25 – Intrusion Detection and Access Control Systems for Secured Spaces
354th Civil Engineering Squadron
OPR: CES/CEOFA
ISSUED: 22 August 2017

Purpose

This standard shall be used in conjunction with applicable standards as listed in Paragraph 1 for planning, development, and commissioning of Intrusion Detection Systems (IDS) and Access Control Systems (ACS) associated with secure spaces on Eielson Air Force Base, AK. Examples include, but are not limited to; the development of scopes of work, DD1391 documentation, drawings, specifications and request for proposals. These standards will serve as the primary IDS and ACS criteria reference documents for services provided by architectural and engineering (A&E) firms and consultants in the development of both design-bid-build and design-build contracts. This document is not intended to be used in lieu of detailed design documents in the procurement of Facility construction. No part of this document should be considered inclusive to all government requirements.

In accordance with the "HQ USAF/A7S, Non-Nuclear Intrusion Detection System Equipment Approval" memorandum, dated 29 January 2014 Eielson AFB is allowed to use only the Will-Burt Annunciator, Advantor Annunciator, or Vindicator Annunciator; the current Eielson configuration is with Vindicator. Therefore, the only Electronic Security System (ESS) that is compatible with Eielson AFB systems is the Honeywell Vindicator Security Platform.

1. References

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

1.1.1. American National Standards Institute (ANSI)

a. ASC/X9 X9.52 (1998) Triple Data Encryption Algorithm Modes of Operation

1.1.2. Institute of Electrical and Electronics Engineers (IEEE)

a. IEEE 142 (2007; Errata 2014) Recommended Practice for Grounding of Industrial and Commercial Power Systems - IEEE Green Book

b. IEEE C2 (2012; Errata 2012; INT 1-4 2012; INT 5-7 2013; INT 8-10 2014; INT 11 2015) National Electrical Safety Code

c. IEEE C62.41.1 (2002; R 2008) Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits

d. IEEE C62.41.2 (2002) Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits

1.1.3. National Electrical Manufacturers Association (NEMA)

a. NEMA 250 (2014) Enclosures for Electrical Equipment (1000 Volts Maximum)

b. NEMA ICS 1 (2000; R 2015) Standard for Industrial Control and Systems: General Requirements

1.1.4. Telecommunications Industry Association (TIA)

a. TIA-568-C.1 (2009; Add 2 2011; Add 1 2012) Commercial Building Telecommunications Cabling Standard

1.1.5. U.S. National Archives and Records Administration (NARA)

1.1.6. Code of Federal Regulations, Title 47, Part 15 (47 CFR 15) Radio Frequency Devices

1.1.7. Underwriters Laboratories (UL)

a. UL 1037 (1999; Reprint Dec 2009) Safety Antitheft Alarms and Devices

b. UL 1076 (1995; Reprint Mar 2015) Proprietary Burglar Alarm Units and Systems

c. UL 294 (2013; Reprint Feb 2015) Access Control System Units

d. UL 634 (2007; Reprint Mar 2015) Connectors and Switches for Use with Burglar-Alarm Systems

e. UL 639 (2007; Reprint May 2012) Standard for Intrusion Detection Units

f. UL 681 (2014) Installation and Classification of Burglar and Holdup Alarm Systems

g. UL 796 (2010; Reprint Sep 2013) Standard for Printed-Wiring Boards

h. UL 2050 Extent 3

1.1.8. Intelligence Community Directive (ICD)

a. ICD 705 IC Tech Spec Chapter 8

2. Field Equipment

2.1. All computing devices, as defined in 47 CFR 15, shall be certified to comply with the requirements for Class A computing devices.

2.2. Field equipment shall include local processors, sensors and controls; local processors shall serve as an interface between central station(s) and sensors and controls.

2.3. Data exchange between the central station and the local processors shall include down-line transmission of commands, software and databases to local processors, up-line data exchange from the local processor to the central station shall include status data such as intrusion alarms, status reports and entry control records.

2.4. Final connection of field equipment and base owned systems shall be accomplished by government personnel.

3. System Network

3.1. System networks shall interconnect all major components of the system. These networks shall include communications between a central station and any peer or subordinate workstations, enrollment stations, local annunciation stations, portal control stations or redundant central stations as required or identified.

3.2. The systems network shall provide totally automatic communication of status changes, commands, field initiated interrupts and any other communications required for proper system operation.

3.3. System communication shall not require operator initiation or response.

3.4. System communication shall return to normal after any partial or total network interruption such as power loss or transient upset. The system shall automatically annunciate communication failures.

4. Electrical

4.1. Electrically powered ESS equipment shall operate on 120 volt 60 Hz AC sources. 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.

4.1.1. Option A

a. Four (4) hours of uninterruptible backup power is required.

4.1.2. Option B

a. Twenty four (24) hours of uninterruptible backup power is required. This may be provided by an uninterruptible power supply (UPS), batteries integral to the ESS, generators, or any combination thereof.

4.2. In the event of primary power failure, the system must automatically transfer to an emergency electrical power source without causing alarm activation, equipment at the monitoring station(s) must visibly and audibly indicate a failure in a power source or a change in power source.

4.3. All annunciators and data transmission subsystem components must transmit a "low-battery" message before their functions degrade

5. Probability of Detection

5.1. The system shall be able to detect a standard intruder moving through a protected zone; a standard intruder to be a person that weighs 100 pounds or more and is 5 ft. tall or more walking, running, crawling or jumping through a protected zone in the most advantageous manner for the intruder.

5.2. Each zone shall have a continuous probability of detection greater than 90 percent and shall be demonstrated with a confidence level of 95 percent.

5.3. The actual number of tests performed, per sensor, to demonstrate system performance shall be nominated by the Contractor in the performance verification test procedures submitted to the Government for approval in the Group IV Technical Data package.

6. Intrusion Detection

6.1. IDS for each secured space as identified shall contain an independent Premise Control Unit (PCU) from any other spaces within facility.

6.2. Interior areas of the secured area through which reasonable access could be gained, including walls common to areas not protected shall be protected by IDS consisting of motion sensors meeting UL 639 standards and high security switches (HSS) that meet UL 634 level 2 requirements.

6.2.1. Option A

a. A sensor or sensors in combination that constitute a line of detection shall meet material list identified in the “AF/A7S Non-Nuclear Intrusion Detection System (IDS) Equipment Approval” listing.

6.2.2. Entrance door sensors may have an initial time delay built into the IDS to allow for change in alarm status, but shall not exceed 30 seconds.

6.2.3. In the space above or below the secure area a passive infrared motion detection system may be required on a case by case basis.

6.2.4. The Building Management System (BMS) installed on emergency exit door(s) shall be monitored 24 hours a day.

6.2.5. Option B

a. Secured area shall be provided with IDS and alarm zones that are independent from systems safeguarding other protected sites and provide local annunciation of alarms.

b. All alarm activations shall be required to be reset in secure area, any IDS with an auto-reset feature shall have the auto-reset feature disabled.

6.2.6. If a single monitoring station supervises several alarm zones, then the audible and visible annunciation for each such zone shall be distinguishable from other zones.

6.2.7. The IDS’s PCU, associated sensors, and cabling protecting the secure area, shall be separate from and independent of fire, smoke, radon, water, and other such systems. (Note: If an ACS is integrated into an IDS, reports from the access control system shall be subordinate in priority to reports from intrusion alarms.)

6.2.8. All alarm installations must be approved by the Site Security Manager (SSM) and/or the cognizant government security organization.

7. Tamper Switches

7.1. Enclosures, cabinets, housings, boxes, and fittings having hinged doors or removable covers and which contain circuits or connections of the system and its power supplies, shall be provided with cover operated, corrosion-resistant tamper switches, arranged to initiate an alarm signal when the door or cover is moved.

7.2. 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.

8. Data Transmission System (DTS)

8.1. All signal and DTS lines shall be supervised by the system based on transmissions of pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication.

8.2. 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.

8.3. The system shall also initiate an alarm in response to opening, closing, or shorting of the signal and DTS lines.

8.4. 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 Federal Information Processing Standards (FIPS) 197 of Triple Data Encryption Algorithm (TDEA) as described in FIPS 46-3 standards, ASC/X9 X9.52, as a minimum.

9. Physical Protection of Cabling

9.1. Installation must protect the cabling between the sensors and the control unit (called the detection loop) for the IDS.

9.2. IDS cabling may be routed in rigid pipe (e.g., metal conduit or polyvinyl chloride (PVC) or equivalent raceways, these materials must comply with national electric code standards.

9.3. Physically protect permanently installed exterior communications cable data links and circuits using conduit, direct burial, or above-ground installation methods.

10. IDS Event (Alarm) Log

10.1. The IDS shall incorporate within the secure working area, security office, and/or at the monitoring station as identified, a means for providing a historical record of all events through an automatic logging system for no less than 1 year.

11. Miscellaneous System Components

11.1. System components shall be designed for continuous operation.

11.2. Electronic components shall be solid state type, mounted on printed circuit boards conforming to UL 796.

11.3. Printed circuit board connectors shall be plug-in, quick-disconnect type.

11.4. Power dissipating components shall incorporate safety margins of not less 25 percent with respect to dissipation ratings, maximum voltages, and current carrying capacity.

11.5. Control relays and similar switching devices shall be solid state type or sealed electro-mechanical.

12. Perimeter Access/Secure Switches

12.1. An access/secure control station shall be used to place a protected zone in the ACCESS or SECURE mode.

12.2. Keypads shall include an LED or other type of visual indicator display and provide visual and audible status indications and user prompts.

12.3. The switch shall consist of a keypad to accept PINs to allow access/secure events.

12.4. Operation of the access/secure switch shall be restricted to the secure area.

12.5. The switch shall disable zone sensor alarm outputs, but shall not disable tamper alarms, duress alarms, and other 24-hour sensors, as identified.

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

13. Hazardous Environment

13.1. System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers or flying particles, shall be rated and installed according to Chapter 5 of the NFPA 70.

14. ACS Considerations

14.1. ACS for each secured space as identified shall be independent of other spaces to include unsecured areas within same facility.

14.2. A UL 294 listed card reader with an integrated keypad shall be used at all identified portal(s) for secured space.

14.3. Keypads shall include an LED or other type of visual indicator display and provide visual and audible status indications of power conditions, user prompts, and user passage requests whether accepted or rejected.

14.4. Each local processor shall contain an operating system that controls and schedules that local processor's activities in real time.

14.5. The local processor shall have startup software that causes automatic commencement of operation without human intervention, including startup of all connected Input/Output functions.

14.6. Storage for the latest 4000 events shall be provided at each local processor, as a minimum.

14.7. The system shall be able to be configured for a minimum 50 enrollees with a facility-tailorable reference file database containing personal, access authorization, and identifier and verification data for each enrollee as required.

14.8. The system shall annunciate an alarm when the following conditions occur.

15. Submittal of Technical Data and Computer Software

15.1. 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.

15.2. System Drawings should include:

15.2.1. Functional system block diagram identifying wire type and quantity.

15.2.2. Details of connections to power sources, including power supplies and grounding.

15.2.3. Entry control system block diagram and layout.

15.2.4. Intrusion detection system block diagram and sensor layout (including exterior and interior zones) as well as sensor detection patterns.

15.2.5. Software data package consisting of descriptions of application software as specified and major build or version and/or revision.

15.2.6. Materials sheet with manufacturer specifications.

16. Alarm Shop Support

16.1. In the event that a contractor requires 354 CES Alarms shop support for the performance of duties as outlined in a contract or is doing work on an IDS or ACS, the contractor must coordinate with the Alarm Shop Supervisor/NCOIC, 24 to 72 hours in advance for scheduling purposes.