# Immigration and Customs Enforcement
# Office of Professional Responsibility
# Security Division
# Physical Security Operations Unit

# Electronic Security Systems (ESS)
# Scope of Work

# E-PACS/IDS/VSS

# Ft. Benning Georgia Immigrations and Customs Enforcement Advance Training Operations Center

**Version: 2**

**June 18, 2026**

**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to- know" without prior approval of an authorized DHS official.

**Document Control:** At a minimum, this document, and any products made from this document, will be marked as "FOR OFFICIAL USE ONLY," disseminated only on a need-to-know basis, and stored in a locked container or password-protected file or system offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure. When no longer needed, destroy physical copies by shredding, pulping, or burning to assure destruction beyond recognition.

U.S. Immigration and Customs Enforcement

Internal SOW Template Version: 4/8/2022

TABLE OF CONTENTS

SECTION I - GENERAL REQUIREMENTS ..... 3
1. Project Overview ..... 3
2. Project Location and Contacts ..... 3
3. Project Scope ..... 4
4. Compliance ..... 4
5. Qualifications ..... 5
6. Project Site Visit ..... 6
7. Timeline and Benchmarks ..... 7
8. Project Closeout ..... 8
9. Training ..... 9
10. General Notes ..... 10
11. Infrastructure ..... 10
12. Warranty ..... 12
13. Review and Approvals ..... 14

SECTION II - ELECTRONIC SECURITY TYPICAL BLOCK DIAGRAMS ..... 15

SECTION III - ELECTRONIC SECURITY SYSTEMS (ESS) COMPONENT TASKS ..... 16
A. Physical Access Control (PACS) ..... 16
B. Intrusion Detection Systems (IDS) ..... 22
C. Video Surveillance System (VSS) ..... 23

SECTION IV - SECURITY SYSTEMS DETAILS ..... 28
A. Interior Physical Access Control System (PACS) Devices ..... 28
B. Interior Intrusion Detection System (IDS) Devices ..... 28
C. Interior Video Surveillance System (VSS) Devices ..... 30
D. Exterior Physical Access Control System (PACS) Devices ..... 30
E. Exterior Video Surveillance System (VSS) Devices ..... 30

ATTACHMENTS ..... 32
PACS Paperwork ..... 32
ESS Component Checklists ..... 32
MegaCenter Alarm Requirements (MAR) Form ..... 33

## SECTION I - GENERAL REQUIREMENTS

### 1. Project Overview

1.1. The U.S. Immigration and Customs Enforcement (ICE) is the premier Federal Law Enforcement Agency within the U.S. Department of Homeland Security with primary mission to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade and immigration.

1.2. ICE requires the Contractor/vendor to design and install our Electronic Security Systems (ESS). The Contractor proposed ESS solution must reflect consideration for the sensitivity of the ICE mission, the safety and security of all personnel, information, facilities and the requirements set forth in this document.

### 2. Project Location and Contacts

2.1. The place of work performance is the ICE office located at Ft Benning Georgia Immigration & Customs Enforcement Advanced Training Operations Center.

2.2. The following ICE Office of Professional Responsibility (OPR) Field Security Manager **(FSM)**, or his/her supervisor in their absence, is the final technical security authority for this project:

**Brian K. Alexander**
**Brian.K.Alexander@ice.dhs.gov**
**(504) 239-2738**

2.3. The ICE Office of Assets and Facilities Management (**OAFM**) Project Manager is:

**Connor Kreston**
**Facilities Portfolio Manager**
**Connor.B.Kreston@associates.ice.dhs**
**.gov**
**Mobile: (215) 630-8171**

### 3. Project Scope

3.1. ICE requires the Security Contractor to design, procure, install, configure, program, test, document, maintain components and installation work through the warranty period and train personnel on a turn-key Electronic Security Systems (ESS). The ESS sub-systems shall include but may not be limited to:
(1) Physical Access Control System (PACS); (2) Intrusion Detection System (IDS); and (3) Video Surveillance System (VSS).

3.2. All programming, software loads and maintenance will be done on-site. The Contractor will not be authorized remote (client) access to the network or systems to perform maintenance, troubleshoot problems, or apply software changes.

3.3. A description of acceptable fielded security devices and typical ESS block diagrams are included in this document for reference. The Contractor may propose other ESS solutions they believe will be beneficial to ICE.

3.4. A detailed listing of all ESS equipment product data (including quantity, make, model, part numbers) and fielded device locations must be provided by The Contractor and approved by the FSM to

ensure compliance with this document.

3.5. The Contractor shall provide drawings for each ESS component sub-system (PACS, IDS, VSS) and a combined ESS drawing with all component sub-systems. Drawings shall list each component individually (i.e. workstation(s), panels, enclosures, power supplies, fielded devices) and their installation locations. The Contractor shall ensure that all mounting details and all devices are cross referenced in the drawings including all data cabling that interconnect components, and all power connections.

3.6. Any conflicts between the requirements of this Security SOW and any other project requirements or specifications, to include the ICE Facilities Design Guide (FDG), will be identified to the ICE OAFM Project Manager and FSM for resolution. All coordination and resolution shall occur through prescribed GSA channels.

3.7. This Scope of Work (SOW) will be periodically reviewed to assess the future use of the components described within. ICE reserves the right to change system components listed within this SOW through proper coordination through prescribed GSA channels.

## 4. Compliance

4.1. In compliance with General Services Administration (GSA) specifications or in the absence of GSA Schedules the following will apply and are required for all U.S. Immigration and Customs Enforcement (ICE) security system projects: Homeland Security Presidential Directive 12 (HSPD-12), Office of Management and Budget (OMB) M-19-17, M-11-11 and M-05-24, Interagency Security Committee (ISC) Standards, Department of Homeland Security (DHS) Management Directive System, National Institute of Standards and Technology (NIST) 800-116 and 800-53, Federal Information Processing Standards (FIPS) 201-2, and Underwriters Laboratory (UL).

4.2. All work performed shall comply with national and local codes, ordinances, regulations, and other legal requirements of the authority having jurisdiction (AHJ), which bear on the performance of work. The Contractor is to acquire all necessary permits for the completion of this work. All ESS components provided by the Contractor are required to meet applicable regulations, directives and guidelines for that respective activity.

4.3. The Contractor shall comply with the most recent applicable codes and standards published by the National Fire Protection Association (NFPA). This includes, but is not limited to, NFPA 1 Fire Code, NFPA 70 National Electric Code (NEC) and NFPA 101 Life Safety Code.

## 5. Qualifications

5.1. The Contractor or Sub-Contractor shall strictly adhere to engineering, installation and testing procedures in accordance with the requirements of GSA and equipment manufacturer(s) and maintain a service center near the project site or the ability to expedite parts to the project site within 24 hours.

5.1.1. Contractor or sub-Contractor for PACS - Due to DHS PACS Modernization requirements, Software House C•CURE 9000 is the only Physical Access Control System (PACS) that may be used; no other PACS systems may be substituted for this project. The Contractor or Sub-Contractor for PACS must:

5.1.1.1. Be an approved vendor of Security System Integration, Design, Management, and Life Cycle Support under the GSA Multiple Award Schedule (MAS) program: SIN541330SEC. This requirement includes services related to PACS design, integration, implementation, and installation/testing. Employees of offerors of this SIN are CSEIP (Certified System Engineer

ICAM PACS) certified, and such certification can be verified at IDmanagment.gov." Offerors under this SIN have at least one employee who is CSEIP (Certified System Engineer ICAM PACS) certified and such certification can be verified at IDmanagment.gov. GSA eLibrary Contractor Listing

5.1.1.2. Be listed as a Software House Enterprise Partner in the Software House Dealer-Certification Program (http://www.swhouse.com/support/Dealer_Certification.aspx), or provide proof of certification.

5.1.1.3. Be qualified to perform the software application functions for Software House C•CURE 9000 Enterprise installation and connectivity back to ICE HQ's infrastructure

5.1.2. Contractor must provide a minimum of three past performance references demonstrating successful implementation and configuration of a HPSD-12 compliant CCURE9000 solution within the past 5 years.

5.2. Technician - All ESS components shall be installed by an Electronics or Security System Installation Technician. The technician must have sufficient experience, knowledge, skills, and abilities to perform the required tasks for the installation of the ESS as outlined in this scope. The followingskills are preferred:

- Possess a 2-year degree or certification in the electronics discipline from an accredited educational institution or trade school
- Be proficient at maintaining, repairing, and installing access control, intrusion detection/alarm and IP video systems
- Possess the ability to isolate network deficiencies, equipment failures and operational anomalies through use of technical manual reference, diagnostic equipment/software and established troubleshooting techniques
- Have a working knowledge of network architecture with an understanding of IP configuration and transport principals
- Experience in how to run and install conduit and cabling per NEC code

5.3. Specialized Technician - A Specialized Technician for PACS must possess all Technician qualifications as identified above and one of the following current Tyco Software House certifications:

- C•CURE 9000 System Installer/Maintainer
- C•CURE 9000 Advanced Integrator

5.3.1. The certification shall be provided to the FSM upon award of the contract.

5.3.2. During the installation and testing phase, the Contractor shall make no substitutions of specialized technicians unless the substitution is necessitated by illness, death, termination of employment or other non-discretional reason. The Contractor shall notify ICE personnel within five (5) business days after the occurrence of any of these events and provide a detailed explanation of the circumstances necessitating the proposed substitution, complete credentials for the proposed substitute, and any additional information requested by ICE personnel. All proposed substitutes shall possess the same minimum qualifications as those of the persons being replaced. The ICE personnel will notify the Contractor within fifteen (15) calendar days after receipt of all required information of the decision on the substitution.

5.4. Project Manager - The Contractor shall also ensure that a Project Manager is dedicated to the project from contract award until project acceptance is achieved. The Project Manager shall have:

5.4.1. A minimum of four (4) years of progressive experience in the security systems field, including at least three (3) years in a management capacity directing security systems implementations, preferably on behalf of a federal client.

5.4.2. The Project Manager should also demonstrate experience managing projects of similar size and scope to this ICE project.

5.4.3. The Contractor shall ensure that the Project Manager is on-site for all critical phases of the project. Critical phases include project kickoff, all testing phases for project closeout, final ICE acceptance, and any security coordination meetings to resolve critical issues.

5.5. Systems Engineer - A Systems Engineer with demonstrated experience in the implementation of PKI and federal ICAM architectures for E-PACS of similar size and scope to this ICE project must be used. Professional services by CSEIP Certified Staff required for system installation, on site configuration, commissioning, documentation and acceptance tests.

5.6. The Systems Engineer shall have attained:

5.6.1. Software House C•CURE 9000 Advanced Integrator or C•CURE 9000 Enterprise Architecture certification, and

5.6.2. Be a current Certified System Engineer ICAM PACS (CSEIP) listed on the Secure Technology Alliance Registry (https://www.securetechalliance.org/activities-cseip-registry/).

## 6. Project Site Visit

6.1. Prior to commencing work, the Contractor is required to perform a site walkthrough with the GSA, ICE Field Security Manager or designated alternate and the local ICE program office management to discuss aspects of the facility and job specific requirements, specific work methods and proposed schedules. If the FSM is not available to meet at the project site, the Contractor may request a conference call through GSA.

6.1.1. The Contractor shall become familiar with local conditions under which work is to be performed and correlate observations with requirements of contract documents.

6.1.2. The Contractor shall identify areas of concern, review important procedural and safety precautions, and agree upon desired installation timetables through a project plan developed by the Contractor.

6.1.3. Before ordering any materials or performing work, the Contractor shall verify space requirements and be responsible for their correctness.

6.1.4. For observation(s) that should be made during the site visit no allowance for claims of concealed conditions by the Contractor shall be made. If in-wall inspections are requested but not allowed, the Contractor shall note this on their quote.

6.1.5. Based on NFPA fire code requirements all doors shall be identified as either *fail safe* or *fail secure* during the walkthrough. Doors that require delayed egress will also be identified. ICE

perimeter doors and high security doors will typically be *fail secure* (normally locked) while yet allowing appropriate egress.

## 7. Timeline and Benchmarks

7.1. The requirement to provide a turnkey solution will necessitate the Contractor to coordinate several actions and deliverables with the Architectural Engineer, General Contractor, other sub-contractors and various ICE program offices. All coordination shall occur through prescribed GSA channels.

7.2. Typically, within 30 days of award, the Contractor shall provide, or incorporate in the overall project schedule, a plan which will address date of completion for the following administrative benchmarks. This information should be displayed in a Gantt Chart or other timeline product with key dates annotated. Please note that expedited coordination may be required for small projects or urgent circumstances.

| Activity / Deliverable | Benchmark |
|---|---|
| Provide final security design/drawings, device lists and updated project schedule | Within 30 days of contract award |
| Provide product data submittal, proof of certification, etc. | |
| Provide all PACS paperwork (port charts, Input/Output worksheets, etc.) and MegaCenter Alarm Requirements (MAR) form to FSM for review and approval.<br>Local ICE Office to provide PACS personnel worksheet | |
| Coordinate installation of IP connection with project team | |
| Coordinate with FSM to provide necessary information for Site Security Addendum | |
| Provide final copy of ICE approved MAR form to FPS MegaCenter for programming via FSM. (Minimum 3- | No later than 30 days prior to projected test and acceptance date |

| | |
|---|---|
| day turnaround by FPS) | |
| Provide confirmation of test and acceptance date | |
| Provide Letter of Completion and completed ESS COMPONENT CHECKLISTS to FSM; place approved Port Charts in each PACS panel enclosure | No later than 14 days prior to projected test and acceptance date |
| Provide training, materials, handouts, passwords, and O&M Manuals (1 complete set) | On projected training date |
| Completion of punch list corrections | Within 14 days of discovery |
| Provide closeout docs | Within 30 days of project completion, unless specified otherwise by GSA |

## 8. Project Closeout

8.1. When the Contractor has completed all ESS work, the Contractor is to test and certify the work performed has been completed, and the systems/hardware provided are in good working order. A Letter of Completion must be signed by a senior company official on letterhead identifying each task and ESS component applicable to the certification. The Contractor must complete the **ESS COMPONENT CHECKLISTS** referenced at the end of this document. The Contractor must follow the prescribed GSA channels when submitting certifications.

8.2. Approximately two weeks after receipt of the Letter of Completion, the ICE Field Security Manager, or designated alternate, and the Contractor will perform a final walk-through inspection and acceptance test of the ESS to ensure the system is complete and acceptable. Inspections and tests will be conducted during the final walk-through, including but not limited to the following:

8.2.1. During the inspection, the Contractor shall demonstrate all equipment and system features, to include emergency power solution demonstration, to ICE Field Security Manager.

8.2.2. Any portions of work found to be deficient or not in compliance with these requirements must be responded to and/or corrected within 14 days. A reasonable time extension may be granted as determined by ICE Field Security Manager. Upon correction of deficiencies, the Contractor shall submit a request in writing for another acceptance test with the ICE Field Security Manager.

8.2.3. After all deficiencies have been corrected and prior to the final acceptance test walk-through there will be a one-week monitoring period of all installed equipment to ensure proper operation.

8.2.4. If all work is found to be acceptable and in compliance with the requirements, the Government will issue a letter of acceptance.

8.2.5. Additional testing may be done or required by the ICE Field Security Manager.

8.3. The start date of the beneficial use and warranty will not commence prior to a successful final walk-through test. Failure of any contractor-provided hardware or software system to perform as specified will be construed as a failure to comply with requirements of the contract.

8.4. The Contractor will provide an as-built package including one electronic PDF format file and three (3) hard copies of the Electronic Security Systems (ESS) diagrams identifying the locations of all ESS components, unless directed otherwise by the FSM. This will include but is not limited to floor plans, riser diagrams, port charts, door details and device wiring details. Additionally, the as-built package shall contain any other deliverable items to include documents generated as a result of the final walk-through checklist and acceptance testing.

8.5. The Contractor shall provide a training sign-in roster with the closeout documents. The roster shall include a description of the topics covered, date of training, name and signatures of attendees, and name and signature of instructor.

## 9. Training

9.1. The Contractor shall provide training upon completion and acceptance of the ESS. Training services must provide attendees with the necessary skills to configure, install, operate, and troubleshoot installed security systems and devices. Training is to be a combination of face-to-face lecture and lab instruction with emphasis on hands-on activities. Operational system hardware shall be utilized during training to provide attendees with installed security systems environment familiarization.

9.2. The Contractor will provide a minimum 4-hour basic training session to system operators. The dates and times of each session shall be jointly determined by the ICE supervisor, the Field Security Manager and the Contractor.

9.3. Training material used, a complete set of product manuals, quick reference guides, and a certificate of training completion are to be given to each participant.

9.4. Training will cover all ESS components:

9.4.1. Physical Access Control System (PACS) training topics will include:

- Location and identification of PACS panels and enclosure keys
- Reading controller status and diagnostic information from LCD display
- Identifying card reader type
- Recognition of audio and visual indicators from card readers
- Identifying electronic locking device type (electric strike or mortise electrified lockset)
- Function of Request-to-Exit (REX) device and Door State Monitor (DSM)
- Overview and maintenance of emergency power (how to identify correct battery type and replace, if needed)

9.4.2. Intrusion Detection System (IDS) training topics will include:

- Location and identification of IDS panels and enclosure keys
- Adding and removing personnel from the system (manually via the keypad)
- Activating the Duress and resetting
- Location and resetting of any local Duress annunciation devices
- Performing an annual test with the MegaCenter
- Recognizing and investigating zone/device faults
- How to bypass and un-bypass a zone/device
- Viewing zone/device status
- Resetting sensors
- Silencing and clearing alarms via the keypad
- Overview and maintenance of emergency power (how to identify correct battery type and replace, if needed)

9.4.3. Video Surveillance System (VSS) training topics will include:

- Location and identification of VSS components and any enclosure keys
- Accessing and viewing cameras
- Moving and focusing cameras

- Changing monitor view mode from single to multicamera mode
- Enabling and administering privacy masking
- Searching, retrieving, and reviewing camera videos
- Downloading and exporting video in open file format and proprietary format
- Adding personnel to the system as both operator and administrator roles with passwords
- Overview and maintenance of emergency power (how to identify correct battery type and replace, if needed)
- How to obtain and install future software and firmware updates

**10. General Notes**

10.1. The Contractor is responsible for damage to any equipment, materials, surfaces or other work disrupted as result of the work. The Contractor will patch and paint any holes and make any repairs to any surface (i.e. walls, doors, ceiling, etc.) that is the result of the Contractor's work. Repair work must match existing construction in grade and likeness. Repair or remuneration will be the sole responsibility of the Contractor. If such work cannot be repaired within a reasonable time, the Government reserves the right to repair damaged equipment, materials or surfaces and offset the costs for such repairs from the awarded contract price. The Contractor will coordinate any anticipated ESS downtime with the ICE FSM and local ICE Program Offices.

10.2. Conflicts between manufacturer's recommendations, specifications, and/or contract documents must be reported in writing to the GSA or Contracting Officer Representative for resolution.

10.3. All passwords for ESS component systems will be changed from the default and be provided to local management in the training session and recorded in the closeout documentation.

**11. Infrastructure**

11.1. The Contractor is to install all wiring including, but not limited to, communication and power support necessary for the operation of the ESS. All wiring shall consist of a single, unbroken run that is free of splices and T-Taps. Wiring for all ESS devices shall be tamper resistant. Wiring for all ESS field devices shall not be exposed (i.e. must be internal to a secure space wall, ceilings, doorframes, etc.) upon installation. Wiring for all ESS components shall fully remain within ICE space possible. When it is not feasible for wiring to remain internal to ICE space the Contactor shall provide a tamper resistant or conduit solution. Writing approval by the ICE Field Security Manager is required for any wiring to be placed externally of ICE controlled space.

11.1.1. In compliance with NFPA 70 NEC and as prescribed by the manufacturer, for PACS card readers, all cabling shall be plenum-grade, listed as having adequate fire-resistant and low smoke-producing characteristics.

11.1.2. Additionally, for PACS, the Contractor shall ensure that all cabling within the enclosure does not exceed one spare pair per cable and is properly terminated with a sleeve to prevent unraveling/unwinding.

11.2. For PACS renovation projects, The Contractor is required to remove the existing access control infrastructure including controllers, card readers and reader modules, power supplies, door position switches, request-to exit devices, and cabling. The Contractor may reuse the existing electrified lock sets. If the Contractor chooses to reuse the existing electrified lock sets, the Contractor shall maintain and at no cost to the government these locks sets during the warranty period. If the Contractor cannot remove

existing cable, they shall terminate all cable ends and tag the cable as "Abandoned Security Wire" and shall not re-use any portion of the legacy PACS wire in the new PACS.

11.3. The Contractor shall securely fasten all ESS wiring above drop ceilings to provide adequate support in an approved method and per the latest version of the GSA PBS-P100 Facilities Standards for the Public Building Service and the National Electric Code (NEC). No wiring may be directly in contact with acoustical ceiling tiles. When replacing existing security system wiring the Contractor must remove abandoned ESS wiring in the ceiling. Line security to end devices shall be implemented through End-of-Line resistors installed at the device.

11.4. High security screws must be used for all ESS components that are exposed (i.e. can be viewed externally or are not secured behind a face plate).

11.5. All wiring shall be labeled at both ends using a numerical system to allow for identification. The wire labeling configuration shall be called out on the as-built ESS drawings to be provided and verified during final walk through and acceptance.

11.6. All grounding is to be performed in accordance with ANSI-J-STD-607-A, NFPA 70 NEC and local codes and practices. Grounding for all electrical work performed by The Contractor shall include, but is not limited to, the highlights below:

11.6.1. Provide grounding at security device location and ensure proper bonding to existingfacilities.

11.6.2. Ensure equipment racks are properly grounded to facility grounding buss bar.

11.6.3. Ensure grounding continuity by properly bonding appropriate cabling, closures, cabinets, conduits, service boxes, and head end equipment.

11.6.4. Power shall only be applied to the system after re-checking for proper grounding of the system and measuring all loops for lack of shorts and open circuits.

11.7. The Contractor will provide lockable electronics equipment rack(s), mounts, slides, shelves and other necessary items to install and mount hardware. (Do not install security equipment into ICE OCIO IT racks(s)/cabinet(s) unless approved in writing by the FSM.

11.8. The Contractor's proposal must identify by square footage all wall and floor space requirements for rack and wall mounted equipment. The Contractor's proposal must identify by amperage all ESS power requirements to ensure appropriate rated circuit breakers are installed in power panels supporting the equipment.

11.9. The Contractor shall coordinate with GSA and OAFM to request that all security equipment be on its own dedicated electrical circuit. The security technician is not responsible for this; a licensed electrician will need to make sure this is accomplished.

11.10. The Contractor is to provide and install all equipment associated power for ESS operation. All ESS management and backend equipment (i.e. reader controllers, IDS panels, etc.) is to be installed in the suite's IT LAN room, security equipment room or other secured area, with approval from the FSM. The Contractor will ensure each equipment room contains sufficient HVAC air circulation and conditioning to support electronic equipment requirements. In each designated equipment room, high quality fire rated plywood, or better, must be installed by the Contractor to support wall mounted backend equipment (i.e. panels, power supplies, etc.).

11.11. The Contractor shall provide and install a minimum of an 8-hour emergency power solution for all ESS hardware. The power solution can be provided through the use of batteries, emergency generators, UPS, or a combination thereof to meet the requirements.

11.11.1. If emergency power is available, via generator, a battery backup must be provided to cover transfer time.

11.11.2. Unless specified differently by the manufacturer, PACS power supplies have 12 Vdc/18ah batteries. Any batteries for IDS panels shall have no less than a 12 Vdc/7ah battery each, unless specified differently by the manufacturer.

11.11.3. For uninterruptable power supply (UPS) installations the UPS must have surge protection and line conditioning features.

11.12. Power supplies to ESS equipment shall be wired to minimize likelihood of accidental disconnect. Unsecured plug-ins to power supplies not located in a rack or enclosure are not acceptable.

11.13. The Contractor shall ensure that all power supplies are rated to power the maximum load plus a minimum of 10 percent spare capacity. ICE defines maximum load as the simultaneous use of all devices at their maximum current requirements.

11.14. The Contractor shall supply voltage load calculations for each Electrical/LAN closet that supports the PACS. The Contractor shall calculate power supplies and back-up capacity by maximum load. Separately, The Contractor shall calculate nominal power and typical duty-cycle to determine the duration of the back-up system.

11.15. The Contractor shall ensure that all power supplies to PACS panel(s) are co-located. The Contractor shall ensure that new power supplies are optioned to transmit a trouble condition to the PACS when the following conditions exist: (a) low battery, (b) AC fail.

11.16. The Contractor shall ensure outputs are individually fused and sufficient for the connected load. The Contractor shall ensure that all battery calculations are based upon peak usage (i.e. simultaneous use of all devices.). The Contractor shall provide batteries sufficiently sized to support the stand-by requirements.

11.17. In compliance with NFPA 101 Life Safety Code means of egress standards and as determined from the pre-construction site walkthrough the Contractor shall ensure that all doors are properly wired for either *fail safe* or *fail secure* mode of operation. All egress path doors, unless otherwise designated by the FSM, scheduled with electronic hardware shall unlock from inside the facility upon actuation of a life safety device or fire alarm.

## 12. Warranty

12.1. A warranty period of one year will commence on official date of use after testing and acceptance by ICE Field Security Manager or designated alternate. ICE shall incur no equipment or labor costs during this warranty period.

12.2. The Contractor will identify a technical support or service contact for consultation during normal business hours, which is reachable by telephone or email.

12.3. Any critical security component that becomes inoperable must be replaced or repaired within 72 hours. Critical components are those required to provide security (PACS, IDS, VSS) for a perimeter

access point or high security/critical area.

12.4. For any non-critical component that becomes inoperable, the Contractor shall schedule a service call as soon as practical but not to exceed 14 days.

12.5. The Contractor must notify the customer of all projected downtime and estimated time for repair and provide a written report of all services rendered at time of repair.

12.6. Replacement security devices must be approved by FSM prior to installation.

12.7. ICE shall receive the full benefit of all manufacturers' warranties on all components beyond the initial warranty period.

12.8. The Contractor shall propose an extended warranty plan that includes ESS equipment replacement costs and hourly labor costs for service requirements. The proposed extended warranty should include the regularly scheduled and routine upkeep of equipment. The repair or replacement of any critical security component, as defined above, must occur within the same timeframe established in this document. For any non-critical security component that becomes inoperable, the Contractor shall schedule a service call as soon as practical.

12.9. The Contractor shall propose a preventative maintenance and repair plan that includes firmware/software updates, equipment replacement costs and hourly labor costs for service requirements. The proposed maintenance plan should include the regularly scheduled and routine upkeep of equipment and software as prescribed by the manufacturer. The repair or replacement of any critical security component, as defined above, must occur within the same timeframe established in this document. For any non-critical security component that becomes inoperable or requires servicing, the Contractor shall schedule a service call as soon as practical.

## 13. Review and Approvals

**Completed by**: Field Security Manager: Brian Alexander

Signature: BRIAN K ALEXANDER Digitally signed by BRIAN K ALEXANDER Date: 2026.06.18 07:31:29 -05'00' Date: _____

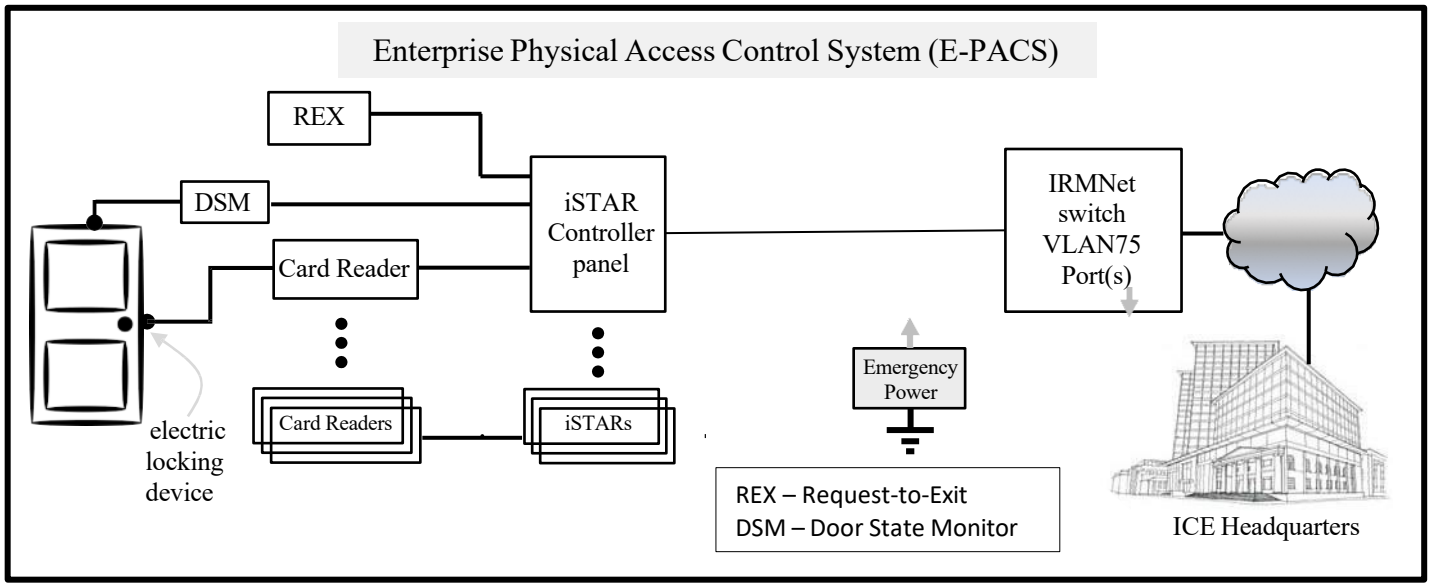
**Approved by:** Regional Security Manager: Steven Tod Ingwersen

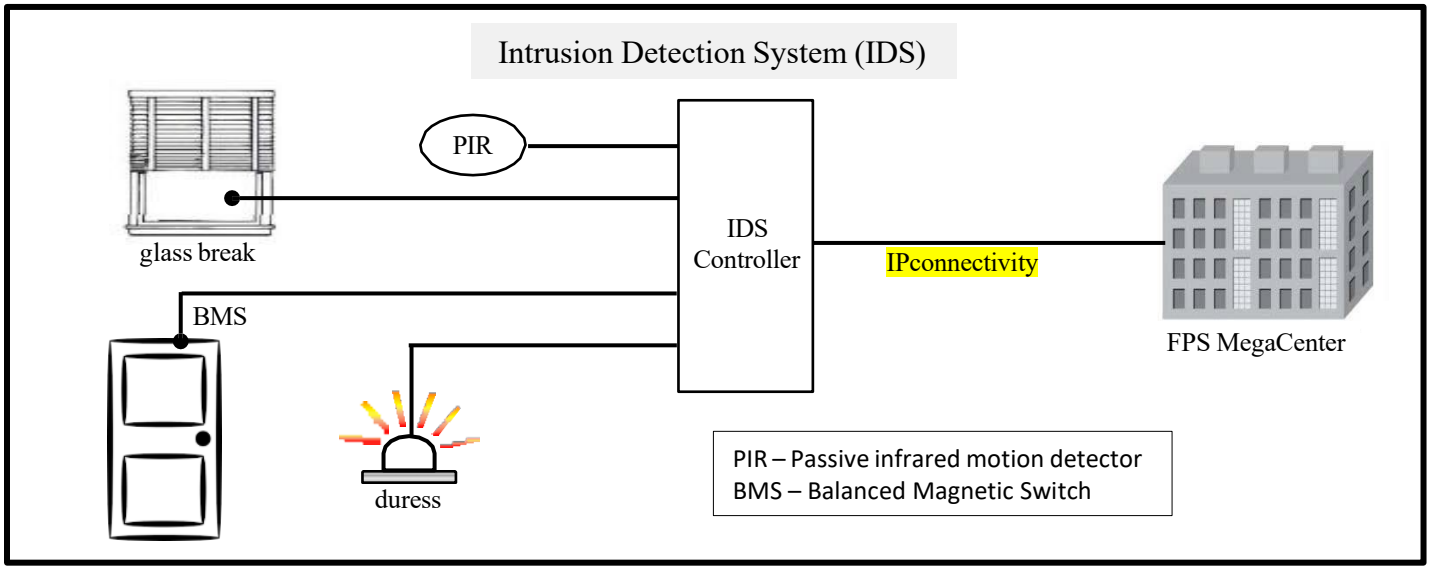
Signature: STEVEN T INGWERSEN Digitally signed by STEVEN T INGWERSEN Date: 2026.06.18 08:40:13 -04'00' Date: _____

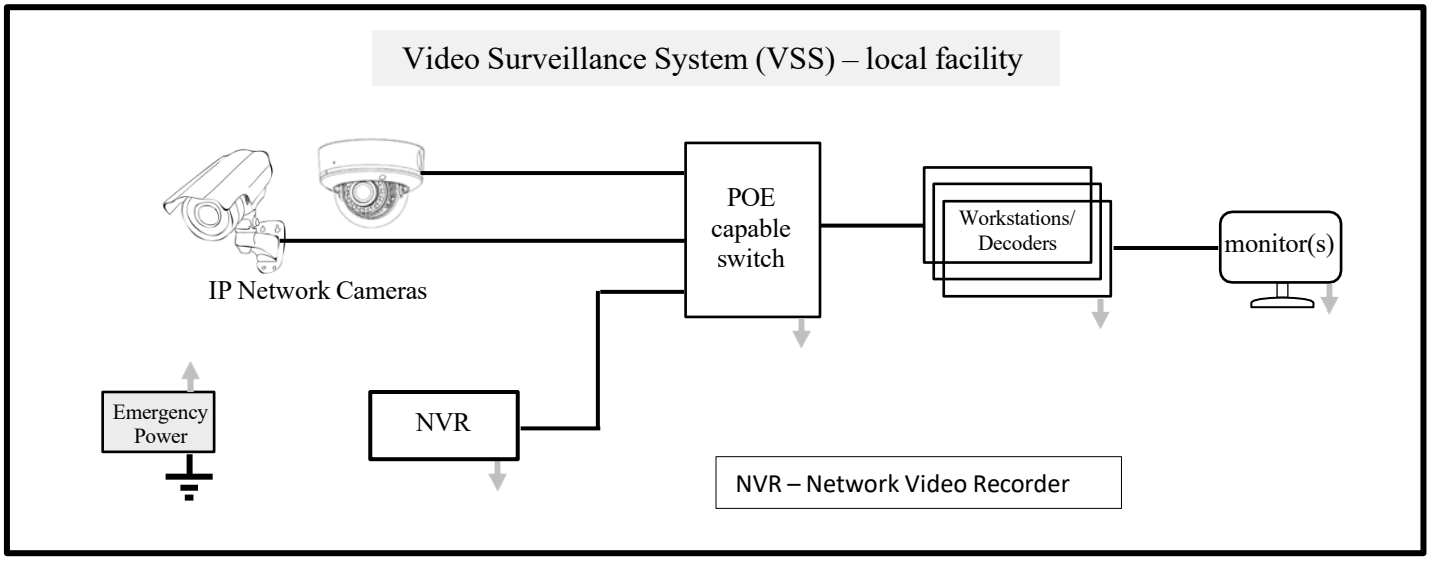
**Transmitted to** (OAFM PM)

Signature: _____ Date: _____

## SECTION II - ELECTRONIC SECURITY TYPICAL BLOCK DIAGRAMS



## SECTION III - ELECTRONIC SECURITY SYSTEMS (ESS) COMPONENT TASKS

### A. Enterprise Physical Access Control System (E-PACS)

A.1. This ICE location will be established as a client to the ICE E-PACS; no other PACS systems may be substituted for this project. ICE has procured Software House C•CURE 9000 Enterprise Physical Access Control System (E-PACS) to implement HSPD-12 within the Agency. The E-PACS hardware, system architecture and parameters described in this E-PACS task have been approved by the FIPS 201 Evaluation Program and meet the directives, regulations and standards referenced within this document. No deviation from the products specified and/or described, or from the installation methods identified is allowed.

A.2. Hardware Compatibility. The Contractor is responsible for ensuring the hardware provided is compatible with the ICE Enterprise Software House C•CURE 9000 E-PACS (Approved Products List #10115).

A.3. Connect the iSTAR panel to the designated IRMNET switch/port. The IRMNET switch is Government Furnished Equipment (GFE), and the Contractor is responsible for connecting each iSTAR panel to the IRMNET device for communications over the enterprise network. Contractor must consult with OCIO staff and E-PACS team to ensure panel connectivity with IRMNET.

A.4. PACS Panels.

A.4.1. The only acceptable E-PACS panels for this project are the following Tyco Software House products:

- For E-PACS Panels that require up to 16 readers
  - iSTAR Ultra **G2** (not SE model)
  - Life Safety FPO250/250-2D8P2M8PNL4E8S/P16-B Power Supply Enclosure (Supplies power to panel and Innometriks Readers)
  - Two (2) 12V 18Amp Hour Batteries
- For E-PACS Panels that require only 8 readers
  - iSTAR Ultra **G2** (not SE model)
  - Life Safety FPO150/150-D8PM8PNL4E6S/P8-A Power Supply Enclosure (Supplies power to panel and Innometriks Readers)
  - Two (2) 12V 18Amp Hour Batteries
- For panels requiring up to 4 readers and no more than 16 inputs and 4 outputs
  - iSTAR Edge2
  - Life Safety FPO75/150-D8PM8PNL4E4S-EB01 Power Supply Enclosure
  - One (1) Life Safety FPO250-2DPE2 Power Supply (Supplies power to panel and Innometriks Readers)
  - Two (2) 12V 18 Amp Hour Batteries

A.4.2. Ensure power supply is set to the appropriate voltage. The Innometriks readers will be configured to use 24V.

A.4.3. Power source must deliver at least 4 Amps of in-rush current for initial power up.

A.4.4. If adding Innometriks readers to an existing E-PACS panel:

- 16 readers add Two (2) Life Safety FPO250-2D8PE2 Power Supplies w/two (2) 12V 18

Amp Hour batteries in each enclosure for powering the new Innometriks readers.

- 8 readers add One (1) Life Safety FPO250-2DPE2 Power Supply w/two (2) 12V 18 Amp Hour batteries for powering the new Innometriks readers.

A.4.5. Access Control doors require a UL Listed and Rated Type CMP Plenum Composite cable to support OSDP reader communications, power, and door control.

The cable shall be or equivalent to:

- SMARTWIRE OSDP COMPOSITE CABLE E102194 CL2P (UL) 6C 18+8C 22AWG75C CMP C(UL)RS-485 ROHS.

A.4.6. Ground all reader cable drains or shields at the panel. This is important for reliable connectivity and to prevent comm fails between the Ultra controller and card readers

A.5. E-PACS Programming. The Contractor will provide a completed **E-PACS Paperwork** (E-PACS Port Charts Form, Input/Output Board Form and as-built drawings showing the location of each card reader) in order for the ICE E-PACS Team to complete programming and for the local ICE Program Office to complete related actions. Local ICE program office personnel are responsible for completing the Personnel Worksheets. Advice on establishing the clearance codes and Master Granting Authority List (MGAL) will be provided by the FSM. The current version of the Port Charts Form will be provided to the Contractor by the ICE Field Security Manager. Prior to final acceptance the Contractor shall ensure acopy of the ICE-approved Port Charts is placed in each PACS panel enclosure.

A.6. Card Reader.

A.6.1. The only acceptable card reader type for this project is the Innometriks Cheetah SE Reader. This product has been tested and approved as a component of a full FICAM solution. This reader component comprises one aspect of the E-PACS end-to-end solution.

**Note:** As all PKI validation will be managed centrally through DHS-ICE Headquarters PCN, procuring and installing the Innometriks Validation System and High Assurance Software Suite is **NOT** required for this project.

**Innometrik's Cheetah SE Reader:**

A.6.1.1. Name of Product: Innometriks Cheetah SE
A.6.1.2. Part Number: INN-SECHTA-CTO
A.6.1.2. Part Number: INN-RDR-LIC (1-Per Reader)
A.6.1.3. Firmware must be current manufactures released version
A.6.1.4. Approved Products List (APL) #10130

**CCURE System Serial Number: 9-17612**

**Satellite Application Server Serial Number (SAS):**
**EAST SAS Serial # 9-10527**

A.6.2. The Contractor shall ensure card readers are wired to meet factory standards and to ensure proper grounding

A.6.3. The Contractor shall ensure that the card reader is configured using the Open Supervised Device Protocol (OSDP) Secure Channel RS-485 connectivity, and the reader is set in the FICAM mode ensuring high assurance validation of single (PKI-CAK) and dual (PKI-AUTH) at the E-PACS through the challenge-response exchange protocol of the PIV certificates.

A.6.4. The Contractor shall ensure that the card readers are installed in compliance with theAmerican with Disabilities Act (ADA) and Uniform Federal Accessibility Standards (UFAS) and provide the following audio/visual indication:

A.6.4.1. An audio beeper providing various tone sequences to signify access granted, access denied

A.6.4.2. Two LED light bars at the left and right sides of the reader indicate status:

- Red – access denied, or reader not ready
- Green – access granted
- Gold – The gold LED light bar at the bottom of the contact reader indicates reader readiness for user to insert a chip card.

A.6.4.3. The Contractor shall interface the PACS into the ADA/UFAS automatic dooropeners.

A.7. Card Readers. Card readers shall be installed on the same side as the door handle, unless specified otherwise by the FSM.

A.8. Contractor must read the attached Innometriks Cheetah SE Reader Release Notes – Firmware Version 2.2.1 or later version. This document provides important information on installing the Innometriks Cheetah SE Reader.

A.9. Card reader-controlled doors shall be connected to a Door State Monitor (DSM) and Request-to-Exit (REX) device for operation of the door.

A.9.1 The Contractor shall configure doors with a REX device so an authorized egress from the secure area does not cause an alarm. No REX device is necessary if the door is controlled by a card reader on both sides.

A.9.1.1 REX devices can be push-button, motion sensors or incorporated in the mortise electrified lockset and shall shunt the alarm, not release the locking mechanism, unless specified otherwise by applicable NFPA 101 Life Safety Codes or the AHJ.

A.9.1.2 The Contractor shall ensure that the REX is a listed device for the specific operation to provide delay time to the DSM to prevent false alarms and is installed and configured to prevent activation by normal movement inside the secure area.

A.9.1.3 The Contractor shall ensure that the REX remains active for a maximum durationof five (5) seconds and that the timer is non-resettable.

A.9.1.4 Crash bar/delayed egress exit devices installed on doors must be approved by the FSM and shall have a local annunciator.

A.10. The Contractor shall ensure the DSM connects as an input or output directly to the PACS panels

for communication to ICE's Enterprise C•CURE 9000 server. **PACS shall not interface with double-pole, double-throw (DPDT) switches that interface to the IDS.**

A.10.1. For all card reader equipped doors the Contractor shall install a DSM that monitors the position of the door so that a forced-door or held-open door causes an alarm.

A.10.2. The DSM shall be concealed, a self-lock mounting, have rugged construction, ¾" in diameter, ABS plastic enclosure, be a hermetically sealed reed switch, be of high security, and is similar in color to the door frame.

A.11. Locks. Electric strikes, electrified mortise locksets and magnetic locks are acceptable locking mechanisms for this project. All locking mechanisms are to return to a locked state immediately after use or within 3 seconds of non-use, unless specified differently by the ICE Field Security Manger. Electric locking mechanisms must meet UL 1034, Standard for Burglary-Resistant Electric Locking Mechanisms and be listed as burglary-resistant. Additionally, electric strikes must meet American NationalStandard for Electric Strikes and Frame Mounted Actuators - ANSI/BHMA A156.31, Grade 1 (Cycle 500,000, Static Strength—Voltage @ 100% and 85% of rated = 1500 pounds., Dynamic Strength— Voltage @ 100% and 85% of rated = 70 ft. lb. (95J).

A.11.1. Additional electric strike specifications:

- Construction: Stainless steel, tamper resistant, internal solenoid
- Operation: Field reversible, plug-in connectors
- Solenoid: Internally mounted to facilitate electric strike installation in hollow metal, concrete filled, and aluminum and wood jambs, operated by direct current to provide silent operation
- Electric Strike: Capable of operation with less than 30 pounds of force against keeper

A.11.2. Additional magnetic lock specifications:

- 600 lbs. holding force to be placed controlled interior rooms and secure areas within buildings
- 1200 lbs. holding force to be placed on detention and perimeter doors
- Magnetic locks shall have magnetic bond sensor
- Power override solution to be proposed for doors not identified as *fail safe*

A.12. Other Door Hardware. For card reader-controlled doors the Contractor shall provide and install:

A.12.1. A door latch guard which will prevent the lock bolt from being retracted from the unsecure side of the door or install a door strike that engages the guard bolt or auxiliary dead latch located on door hardware.

A.12.2. A functioning heavy-duty door closer.

A.12.3. All deadbolts with minimum 1-inch throw on perimeter or high security doors shall be independent action, not integrated with the card readers. The Contractor shall coordinate with the FSM on which high security doors need deadbolts. As specified in the ICE FDG, the deadbolts required for all ICE perimeter doors, O P R / HSI Seized Evidence Storage Rooms and HSI Computer Forensics Lab shall be Underwriters Laboratories (UL) listed under UL437 and certified under American National Standards Institute (ANSI)/Builder's Hardware Manufacturer's Association (BHMA) certification A156.30, Levels M1AAAM and ANSI/BHMA A156.5, Grade 1. In the event the deadbolt is not integrated into the Heavy-Duty Grade 1 Mortised Hardware storeroom function lock, both the lock and cylinder (or core) must meet or exceed the listing and certification requirements specified above.

A.12.4. Transfer hinge for electrified lockset or REX devices, as necessary.

A.12.5. The Contractor will coordinate with the Project Team to ensure there are no conflicts between door hardware and door or door frames.

A.13. Connectivity Handshake. The Contractor shall work with the ICE PACS Team for any network handshakes that will be required to do with the installed E-PACS panels and IRMNET network switch devices. This work is not limited to re-programming the devices to set specifications using the iSTAR Configuration Utility (ICU). The Contractor will remain involved in this task until the connection is successfully completed. After acceptance by ICE the Contractor will provide a CD (or other acceptable electronic medium) with system configurations as a back-up in case of C•CURE server failure.

A.14. The Contractor shall design and install a complete hardwired IP based audio and video intercom system with door station(s) and room master/sub-station(s) based upon the site layout and operational requirements. It shall not have any wireless capability to include interconnection for communications through a wireless router for mobile or remote application management. The system shall be installed in accordance with American National Standards Institute (ANSI) 568 Commercial Building Telecommunication Cabling Standard. A non-IP digital system installation based upon site layout and operational requirements may be authorized based on FSM's written approval.

A.14.1. The video intercom system will provide door release capability integrated into the Physical Access Control System (PACS) by shunting the system to provide a valid entrance notification when releasing the door. For door release, the system shall be configured as an input into the PACS door control panel to release the lock and shunt the door contact when the door release button has been activated. The intercom system shall not be further integrated into the PACS.

A.14.2. Door station. Door stations installed in outdoor settings shall be vandal resistant and rated for the prevailing weather conditions of the area.

A.14.3. Video capabilities shall contain:

- Equipped with an advanced light adjustment feature to compensate for varying light levels. If a picture is too dark, increase of the brightness level at the door station shall be controlled at the master/sub-station.

- The door station will be mounted within the manufacturer's recommendations (typically 5 feet from the ground).

A.14.4. A list of locations/rooms or doors that require video intercoms is contained in the **SECURITY SYSTEMS DETAILS** section of this document.

A.15. Device Labeling. The Contractor shall label all PACS panels, power supplies, security enclosures, workstations, and any other enclosure installed in support of the project using a plastic label permanently mounted to the door that meets the requirements listed below:

A.15.1. Engraved-- Plastic Labels: Engraving stock, melamine plastic laminate punched or drilled for mechanical fasteners, 1/16-inch minimum thickness for signs up to 20 sq. in. and 1/8-inch minimum thickness for larger sizes. The Contractor shall provide an engraved legend in black letters on white background. Additionally, the Contractor shall label all card readers with the designation on the port charts.

A.15.2. The Contractor shall identify, with ½" lettering, all cabinets including security equipment panels, power supplies, system interface cabinets, and similar security equipment.

A.16. The location of E - PACS fielded devices is identified in the **SECURITY SYSTEMS DETAILS** section of this document.
**ALL INPUTS MUST HAVE END OF LINE RESISTORS**

A.17. Workstation Configuration. On a limited, case by case basis, the ICE program office will provide the Contractor with a Software House C•CURE 9000 workstation. Approval to deploy the workstation is granted by the E-PACS Program Manager.

A.17.1. In such a scenario, the Contractor shall procure, install and test the workstation that meets the requirements specified by Software House.

A.17.2. The Contractor is responsible for all costs to ship the workstation to ICE HQ for programming and back to the project site. The Contractor shall ensure a shipping label with a complete return address to the project site is provided. The shipping address is identified above.

A.17.3. The E-PACS Program Office shall assign administrator and operator logons for each workstation at the direction of the FSM.

A.17.4. The Contractor shall ensure that PACS software is accessible from the PACS workstation with administrator / operator log-on for viewing located in the ICE facility. The Contractor shall supply, install and terminate to TIA 586B standard plenum-rated Category 6 cable between workstations and IRMNET network switch device. ICE personnel will provide the Contractor with the network switch location and ports.

A.17.5. The E-PACS Program Office shall develop log-on access levels for appropriate viewing/administration by users.

**B. Intrusion Detection Systems (IDS)**

B.1. The Contractor shall also design an IDS solution for ICE perimeter entry points (suite or building), high security areas, and general office spaces. This solution may include balanced magnetic switches (BMS) meeting UL 634, motion sensors, glass break sensors and duress devices.

B.2. The Intrusion Detection System will be programmed, administered and monitored by the Federal Protective Service (FPS) MegaCenter. As such, the requirements set forth in the **MEGACENTER ALARM REQUIREMENTS** referenced at the end of this document, to include Installer (Contractor) deliverables, must be met in addition to this task description.

B.2.2. The MegaCenter can monitor UL commercially grade listed panels from the following manufacturers only (proprietary panels cannot be monitored or supported):

B.2.3. For Internet monitored accounts:

- **Bosch (Radionics)**
- The OCIO MUST provide a static IP address for the control panel. The OCIO also needs to open port 7700 (Bosch) bi-directionally on their firewall and forward the port on their firewall to the alarm panel.

B.3. The Contractor shall coordinate with the project team, ICE OAFM Project Manager, FSM and local program office representative to determine connection to the MegaCenter will be an **IP line.** Further coordination may be necessary throughout the project to ensure the IP line is available in a timely manner. All coordination shall occur through prescribed GSA channels.

B.4. All IDS devices and panels containing ESS equipment must have functional internal tamper switches which create a point specific alarm, unless directed otherwise by the FSM.

B.5. All devices and points/zones are to be separately identified in the IDS panel to support the responding entity with an exact locality description for a quick and accurate response.

B.6. Motion detectors must be dual technology (microwave and passive infrared or adaptive RADAR and passive infrared) unless otherwise specified.

B.7. ICE suite or facility perimeter doors will be designed in a multi-layered approach with balanced magnetic switches and a motion sensor(s) inside.

B.7.1. Double doors or split doors shall be zoned on each leaf, not as one zone.

B.7.2. Overhead doors should have a sensor on each side to prevent the lift on one side without an alarm.

B.7.3. Door contacts will be installed on the secure side of the door near the opening and shall not allow the door to open far enough to provide the ability to tamper with the contact inside without going into alarm.

B.8. All IDS keypads will be located on the interior of the protected space or room, to include individual partitions/areas, unless expressly instructed otherwise by the Field Security Manager in

writing.

B.9. Duress devices shall be concealed from the public and shall annunciate for an immediate response. Reset of duress devices shall require a deliberate manual function of the alarm button i.e. flip/toggle switch, pullout mushroom or key reset.

B.9.1. Duress annunciation may include locally installed strobe lights and sirens, and a signal sent to the MegaCenter.

B.9.2. If required, strobe lights should be visual/audible tri-colored units with minimum 70-decibel audible alarm.

B.9.3. The Contractor shall coordinate with FSM on annunciation requirements, to include strobe light colors and device locations.

B.10. The Contractor must complete all "Installer Sections" of the **MEGACENTER ALARM REQUIREMENTS FORM** referenced at the end of this document and provide the final IDS floor plan to the MegaCenter after review by the FSM.

B.10.1. Each point/zone of ESS must be individually identified at the keypad and at the MegaCenter.

B.10.2. The Contractor shall use a naming convention for each alarm point/zone that contains the architectural room number and room description, unless specified otherwise by the FSM.

B.11. All points/zones must be tested with the FPS MegaCenter to ensure they are fully operational and provide accurate reporting prior to acceptance.

B.11.1. The Contractor will ensure that all points/zones, including duress activation locations and annunciation methods, have been fully tested and communicate with the FPS MegaCenter prior to the final acceptance test and job completion.

B.11.2. The ICE FSM may require a retest or additional testing during the acceptance process.

B.12. A temperature monitoring system shall also be established within the IT/LAN room (or Security Equipment Room) with trouble notification to the FPS MegaCenter. The acceptable temperature shall be set between 65 to 75-degrees Fahrenheit.

B.13. A list of locations/rooms or doors that require IDS components is contained in the **SECURITY SYSTEMS DETAILS** section of this document.

**C. Video Surveillance System (VSS)**

C.1. The Contractor shall provide a complete VSS solution designed such that it meets the physical security needs of the facility. The solution shall include cameras, network video recorders (NVR) and associated peripheral hardware for management and network transport purposes. The VSS solution must be built on an Internet Protocol (IP) based architecture on an isolated LAN platform; this network will not connect to the Internet nor any other network. The Contractor shall provide all network related hardware for this platform. Procurement of VSS hardware must follow GSA guidelines and the purchasing or use of hardware manufactured or assembled in China is prohibited. All network switches

will be rated to support IP camera Power-Over-Ethernet (POE) requirements as per manufacturer specifications. The VSS solution will contain local management capabilities utilizing a standalone configuration. System management software shall be compatible with all functional requirements of the VSS system. The contractor shall provide a Network Time Protocol (NTP) Server, like Time Machines TM-1000, as an element of the VSS solution. This is to ensure system timing accuracy without Internet connection. All network devices shall be set to periodically communicate with the NTP server to adjust for timing inaccuracies. System management software shall only require a one-time license procurement and be compatible with all functional requirements of the VSS system. The contractor shall provide a Network Time Protocol (NTP) Server, like Time Machines TM-1000, as an element of the VSS solution. This is to ensure system timing accuracy without Internet connection. All network devices shall be set to periodically communicate with the NTP server to adjust for timing inaccuracies. System management software shall only require a one-time license procurement and be compatible with all functional requirements of the VSS system. Exceptions must be approved by the FSM.

C.2. The Contractor will design a VSS solution that contains, at a minimum, the following:

C.2.1. An NVR model/type that shall produce an open file format, such as *.avi* or *.mov*, and a proprietary water-marked format for download or export

C.2.2. A system that includes the ability to visually present a variety of groupings of real-time videoas selected by the administrator or local operator

C.2.3. Basic camera management functions

C.2.4. An NVR model/type where an administrator can pre-program pan-tilt-zoom (PTZ) cameras to view a pattern or tour during predetermined timeframes but, manually controlled when needed

C.2.5. A system that can detect a duress activated alarm and display the closest camera to the location of the alarm in full screen on a preselected monitor until reset to normal video display operation, as specified by FSM

C.2.6. All required software and hardware licenses shall only require a one-time procurement. Recurring license requirements are not acceptable.

C.2.7. The Contractor will ensure all required firmware and software updates are applied to all VSS equipment prior to deployment.

C.3. Network Video Recorder (NVR) equipment is required for the storage and review of historical security camera videos. NVR systems shall be capable of changing the recording frame rate and frames-per-second (fps) based upon a set schedule and analytical inputs such as motion. The NVR system shall have the capability to assign multiple levels of logins with password protection (Administrator, Supervisor, User). The typical minimum recording solutions for each camera location are listed below.

C.3.1. Exterior Perimeter: 24/7 minimum 15 fps continuous

C.3.2. Public entrance/exit (interior side), transaction windows, lobbies:

C.3.2.1. Business hours (One hour before facility opens to one hour after facility closes): minimum 15 fps continuous

C.3.2.2. Non-business hours (One hour after closing to one hour before opening): Motion and alarm activated, a minimum of 15 fps from 10 seconds before to 30 seconds after. (motion period shall include 2 hours of 15 fps recording for storage calculations)

C.3.3. Detainee areas (Sally Port, holding, processing, etc.), evidence rooms, armory:

C.3.3.1. Business hours (One hour before facility opens to one hour after facility closes): minimum 15 fps continuous

C.3.3.2. Non-business hours (One hour after closing to one hour before opening) minimum 7.5 fps continuous. With motion and alarm activation recording increases to a minimum of 15 fps to include 10 seconds before and 30 seconds after. (non-business motion period shall include 2 hours of 15 fps recording for storage calculations)

C.3.4. Non-public entrance/exit, stairwells, hallways, non-detention elevators: 24/7 Motion and alarm activated, a minimum of 15 fps from 10 seconds before to 30 seconds after. (motion period shall include 6 hours of 15 fps recording for storage calculations)

C.4. NVR hard disk drives used for video storage, such as the Western Digital ITB-10TB (a.k.a. Purple Surveillance Storage), must be built to withstand continuous read/write activity. The Contractor will determine the storage capacity of the NVR(s) based on the following criteria:

C.4.1. Quantity of cameras

C.4.2. Period of motion activated recording per camera

C.4.3. Frames-per-Second (fps) for each camera

C.4.4. A minimum of **30 days of storage for each camera**

C.4.5. H.264 or better compression

C.4.6. Camera resolution

C.4.7. Good video quality with a minimum resolution of 40 pixels-per-foot (PPF) at the target distance

C.5. The video system will be calculated to accommodate an additional 20% for storage capacity and future expansion of additional camera channels. Documentation illustrating this calculation shall be submitted to the FSM for review, including a list of cameras and their respective recording rate and duration. This requirement is capped at 10 additional video channels and storage space. The requirement may be lowered by the FSM with written authorization.

C.6. Cameras must provide 100% coverage of perimeter, detention and high-security areas. In detention holding cells, cameras will be mounted such that video is not seen or recorded in the toilet/privacy area. All cameras will have 2-megapixel or better resolution. FSM may designate a select number of cameras covering high security or critical areas as 5-megapixel or better to identify a person (facial recognition) or object (license plate recognition) with enough detail for courtroom quality. All exterior cameras shall have an infrared (IR) cut-filter and/or IR nighttime illuminator either built in or added as an accessory. All exterior cameras shall be environmentally protected based on the prevailing weather

conditions for the geographical area and as prescribed by the camera manufacturer. Fixed, pan-tilt-zoom, 180-degree and 360-degree panoramic or multi-head cameras are acceptable.

C.6.1. Pan-tilt-zoom cameras shall not be programed on an area tour to provide 100% exterior coverage. These cameras shall only be utilized for additional monitoring capability when a guard force is present.

C.6.2. 360-degree panoramic or multi-head cameras should not be utilized as the primary camera to view an area when active monitoring is required.

C.7. The Contractor shall take steps to prevent tampering with the VSS system to include:

C.7.1. Positioning/mounting cameras out of reach

C.7.2. Installing all cameras in a fixed, tamper and vandal-resistant and/or detention grade enclosure

C.8. Monitors shall have the appropriate built-in video and management ports based on the VSS system design requirements and shall not have any wireless connection (Wi-Fi, Bluetooth etc.) capability enabled. Wall mounted monitors shall be installed using a premium type full-motion wall bracket to provide tilt, swivel and arm extension capabilities, unless specified differently by the FSM. For multiple monitor installations videos shall be organized for security personnel to easily follow movement through the facility from one camera to the next in a smooth flowing fashion without having to bounce back and forth among monitors. VSS workstations and decoders shall not exceed the manufacture's recommended number of displayed cameras or connected monitors. Workstations serving wall monitors will be micro or nano form factor with 16 GB RAM or better and wall mounted behind monitors. All monitors shall be capable of viewing the specified number of camera views listed below at 30 fps (real time):

C.8.1. 42-50" monitors are typical for wall and stand mount, general area observation of multiple cameras. Shall be capable of 16 camera views per monitor

C.8.2. 27-32" monitors may be utilized for guard stations and other areas where size restrictions will not allow 42-50" monitors. Shall be capable of 8 camera views per monitor

C.8.3. 22-26" monitors shall be utilized for VSS workstations, alarm call-up, or specific spot area monitors. Shall be capable of 1-4 camera views per monitor

C.9. All AC voltage powered devices shall be connected to a centrally located uninterruptable power supply (UPS) in the designated IT/LAN equipment and frame/closet rooms. Each equipment room will contain a, building-grounded, grounding buss bar which will be utilized for equipment rack and panel grounding connectivity. As part of the VSS package, the Contractor shall provide a rack mount keyboard-video-mouse (KVM) console with appropriate cabling for connection to each NVR and matrix (if used), or properly configured network client with remote access (on the dedicated VSS network), for video and software management and maintenance.

C.10. The Contractor shall propose, procure and install VSS surveillance advisory signage at entrances to the site, facility, parking garages or parking lots, etc., where VSS coverage exists.

C.10.1. Signs shall be large enough to be noticed, placed in easily seen locations, and have both words and pictures indicating VSS is being conducted at the location.

C.10.2. Signs posted outside shall be listed by the manufacturer to withstand the local environmental conditions and permanently affixed to a fence, pole or structure.

C.10.3. The following is an example of an acceptable sign:

Source: https://www.compliancesigns.com/ONE-9544.shtml

C.11. The Contractor shall use a naming convention to label each camera in the VSS that contains the architectural room number and room description, unless specified otherwise by the FSM.

C.12. A list of locations or rooms that require VSS components is contained in the **SECURITY SYSTEMS DETAILS** section of this document.

## SECTION IV - SECURITY SYSTEMS DETAILS

### A. Interior Physical Access Control System (PACS)

*Requires Innometriks Cheetah SE High Assurance Smart Card Reader (INN-SECHTA-CTO) **(OSDP "not" Weigand)**

**Approved Card Reader Options:**

***Option 1: Identiv TouchSecure Reader, Mullion, High Assurance Ready, OSDP Ready - HF/LF - Terminal (APL# 10175) Device: IDV-9010AB-PT**

***Option 2: Identiv TouchSecure SC Keypad Contact Reader -High Assurance Ready, OSDP Ready- HF/LF - Terminal (APL# 10179) Device: IDV-9216AB-PT**

**Physical Access Control card readers**

*Lobby 100 Double Doors
*Double Doors next to Work Rm/Admin 104
*Lobby 100 to Corridor 108 Double Doors
*East Double Doors leading to Corridor 122
*Tel/Com 123 (House IT and security systems)
*Room 105 (2)
*Room 114 (2)
*Room 118
*Room 119
*All exterior except Mechanical 121 and Mechanical/Electrical 116 require card readers.

**These rooms will require a deadbolt lock:**

Mechanical/Electrical room 116
Mechanical Room 121

**AiPhone Base Stations**

Outside Lobby 100 Double Doors

**AiPhone Master Stations**

Inside Lobby 100
Room 117
Corridor 108 next to room 106

### B. Interior Video Surveillance System (VSS) Devices:

Lobby 100 ceiling mounted 360 degree panoramic
Outside Room 105 Gear Locker Room ceiling mounted 360 degree panoramic
Outside Room 114 Gear Locker Room ceiling mounted 360 degree panoramic
Corridor 122 ceiling mounted 360 degree panoramic

**Video Monitors (40 inch)**
Room 102
Room 117

**C. Exterior Physical Access Control System (PACS) Devices**

**Aiphone Base Call Station:**

Main Front Entrance door

**D. Exterior Video Surveillance System (VSS) Devices**

**Fixed camera locations**

**Pan-Tilt-Zoom or 360-degree multi-head/panoramic camera locations**

Front of Building (2)
NW CORNER of building
NE CORNER of building
SW CORNER of building
SE CORNER of building

**Fixed camera locations**

Above Exterior of Lobby 100 Entrance door
SOUTH WEST CORNER **2 fixed day/night cameras**
NORTH WEST CORNER 2 **fixed day/night camera**
NORTH EAST CORNER 2 **fixed day/night camera**
SOUTH EAST CORNER **2 fixed day/night camera**

## ATTACHMENTS

**PACS Paperwork**

- **(Electronic Copy to be provided by ICE Field Security Manager)**

**ESS Component Checklists**

- **(Electronic Copy to be provided by ICE Field Security Manager)**

**MegaCenter Alarm Requirements (MAR) Form**

- **(Electronic copy to be provided by ICE Field Security Manager)**

**Note:** Installer is to request a copy of the FPS MegaCenter Alarm Requirement (MAR) Form from ICESecurity Manger upon award of contract. The MAR is needed for planning and design of IDS.

**Installer to Complete:** Installer Information, Alarm System Information, Floor Plan Instructions, Area / Partition Information, Keypad Information, Relay Information, Zone / Device Information shown above.

**Local ICE Program Office to Complete:** Subscriber Information, FPS Contacts, Authorized Account Contacts, System and Activation, Emergency Contact Information and User Information sections.

**MegaCenter Alarm Requirements (MAR) Form**

- An electronic copy of this document to be provided by ICE Field Security Manager

Department of Homeland Security
National Protections and Programs Directorate
Federal Protective Service
**MegaCenter Alarm Requirements (MAR)**

**INSTALLER INFORMATION**

INSTRUCTIONS: Provide information pertaining to the company providing installation services of the alarm system.

| | | |
|---|---|---|
| COMPANY NAME: | STREET ADDRESS: | CITY: |
| STATE: / ZIP CODE: | OFFICE PHONE: | OFFICE FAX: |
| SERVICE MANAGER: | SERVICE MANAGER PHONE: | |
| TECHNICIAN: | TECHNICIAN PHONE: | |

**ALARM SYSTEM INFORMA**

| | | | | |
|---|---|---|---|---|
| ALARM SYSTEM STATUS: (Check One) | | NEW | | UPGRADE |
| ALARM SYSTEM TYPE: (Check All That Apply) | | BURGLARY | | DURESS |
| ALARM PANEL TYPE: (Write Model Number) | | ADEMCO | | BOSCH |

PANEL PHONE NUMBER: Does system need to dial 9 for outside line? LOCATION OF

NOTE: Phone line connections must be dedicated or RJ31X connections with proper line seizure and programming to enable the MegaCenters to connect remotely at any time.

NETWORK INTERFACE TYPE: DNS SERVER ADDRESS:

EXTERNAL DEVICE IP ADDRESS (MUST BE STATIC): MAC ADDRESS:

DEFAULT GATEWAY SUBNET MASK

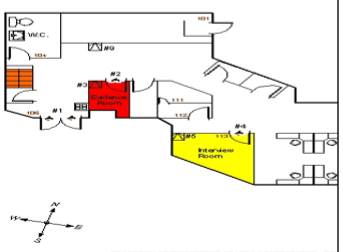
Internet Mon address for the port 7700 (Bos and forward th

NOTE: It is the sure all routers recommended to the panel as

**FLOOR PLAN INSTRUCTI**

INSTRUCTIONS: Provide a clean reproducible copy of building or office area floor These plans will be scanned into our alarm automation software to assist the resp alarm. If possible, we would prefer the above requested drawings or plans in autom BMP or .JPG formats are acceptable. SEE SAMPLE DRAWING.

Account - Number
Agency
Street, Suite
City, State Zip Code




PROPERTY OF THE UNITED STATES GOVERNMENT - FO
Do not remove this notice - Properly destroy documents whe
Last Revised: 5/22/17

**AREA / PARTITION INFORMATION**

INSTRUCTIONS: List information regarding other partitioned areas. Include Account No. (If known) for each area along with the location. Every partitioned area needs to have at least one keypad.

| AREA | ACCOUNT | KEYPAD(S) ASSIGNED | DESCRIPTION OF AREA (Include Location) |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

**KEYPAD INFORMATI**

INSTRUCTIONS: List the manufacturer, model and serial number for each keypad

| KEYPAD ADDRESS | AREA NO. | AUDIBLE ( Y or N ) | LOCATION |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**RELAY INFORMATIO**

| RELAY # | MODEL | TRIGGER | RESET METHOD |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

PROPERTY OF THE UNITED STATES GOVERNMENT - FO
Do not remove this notice - Properly destroy documents wh
Last Revised: 5/22/17

**ZONE/DEVICE INFORMATION**

Only one device can be used per zone

INSTRUCTIONS: List information regarding all alarmed devices (zones). List the manufacturer, model and serial number for each type of device installed. Identify the zone and/or area it is attached to. Provide a zone description that can be used when reporting an alarm condition to a responding authority. Please do not abbreviate. If it is a duress button, state whether it is audible or silent.

| Device Types | Point Source | Response Types |
|---|---|---|
| BUR – Door, roof hatch, overhead, and motions | HWD - Hardwired | 24 - 24 Hour |
| DUR – Duress and panic devices | POP – Octopopit | L – Local only |
| ENV –Temperature, and humidity devices | ZON - Zonex | D - Entry delay |
| GLS – Glass break devices | WIR – Wireless | F - Interior follower |
| TRB – Trouble devices | DIP – Dip switch polling | P - Perimeter |
| FIR – Fire devices | SER – Serial number polling | I - Instant |
| TPR – Tamper devices | OCT – Octo-Input | |
| SUP – Supervisory devices | INO - Inovonics | |

| ZONE | AREA | DEVICE TYPE | SILENT/ AUDIBLE | ZONE DESCRIPTION (Include Location) | RESPONSE TYPE | MODEL NUMBER | SERIAL NUMBER (If Wireless) | POINT SOURCE |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

PROPERTY OF THE UNITED STATES GOVERNMENT - FOR OFFICIAL USE ONLY
Do not remove this notice - Properly destroy documents when no longer needed.
Last Revised: 5/22/17

Page: 9 of 10

**Note:** Installer is to request a copy of the FPS MegaCenter Alarm Requirement (MAR) Form from ICE Security Manger upon award of contract. The MAR is needed for planning and design of IDS.

**Installer to Complete:** Installer Information, Alarm System Information, Floor Plan Instructions, Area / Partition Information, Keypad Information, Relay Information, Zone / Device Information shown above.

**Local ICE Program Office to Complete:** Subscriber Information, FPS Contacts, Authorized Account Contacts, System and Activation, Emergency Contact Information and User Information sections.