence. Reduced or eliminated with filtering technologies.
Nuisance Alarm Rate (NAR)	Nuisance alarms over a given period
Personal Identity Verification (PIV)	A process to verifying a person's identity.
Physical Access Control System	Equipment and related SW that restricts access to controlled areas by identity verification. Synonymous with Entry Control Equipment (ECE).
Physical Security	That part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, materiel, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft. Operations security (OPSEC) and security targeted against traditional criminal activity are included.
Physical Security System Architecture	A system ensuring that IDS components designed by the various services are compatible when used together. Air Force is responsible for systems architecture.
PIN (Personal Identification Number)	A four-digit code that can be assigned to a user. When assigned, the card holder must key in the PIN whenever presenting a card, or when accessing or securing a zone.
Portal	A door, turnstile, etc., providing entrance to a zone. A portal is kept locked and can only be opened by entry of a valid card.
Premise Control Unit	Alarm input board that monitors input devices (e.g., sensors) and controls output devices and provides communications for other components within the ICIDS system. Synonymous with the Remote Area Data Collector (RADC).
Resolution Codes	Codes that provide a general description of alarms produced and/or the action required to resolve them. If the system has been set up to incorporate resolution codes, the user must assign one to each alarm before attempting to process it.
Response	The actions taken by the response force to prevent adversary success

Restricted area	An area defined by an established boundary to prevent admission unless certain conditions or controls are met to safeguard the personnel, property, or material within. These areas are not to be confused with those designated Federal Aviation Administration areas over which aircraft flight is restricted. All restricted areas will be marked and can control access to the area. Restricted areas are identified by the different types of conditions required to permit entry. Conditions for entry vary depending on the nature and degree of importance of the security interest or government assets contained within a restricted area. The three types of restricted areas are controlled, limited, and exclusion.
Risk	The degree or likelihood of loss of an asset. Factors that determine risk are the value of the asset to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the asset to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the asset.
Sensitive Compartmented information (SCI)	Classified information that can be protected only with security measures authorized by AR 380–28.
Sensitive Compartmented information facility (SCIF)	Facility for SCI and governed by AR 380-381, Special Access Programs.
Shunted	Sensor placed in bypass mode. Upon configuration, a point or sensor that is bypassed and will not report state changes to the system. Prevents alarms or status information from reporting.
Special Access Programs (SAP)	A security program established under the provisions of EO 12958 and approved by the Deputy Secretary of Defense to apply extraordinary security measures to protect extremely sensitive information. SAP status is defined by DODD 5200.1–R. Army SAPS include SAPS sponsored by others but for which the Army is designated executive agent.
Systems Administrator Station	Workstation for performing system user functions without interrupting the Local Station Control Console and the Monitoring station. Also works as a Badging Station. Synonymous with the Remote Status Monitor.
Tamper	Alerts the operator that a sensor, panel, or cabinet has been tampered with.
Unified Facilities Criteria (UFC) 4–020–01	Supports the planning of DOD facilities that include requirements for security and antiterrorism.
Unified Facilities Criteria (UFC) 4–022–01	Provides construction standards for these for entry control facilities/access control points.
Uninterruptible Power Supply	Provides backup power to critical ICIDS components. Also UPS provides backup power for 24-hours for SCIF's.

Zone	An alarmed area monitored and controlled for entry and intrusion independent of other alarmed areas.