PERFORMANCE WORK STATEMENT (PWS)

FOR

SAN DIEGO INTRUSION DETECTION SYSTEM WITH MONITORING
11 August 2026

1.0 General:

1.1 Scope: The contractor shall provide all personnel, equipment, tools, materials, supervision, and quality control necessary, except as specified in Paragraph 3.0 as Government Furnished, to perform the installation of an intrusion detection system with monitoring Services**,** as defined in this PWS.

1.2 Background: The California National Guard is moving to a new commercial space where new intrusion detection system and installation is required.

1.3 Period of Performance (PoP): The Period of Performance shall be one base year of 12 months and four 12-month option years.

1.4 General Information:

1.4.1 Place and Performance of Services: The contractor shall provide equipment and installation of intrusion detection system between the hours of 0800-1700 on Monday through Friday, except on recognized US holidays. The contractor shall at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this PWS. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the work force are essential.

4821 Viewridge Avenue, San Diego, CA 92123.

The Contractor shall provide monitoring services 24 hours a day, 7 days a week, including all recognized US holidays or when the Government facility/installation is closed due to local or national emergencies, administrative closings, or similar Government-directed facility/installation closings. Performance shall be remote.

1.4.1.1 <u>Telework</u>: The Government does permit the contractor to telework in support of this requirement. Because all 24/7 monitoring services associated with this contract are performed at the contractor’s own facility and not at the Government site, telework is authorized for these functions. In furtherance of Continuity of Operations Planning (COOP), a telework program may be enacted to ensure that the Government's mission critical operations remain fully operational during times of national emergency or incidents of national significance. Telework shall be at no additional cost to the Government.

1.4.1.2 Reserved.

1.4.1.3 The contractor's employees shall become familiar with and obey the regulations of the installation; including fire, traffic, safety and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times and shall be subject to such checks as may be deemed necessary. The contractor shall ensure compliance with all regulations and orders of the installation, which may affect performance. The Government reserves the right to direct the removal of an employee from Government property or revoke access to Government systems for misconduct, security reasons, or any overt evidence of communicable disease. Removal of contractor employees for reasons stated above does not relieve the Contractor from responsibility for total performance of this contract.

1.4.2 Recognized Holidays: The following are recognized United States (US) holidays. The contractor shall not perform installation services on these days:

1.4.2.1 New Year's Day: January 1st
1.4.2.2 Martin Luther King, Jr.'s Birthday
1.4.2.3 President's Day
1.4.2.4 Memorial Day
1.4.2.5 Juneteenth National Independence Day: June 19th
1.4.2.6 Independence Day: July 4th
1.4.2.7 Labor Day
1.4.2.8 Columbus Day
1.4.2.9 Veteran's Day: November 11th
1.4.2.10 Thanksgiving Day
1.4.2.11 Christmas Day: December 25th

1.4.3 Quality Control (QC): The contractor shall develop and maintain an effective QC Plan (QCP) to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's QCP is the means by which it assures itself that its work complies with the requirements of the contract. As a minimum, the contractor shall develop QC procedures that address the areas identified in Technical Exhibit 1, Performance Requirements Summary (PRS). A final QCP shall be submitted to the Contracting Officer Representative (COR) NLT 10 days after contract award. After acceptance of the QCP, the contractor shall obtain the Contracting Officer's (KO's) acceptance in writing of any proposed changes to its QCP.

1.4.4 Quality Assurance (QA): The Government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government will do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and acceptable quality level(s) or defect rate(s).

1.4.5 Installation Access and Security Requirements. The contractor shall comply with all applicable installation/facility access and local security policies and procedures, which may be obtained from the COR. The contractor and all associated subcontractor

employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor shall ensure compliance with all personal identity verification requirements as directed by Department of Defense (DoD), Headquarters Department of Army (HQDA) and/or local policy (see PWS 6.0). Should the Force Protection Condition (FPCON) change, the Government may require changes in contractor security matters or processes.

1.4.5.1 Reserved

1.4.5.2 For contractors that do not require a CAC, but require access to a DoD facility or installation: Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05), and applicable installation, facility and area commander installation/facility access, and local security policies and procedures (provided by a Government representative).

1.4.5.3 Reserved

1.4.5.4 Reserved

1.4.5.5 Communications Security/Information Technology (COMSEC/IT) Security. All communications with DoD organizations are subject to COMSEC review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DoD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DoD organizations. Therefore, the contractor is advised that any time contractor personnel place or receive a call they are subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DoD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

1.4.5.6 Reserved

1.4.5.7 Reserved

1.4.5.8 Reserved

1.4.5.9 Reserved

1.4.5.10 Reserved

1.4.5.11 OPSEC Training: In accordance with AR 530-1, Operations Security, new contractor employees shall complete Level I OPSEC training within 30 calendar days of their reporting for duty and annually thereafter. The contractor shall submit certificates

of completion for each contractor employee to the COR within 15 calendar days after completion of training. Level 1 OPSEC training is available at https://securityawareness.usalearning.gov/opsec/index.htm.

1.4.5.12 Reserved

1.4.5.13 Reserved

1.4.5.14 Reserved

1.4.6 Physical Security. The contractor shall safeguard all Government property provided for contractor use. At the close of each work period, Government facilities, equipment and materials shall be secured.

1.4.6.1 Key Control. NOTE: All references to keys include key cards. The contractor shall establish and implement methods of ensuring that no keys/key cards issued by the Government are lost or misplaced or are used by unauthorized persons. No keys issued by the Government shall be duplicated**.** Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The contractor shall include procedures covering key control in the QCP.

1.4.6.1.1 The contractor shall immediately report any occurrences of lost or duplicated keys/key cards to the COR.

1.4.6.1.2 In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction by the KO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the Government replaces or re-keys the locks, the Government will deduct the total cost of lock replacement or re-keying from the monthly payment due the contractor. In the event a master key is lost or duplicated, the Government will replace all locks and keys for that system and will deduct the total cost from the monthly payment due the contractor.

1.4.6.1.3 The contactor shall prohibit the use of the Government issued keys/key cards by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contactor employees engaged in the performance of services in those areas, or personnel authorized entrance by the KO.

1.4.6.2 Lock Combinations: The contractor shall establish and implement methods of ensuring that no lock combinations are revealed to unauthorized persons. The contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the contractor's QCP.

1.4.7 Reserved

1.4.8 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference convened by the KO in accordance with FAR 42.5. The KO, COR and other Government personnel, as appropriate, may meet periodically with the contractor to review the contactor's performance. At these meetings, the KO will apprise the contractor of how the Government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. The contractor shall resolve outstanding issues raised by the Government. Contractor attendance at these meetings shall be at no additional cost to the Government.

1.4.9 Contract Manager (CM): The contactor shall designate a CM who shall ensure performance under this contract. The name of this person, and an alternate who shall act for the contractor when the CM is absent, shall be designated in writing to the KO. The CM or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The CM shall work through the COR to resolve issues, receive technical instructions, and ensure adequate performance of services. The CM shall ensure that contractor employees do not perform any services outside the scope of the contract without an official modification issued by the KO. The CM shall ensure contractor employees understand that services performed outside the scope of the contract are performed wholly at the expense of the contractor.

1.4.10 Identification of Contractor Employees: All contractor personnel attending meetings, answering Government telephones and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression that they are Government employees. The contractor shall ensure that all documents or reports produced by contractor personnel are suitably marked as contractor products or that contractor participation is appropriately disclosed. The contractor's status as a "contractor" shall be predominantly displayed in all correspondence types (to include signature blocks on e-mail) and dealings with Government or non-Government entities. Contractor personnel shall wear identification badges distinguishing themselves as such. The badges shall have the company name, employee name and the word "contractor" displayed.

1.4.10.1 Reserved

1.4.11. Combating Trafficking in Persons: The United States Government has adopted a zero-tolerance policy regarding trafficking in persons. Contractors and contractor employees shall not engage in severe forms of trafficking in persons during the period of performance of the contract; procure commercial sex acts during the period of performance of the contract; or use forced labor in the performance of the contract. The Contractor shall notify its employees of the United States Government's zero tolerance policy, the actions that will be taken against employees for violations of this policy. The contractor shall take appropriate action, up to and including termination, against employees or subcontractors that violate the US Government policy as described at FAR 22.17.

1.4.12 Reserved

1.4.13 Reserved

1.4.14 Organizational Conflicts of Interest (OCI): The contractor and subcontractor personnel performing services under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent OCIs, as defined in FAR Subpart 9.5. The contractor shall notify the KO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the KO to avoid or mitigate any such OCI. The contractor's mitigation plan will be determined to be acceptable solely at the discretion of the KO. In the event the KO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the KO may impose other remedies as he or she deems necessary, including prohibiting the contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.4.15 Reserved

2.0 Definitions and Acronyms:

2.1 Definitions:

2.1.1 Contractor: A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

2.1.2 Defective Service: A service output that does not meet the standard of performance associated with the PWS.

2.1.3 Deliverable: Anything that can be physically delivered and includes non-manufactured things such as meeting minutes or reports.

2.1.4 Key Personnel: Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.5 Physical Security: Actions that prevent the loss or damage of Government property.

2.1.6 Quality Assurance: The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.7 Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.8 Quality Control: All necessary measures taken by the Contractor to ensure that the quality of an end product or service shall meet contract requirements.

2.1.9 Subcontractor: One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.2 Acronyms:

AEI	Army Enterprise Infostructure
AR	Army Regulation
AT/OPSEC	Antiterrorism/Operational Security
BI	Background Investigation
CDTF	Counterdrug Task Force
CM	Contract Manager
CMD	California Military Department
COR	Contracting Officer Representative
DA	Department of the Army
DD254	DoD Contract Security Classification Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DSCA	Defense Counterintelligence and Security Agency
FAR	Federal Acquisition Regulation
GFP/M/E/S	Government Furnished Property/Material/Equipment/Services
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IS	Information System(s)
KO	Contracting Officer
NGB	National Guard Bureau
OCI	Organizational Conflict of Interest
PII	Personally Identifiable Information
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
SCR	Service Contract Reporting
SSN	Social Security Number
TE	Technical Exhibit
USD(I)	Under Secretary of Defense for Intelligence

3.0 Government Furnished Property, Material, Equipment and Services (GFP/M/E/S): The Government will provide the property, material, equipment, and/or services listed below solely for the purpose of performance under this contract: None

3.1 Reserved

3.2 Reserved

3.3 Reserved

3.4 Reserved

3.5 Utilities: All utilities in the facility will be available for the contactor's use in the performance of this contract. The contractor shall instruct employees in utilities conservation practices. The contractor shall operate under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount.

4.0 Contractor Furnished Property, Materials, and Equipment (CFP/M/E):

4.1 General: Except for those items specifically stated to be Government-Furnished in Paragraph 3.0, the contractor shall furnish everything required to perform these services as indicated in Paragraph 1.1.

4.2 Reserved

4.3 Reserved

5.0 Requirements:

The contractor shall furnish, install, and configure a complete Trade Agreements Act (TAA)-compliant facility security system consisting of an intrusion detection alarm system, a standalone camera surveillance system, and a keyless entry access control system. The contractor shall provide all TAA-compliant equipment, materials, software, tools, and labor necessary to deliver a fully functional and compliant security solution.

For the camera surveillance and keyless entry systems, the contractor's requirement is to equipment provision, installation, configuration, and a standard warranty. No monthly monitoring, maintenance, or inspection services are required for the camera or keyless entry systems.

Continuous 24/7 remote monitoring, monthly inspections, diagnostics, and emergency repair services are only required for the intrusion detection system (IDS). The IDS shall secure the suite against unauthorized entry through sensors such as glass break detectors, door breach sensors, and interior motion detectors. For the IDS, the contractor shall ensure immediate response, notification, and escalation in accordance with reporting timelines defined in this PWS; notify the COR of all malfunctions immediately; and ensure redundancy and continuity of operations.

5.1 <u>Intrusion Detection:</u> The system shall be capable of fully securing the suite by detecting and preventing unauthorized entry. Upon activation of any intrusion-related event, the system shall immediately trigger the alarm and initiate all required alerting functions. To ensure continuous operation, the system shall incorporate redundant power and communication pathways that allow it to remain functional during primary

power loss or communication disruptions. In addition, the system should include an audible alarm component of sufficient volume and clarity to deter further unauthorized activity and to alert personnel in the vicinity to a potential security breach.

5.1.1 The contractor shall provide continuous monitoring of the alarm system 24 hours per day, 7 days per week (24/7), to ensure immediate awareness and response to any alarm activation. Monitoring shall include real-time oversight of all intrusion detection sensors installed within the suite. Alarm triggering devices include, but are not limited to, glass break sensors designed to detect forced entry through windows or glass partitions; door breach sensors that register unauthorized opening, tampering, or forced access; and interior motion detection sensors that identify unauthorized movement within the protected area. The contractor shall maintain the capability to promptly identify, assess, and escalate any alarm event in accordance with the reporting and response procedures detailed in this PWS, ensuring uninterrupted situational awareness and timely notification to the appropriate Government personnel.

5.1.2 The contractor shall report all alarm triggers within one (1) minute of an alarm triggering event, or if communication with the alarm system is interrupted for more than two (2) minutes. The contractor shall notify the COR and/or designated point of contact (POC) via cellular telephone call, text message, and email notification. If POCs do not respond to alerts within five (5) minutes, the contractor shall call local law enforcement authorities out to the location.

5.1.3 The contractor shall complete any required IDS functions test or system synchronization on the same day that monitoring services begin.

5.1.4 Inspections: The contractor shall perform a monthly system test/inspection to ensure the alarm system is in good working order and remote monitoring is fully functional. Scheduled system tests/inspections shall be coordinated with the COR prior to performing this action.

5.1.5 Maintenance/Repair: The contractor shall immediately alert the POC/COR in the event of a malfunction to any portion of the alarm system. Within two (2) hours of any malfunction, the contractor will complete a system diagnostic assessment and provide the POC/COR with a technical description of the fault, recommended immediate and/or remedial actions, and an estimated task completion time to correct/clear or repair faults.

If the malfunction requires physical repair or cannot be resolved remotely, the contractor shall dispatch an on-site technician to perform an in-person follow-up at the facility within twelve (12) hours of the initial two (2) hour diagnostic response. In the event of a malfunction or issue, the contractor shall complete emergency repair/replacement services to restore full system operations. Any site visit needed shall be at a fixed rate established and provided at the time of award.

5.1.6 Reports: The contractor shall provide reports to the COR and designated POC at the frequency indicated in Section 5 of this PWS. The reports shall contain at a minimum: alarm event date, alarm event time, and type of alarm event (armed, disarmed, unsuccessful attempt, motion detected, break-in, fault).

5.1.6.1 Test/Inspection Report: After completion of each monthly functions test, the contractor shall provide a report detailing any found functions issues no later than 72 hours of the completed test/inspection.

5.1.6.2 Access Report: The contractor shall provide a system that features a web-based access report available to the COR. The report will detail by username the time and location of arming, disarming, and access granted to interior rooms.

5.1.6.3 Within one (1) hour of an alarm triggering event, the contractor shall provide a log file documenting alarm access attempts over the last 48 hours.

5.1.6.4 No later than the 5th business day of the month, the contractor shall provide a log file documenting all alarm access attempts from the previous month.

5.1.6.5 Within 24 hours of a request from the COR, the contractor shall provide a log file of all alarm access attempts for the last 48 hours.

5.2 Camera System: The system shall include all-weather, tamper-resistant day/night cameras located on the building interior and exterior capable of high-definition resolution sufficient to identify people and vehicles. Cameras shall provide coverage of the building's designated interior rooms to include the break room, supply room, and front entrance area; exterior perimeter, both entrances, and the front row of vehicle parking spaces. The system shall also include an internal data storage capability of 4TB or greater. The cameras are not required to interact with or activate the alarm system.

5.2.1 Recording: The cameras shall be capable of continuous recording to a secured web-based storage site with a 30-day retention period and allow for remote access/viewing by the user.

5.2.2 Standard Warranty: The contractor shall provide a standard manufacturer and installation warranty for all camera system equipment and configurations. No monthly maintenance, inspections, or monitoring services are required by the contractor for this system post-installation.

5.2.3 System Control: The contractor shall provide the COR and designated POCs with full administrative access to the camera system upon installation completion. The system shall be user-configurable, allowing authorized Government personnel to securely view live feeds, review recorded footage, download video files, adjust user permissions, and manage access credentials. The system shall support remote access through a secure, authenticated web-based platform and shall operate fully independent of the alarm system.

5.2.4 Access Report: The contractor shall configure a web-based camera system access report that is continuously available to the COR and designated POCs. The report shall document all user access activity to the camera system, including usernames, dates, times, and the specific functions accessed (such as live view access, playback review, video downloads, or administrative changes). The system shall

maintain accurate, real-time logging of all user interactions to ensure authorized Government personnel can securely view, download, and retain these records for auditing purposes.

5.3 Keyless Entry System: The contractor shall provide and install a keyless access control system that secures the building, server room, storage room, and any additional rooms designated by the COR. Within 24 hours of completing the initial installation and synchronization, the contractor shall provide the COR and designated POCs with access to the system. The system shall support secure electronic access using key cards, key fobs, and app-based smartphone credentials, and shall be fully user-configurable to grant, modify, and revoke access for up to 100 users. Authorized Government personnel shall be able to manage user permissions in real-time, assigning access on a per-user and per-location basis. The system shall operate reliably across all designated entry points and maintain accurate, real-time logging of all access attempts.

5.3.1 Standard Warranty: The contractor shall provide a standard manufacturer and installation warranty for all keyless entry system hardware, software, and configurations. No monthly maintenance, inspections, or monitoring services are required by the contractor for this system post-installation.

5.3.2 System Control: The contractor shall provide the COR and designated POCs with full administrative control of the keyless entry system upon installation. Authorized Government personnel shall be able to add, modify, and revoke user credentials; configure access permissions for designated rooms; and review system activity logs in real-time. The administrative interface shall be secure, user-friendly, and accessible through a web-based platform with authenticated login. The keyless entry system shall operate independently of the alarm and camera systems.

5.3.3 Access Report: The contractor shall configure a web-based keyless entry access report that is continuously available to the COR and designated POCs. The system shall document, by individual username, all access-related activity occurring at any controlled entry point. Each entry in the report shall include the date, time, access location, whether access was granted or denied, and any system-recorded anomalies. The system shall maintain accurate, real-time logging of all credential usage and administrative actions for Government oversight and auditing.

5.4. Reserved

5.5 Reserved

5.6. Reserved

6.0 Applicable Publications: Publications applicable to this PWS are listed below:

Publication (Chapter/Page)	Date of Publication	Website
Federal Acquisition Regulation		https://www.acquisition.gov/

Defense Federal Acquisition Regulation Supplement		http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html or https://www.acquisition.gov/dfars
Joint Travel Regulation (JTR)		https://www.defensetravel.dod.mil/site/travelreg.cfm
DoDM 1000.13-M-V1 DoD Identification (ID) Cards (Enclosure 2, paragraph 3.b)	01/23/2014 (Change 1: 07/28/2020)	http://www.esd.whs.mil/Directives/issuances/dodm
Federal Information Processing Standards (FIPS) Publication 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (paragraph 9)	August 2013	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
DoDM 5200.2 Procedures for the DoD Personnel Security Program (PSP)	04/03/2017	https://www.esd.whs.mil/Directives/issuances/dodm/
DoDI 5200.46 DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)	09/09/14 (Change 1: 05/04/2018)	https://www.esd.whs.mil/Directives/issuances/dodi/
Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification Standard for Federal Employees and Contractors	08/27/2004	https://www.dhs.gov/homeland-security-presidential-directive-12
DoDI 5400.11 Department of Defense Privacy and Civil Liberties Programs	01/29/2019	https://www.esd.whs.mil/Directives/issuances/dodi/
DoD 5400.11-R Department of Defense Privacy Program	05/14/2007	https://www.esd.whs.mil/Directives/issuances/dodm/
DoDD 8140.01 Cyberspace Workforce Management	10/05/2020	https://www.esd.whs.mil/Directives/issuances/dodd/
DoD 8570.01-M Information Assurance Workforce Improvement Program	12/19/2005 (Change 4: 11/10/2015)	https://www.esd.whs.mil/Directives/issuances/dodm/
DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)	02/28/2006 (Change 2: 05/18/2016)	https://www.esd.whs.mil/Directives/issuances/dodm/
Army Directive 2014-05 Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	03/07/2014	https://armypubs.army.mil/ProductMaps/PubForm/ArmyDir.aspx
AR 25-2 Information Assurance	04/04/2019	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 530-1 Operations Security	09/26/2014	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 525-13 Antiterrorism	12/09/2019	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 381-12 Threat Awareness and Reporting Program (TARP) (Section II, ¶ 2-4.b)	06/01/2016	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx

6.1 Applicable Forms: Forms applicable to the PWS are listed below:

Form	Date	Website
DD 1172-2 Application for Identification Card/DEERS Enrollment	Mar 2017	http://www.dtic.mil/whs/directives/forms/index.htm
I-9 Employment Eligibility Verification	Oct 2019	https://www.uscis.gov/sites/default/files/files/form/i-9.pdf
DD 441 Department of Defense Security Agreement	Feb 2020	http://www.dtic.mil/whs/directives/forms/dd/ddforms0001-0499.htm
DD 250 Material Inspection and Receiving Report	Aug 2000	https://www.esd.whs.mil/Directives/forms/dd0001_0499/

7.0 Attachments

7.1 TECHNICAL EXHIBIT 1 – Performance Requirements Summary (PRS)

7.2 TECHNICAL EXHIBIT 2 – Deliverables

7.3 TECHNICAL EXHIBIT 3 – Equipment List

7.4 TECHNICAL EXHIBIT 4 – Floor Plan

TECHNICAL EXHIBIT 1

Performance Requirements Summary (PRS)

This PRS includes performance objectives the Government will use to determine contractor performance and will compare contractor performance to the Acceptable Quality Level (AQL).

Performance Objective	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
5.1.1 & 5.1.2 IDS: Continuous Monitoring & Alerting	Contractor provides 24/7 monitoring. Alarm triggers reported within 1 minute (or within 2 mins of comms loss). Notifies COR/POC via call/text/email. Dispatches local law enforcement if POCs do not respond within 5 minutes.	0% deviation. 100% of critical alarms must be reported and escalated within the prescribed timelines.	System access logs, COR verification of receipt of notifications, monthly test results.
5.1.3 & 5.1.5 IDS: Maintenance & Diagnostics	Immediate notification to COR of any system malfunction. Diagnostic assessment with technical description and estimated repair time provided within two (2) hours of malfunction.	95% compliance for delivering the diagnostic report within the 2-hour window. 100% compliance for immediate initial notification.	COR observation, email time-stamps, submitted diagnostic reports.
5.1.4 IDS: Monthly Inspections & Testing	Conduct scheduled monthly system test/inspection coordinated with COR. Submit finding report within 72 hours of test completion.	100% compliance. Monthly inspections cannot be skipped. Reports must be submitted within 72 hours.	COR direct observation/participation in tests, receipt of monthly inspection report.
5.1.6 IDS: Event & Access Reporting	Provide log files within 1 hour of an alarm event, within 24 hours of a CDTF request, and standard monthly logs by the 5th business day. Maintain web-based access report.	95% compliance for routine monthly log delivery timeline; 100% compliance for post-incident (1-hour) log delivery.	COR review of received log files and web portal availability.
5.2 Camera System: Installation & Configuration	Install TAA-compliant system. Configure 30-day web-based storage. Turnover full administrative control to COR.	100% compliance required for final Government acceptance and sign-off	100% Government Inspection at time of installation and turnover. Warranty claim tracking.
5.3 Keyless Entry: Installation & Configuration	Install TAA-compliant system for up to 100 users. Configure web-based access reporting and turnover full administrative control to COR.	100% compliance required for final Government acceptance and sign-off.	100% Government Inspection at time of installation and turnover. Warranty claim tracking.

TECHNICAL EXHIBIT 2

Deliverables Schedule

PWS Reference / Deliverable Title	Frequency / Timeline	Number of Copies	Medium/Format	Submit To
1.4.3 Quality Control Plan	Within 10 calendar days of contract award.	1	Electronic Mail	COR
1.4.5.11 OPSEC Training Certificates	Within 15 calendar days after employee completes training.	1	Electronic Mail	COR
5.1.2 IDS Alarm Trigger Notification	Within one (1) minute of alarm event, or within two (2) minutes of communication loss.	1	Call, Text, *and* Electronic Mail	COR / POCs
5.1.5 IDS Diagnostic Report	Within two (2) hours of any identified system malfunction.	1	Electronic Mail	COR / POCs
5.1.7 IDS Monthly Inspection Report	Within 72 hours of completing the scheduled monthly functions test.	1	Electronic Mail	COR
5.1.10 IDS Monthly Access Log	No later than the 5th business day of the following month.	1	Electronic Mail (Log file)	COR
5.2 & 5.3 Camera & Keyless Entry Turnover	One-time requirement: Within 24 hours of completing initial installation and synchronization.	1	Electronic Mail & In-Person turnover	COR

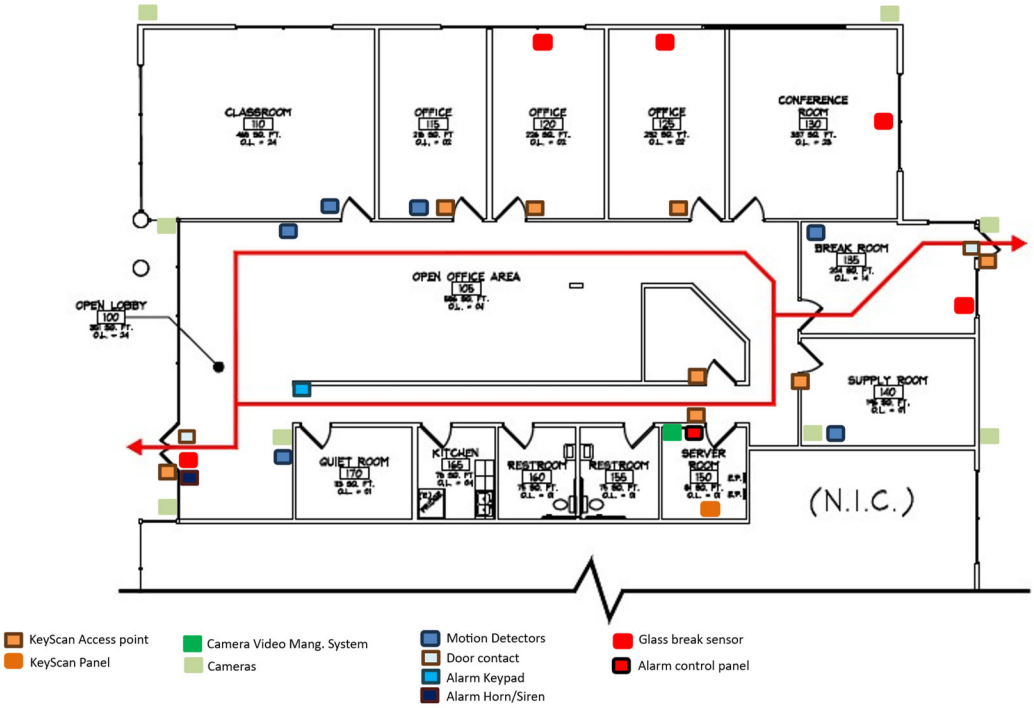
TECHNICAL EXHIBIT 3

Equipment List

The items listed below are provided for guidance purposes only. The specified manufacturer brand names and model numbers are used to establish the minimum standards of quality, performance, and compatibility required by the Government. Salient characteristics listed equal or better products will be considered.

ITEM	NAME	QUANTITY
1	PROFUSION ACCESS CONTROL CABLE 18 4 OAS + 22 12 STR 5C CMR J	800
2	PS Series 12V, 7Ah General Purpose Rechargeable SLA Battery,	2
3	Premium: Pack of 1 entry	8
4	Core Series 8 Port 12/24 Smart Hub, 8 Entry Capacity, Power	1
5	High Frequency Access Cards Solid - Pack Of 10	5
6	Tailored End User Training 1- Hour Sessions Dedicated To Specific Account Management And Use Cases	1
7	Standard Smart Reader - V2	8
8	Alta A100 With 4TB Net Storage, Up To 1 GB Base T Network Connection, Supports Up To 10 Cameras, 1 H	1
9	12V 7AH Sealed Lead Acid Battery, F1 Terminal	1
10	24/4 C5E CMR WHT 5C BOX	1300
11	Alta Cloud Storage License	8
12	Alta Aware Cloud camera - Dome white. 5MP resolution	8
13	Pendant mounting cap for Alta Dome and 360 cameras	8
14	Wall mount arm for Alta Dome and 360 cameras. Pendant	8
15	XR150NL-G, 7160-WP1, 263LTE-V/381-2	1
16	INDOOR SIREN	1
17	Wireless PIR Motion Detector with pet immunity and disarm/disable. 90 degree 40' x 40'	6
18	High Power Receiver For Xr150 And Xr550 Wireless Systems	1
19	12V 7AH Sealed Lead Acid Battery, F1 Terminal	1
20	WIRELESS UNIVERSAL TRANSMITTER	6
21	18/4 STR JKT CL2P 5C BX BGE	50
22	CONTACT SURFACE MOUNT	6
23	Wireless Glassbreak Detector	5

TECHNICAL EXHIBIT 4

FLOOR PLAN

Intrusion Detection System
3,958 sf