PERFORMANCE WORK STATEMENT (PWS)
Pentagon Force Protection Agency (PFPA)
Integrated Security Services Contract 5 (ISSC)

PART 1
GENERAL INFORMATION

1 INTRODUCTION: This is a non-personal services contract to provide Integrated Security Services. The Government shall not exercise any supervision or control over contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Prime Contractor who, in turn is responsible to the Government.

1.1 BACKGROUND: Previous contracts for this requirement provided comprehensive security integrator services to PFPA. Since inception, contract scope has expanded to include additional facilities, new systems, and increased security capabilities. This contract provides baseline support (system support, maintenance, repair, and logistics) to security applications to multiple PFPA facilities. The baseline support will be issued as task order one. Subsequent task orders will be for ordering hardware and installation of security systems and components in facilities identified by PFPA.

1.2 DESCRIPTION OF SERVICES: The PFPA ISSC is a total system approach for providing integrated electronic and physical security systems for the Pentagon Reservation, Mark Center, Defense Health Headquarters (DHHQ), DoD owned and leased facilities, Herbert R. Temple. Jr. Army National Guard Readiness Center (TARC), and Raven Rock Mountain Complex (RRMC) in Adams County, PA.

All services provided by the Contractor, including but not limited to design, implementation, and quality assurance, shall meet the following standards:

High Performance: The system must meet or exceed all performance benchmarks defined in the contract. This includes, but is not limited to, response times, data processing speeds, and alert generation, ensuring that the system supports the high-tempo environment of the security operations centers.

Contractual Compliance: The Contractor shall deliver all systems and services in strict accordance with the terms, conditions, and service level agreements (SLAs) specified in the contract. Quality checks and comprehensive testing shall be conducted to verify that all requirements are met or exceeded prior to delivery and acceptance.

User-Friendly Design: All system interfaces and user-facing functionalities shall be designed with a primary focus on user experience (UX). The system should be intuitive, easy to navigate, and require minimal training for operators to perform their duties effectively.

Minimal Workspace Impact: The Contractor shall conduct all on-site activities, including installation, maintenance, and upgrades, in a manner that minimizes disruption to the customer's workspace and ongoing operations. All work must be coordinated and scheduled with government representatives to reduce impact on sensitive areas.

1.3 OBJECTIVES: The Government's four, inter-related high-level objectives for the ISSC are:

Scalability and Interoperability – Systems shall be capable of scaling to accommodate additional users, sensors, capabilities, and facilities. Similarly, systems shall be able to adjust down as facilities are closed, suites are decommissioned, or requirements adjusted. Systems and their components shall to the maximum extent possible, utilize open standards and commercial-off-the-shelf (COTS) technology. Standard network protocols shall be used to traverse the Government's network. Wherever computers are required, they shall be widely available models based on open systems architecture. Standard operating systems shall be used, such as but not limited to Microsoft Windows, Linux, and UNIX for the computer-based systems provided under ISSC.

Availability and Resiliency – The Government has a goal of operating ISSC systems at or near a 100% operational level. Systems shall be designed and implemented to be resilient to failure such that a failure of a single component should not incapacitate the entire system. To achieve this goal, the Contractor shall leverage industry best practices for assuring resiliency and availability, including but not limited to:

- Built-in redundancy
- Automatic failover
- Fault tolerance
- Virtual environments
- Data backup
- Data archiving
- Automatic updates of operating systems (OS) and applications
- Notification of software/hardware approaching end of life
  Power-on replacement i.e. hot swapping components or peripherals
- Power Continuous i.e., uninterruptible power supplies (UPSs)
- Backup power i.e. batteries and generators
- Surge suppressors

For the purposes of this contract, system reliability is defined as the probability that a system or subsystem, including all hardware, firmware, and software will satisfactorily perform the intended function(s) for which it was designed, during the duration for which it is in operation, and in the operational environment. The Contractor shall maintain system reliability at a level equal to, or higher than, the systems documented percentage or failure rate provided by the manufacture and/or as required by regulatory requirements for classified areas.

For the purposes of this contract, system availability is defined as the ratio of time a system, subsystem, or component is functional to the total time it is required or expected to function.

For the purposes of this contract, system serviceability is defined as the ease with which a component, device, or system can be maintained and repaired. All precautions should be taken to maintain and repair systems to cause as little downtime or disruption as possible and within the expected reliability and availability standards stated in this contract. The Contractor shall notify the government of any potential problems or recommended actions critical to systems operations that can be addressed by maintenance and repair, as far in advance as possible to minimize downtime or failure.

Factors that do not impact contractual requirements for system reliability, availability, or serviceability are where root cause of problems are as a result of network, power, or other external factors outside the scope of this contract and maintained by OGAs or Other Government Contractors (OGC). Outages caused by

external factors shall not count against the availability or reliability statistic until the network, power, or other external factor has been restored, but may require support for the application or equipment impacted. However, the Contractor must work across all task orders and appropriate stakeholders to track problem resolution, help troubleshoot and verify problem resolution and provide continuous updates to the Government.

Reliability and Cost Sustainability – Systems and services shall be affordable across the full lifecycle while meeting the Government's requirements, minimize the use of custom and proprietary solutions, and remove systems, hardware, and software before they incur excessive sustainment costs or reach end of service.

Accountability and Customer Satisfaction – Systems and services shall be designed and implemented, and quality checked (i.e. QA/QC) to be user friendly, mindful of the impact and sensitivities of the customer workspace, high performing, and to meet contractual service requirements

1.4 SCOPE: This contract shall require the contractor to maintain, repair, install, and support all aspects of electronic security systems, including but not limited to, access control; intrusion detection; video surveillance and intelligent video analytics; physical security information management; license plate recognition; gunshot detection; under vehicle inspection; identity, credential, and access management; mass notification; biometric and multi-modal authentication; computer aided dispatch and other law enforcement mission applications; chemical, biological, radiological detection and mitigation; personnel and facility screening, deterrence and detection technology, In Place Monitoring System, wireless detection systems, and operations center collaboration visualization systems, all of which may be stand alone or integrated into an existing system infrastructure.

In addition, the contract shall support all aspects of physical security, including but not limited to, personnel, vehicle, cargo, and parcel screening systems; ballistic rated glass, booths, kiosks, mobile shields; blast-resistant waste receptacles, doors (sound-rated and force protection), window film, locks, and door hardware.

The contractor shall support all aspects of passive and active barriers, including but not limited to, turnstiles, fencing, bollards, gates, traffic control gate arms and anti-vehicle barriers. This contract requires support on infrastructure supporting the above systems, including but not limited to, cabling for electrical and information technology, trenching, grading, utilities, conduit placement, and other civil types of work.

All aspects of the scope will be provided in detail through task orders, to include the first task order to maintain, support, repair, and manage all electronic security systems at the Pentagon, RRMC, and other DoD facilities owned and leased in the National Capital Region (NCR).

To deliver these capabilities, the Contractor shall provide the following services:

a) Full Lifecycle Systems Engineering. The Contractor shall be responsible for providing full lifecycle systems engineering services for upgrades or new electronic and physical security systems. The full lifecycle shall include requirements elicitation and analysis, design, development, testing, installation, configuration, integration, verification and validation, transition, sustainment, and decommissioning.

b) System Support, Sustainment, and Administration. The Contractor shall be responsible for sustainment support of electronic security systems. This support includes system monitoring, troubleshooting, patching and software updates, configuration, and administration.

c) Third Party Software and OGC Support. The Contractor shall provide support to 3rd party software integrations and the OGC installing and maintaining it. This support includes software upgrades, existing or new connections/integrations to ISSC systems, testing, troubleshooting and other areas impacting either

ISSC supported systems or those maintained by OGCs.

d) Preventative Maintenance. The Contractor shall be responsible for performing periodic preventative maintenance on all electronic and physical security systems identified in this Performance Work Statement (PWS) as well as any components installed during this contract unless specified in the individual task order PWS. Periodic preventative maintenance shall be performed at minimum in accordance with manufacturer recommendations and may require additional preventative maintenance work due to amount of use or ambient conditions.

e) Repair and Sustain. The Contractor shall be responsible for responding to and repairing damaged, malfunctioning, or inoperable systems and their components as described in this PWS as well as any components installed during this contract unless specified in the individual task order PWS.

f) Configuration Management. The Contractor shall maintain a database of all ISSC electronic and physical security systems characteristics.

g) Logistics Management. The Contractor shall be responsible for procuring, storing, and inventory of materials and supplies to deliver services under this contract.

h) Quality Management. The Contractor shall be responsible for tracking, baselining, and identifying deviations from ISSC and manufacturers standards for quality and performance.

i) Installation, Decommissioning, Hardware, and Alterations. The Contractor shall be responsible for hardware, installation, extension, relocation, and alterations of electronic and physical security systems per ISSC and manufacturer standards.

j) Design and Technical Evaluation. The Contractor shall be responsible for performing technical evaluations of new and existing electronic and physical security systems to assess their capacity to meet requirements, maturity, and their continued use.

k) Training. The Contractor shall be responsible for delivering initial and reoccurring training on electronic and physical security systems to Government and Contractor personnel.

l) Cybersecurity and Network Infrastructure Engineering. The Contractor shall be responsible for maintaining the Risk Management Framework documentation and coordinate the submission for review of all system data on the network, to ensure applications and hardware are maintained to meet cybersecurity requirements. Additionally, the Contractor shall provide support to ensure applications, systems, and hardware of the security systems operates effectively on the Government network infrastructure.

1.4.1 Overall Enterprise Contractor Responsibilities

The Contractor shall provide comprehensive lifecycle sustainment, administration, and modernization for all Integrated Security Services deployed across the Pentagon Force Protection Agency (PFPA) enterprise. The Contractor assumes full operational responsibility for both current and future mission assets deployed on the Life Safety Backbone (LSB):

System Category	Operational Scope
Existing Baseline Systems	Continuous servicing, proactive maintenance, and administration of all hardware, software, and IT infrastructure present at the time of contract award (as distinctly defined within Task Order 1 and Task Order 2).

Future & Upgraded Systems	Seamless integration, testing, and sustainment of any new capabilities introduced during the contract lifecycle, regardless of whether they were installed by this Contractor or integrated by third-party government vendors via separate projects.

1.4.2 ISSC Contract Operations Framework

This IDIQ contract serves as the enterprise vehicle to install, maintain, repair, and secure mission-critical security systems across the Pentagon and designated National Capital Region (NCR) facilities. The operational work is bifurcated into two foundational Task Orders (TO1 and TO2) designed to sustain the current operational baseline while architecting a secure environment for future technology modernization. All subsequent task orders and credit card purchases executed under this IDIQ will structurally align with this framework.

1.4.3 Core Task Order Alignment

The success of the PFPA mission relies on the execution of two distinct but entirely symbiotic task orders.

Task Order	Operational Focus	Key Performance Requirements
TO1: Security Systems & Mission Applications	Endpoint Functionality & Daily Mission Operations: Focuses on the physical security apparatus and user-facing applications.	Full lifecycle management (design, installation, preventative maintenance, and decommissioning) of physical access control, video surveillance, intrusion detection, and associated software. The Contractor must staff and manage a 24/7/365 Network Control Center (NCC) to deliver rapid triage, dispatch, and technical repair for endpoint systems.
TO2: IT Infrastructure, Platform Health & Cybersecurity	Platform Resilience & Network Security: Focuses on the underlying secure IT network and hardware platform that enables physical security operations.	Proactive administration of the Life Safety Backbone (LSB)including all networks, servers, and databases hosting TO1 systems. The Contractor must maximize platform health, ensure high availability, and execute all cybersecurity duties. This includes rigorous RMF compliance, STIG application, vulnerability patching, and maintaining a continuous Authority to Operate (ATO).

1.4.4 Strategic Interdependency & Operational Synchronization

TO1 and TO2 operate within a shared mission ecosystem and are structurally interdependent. TO1 mission applications cannot be executed without the stable network provided by TO2; conversely, the TO2 infrastructure exists exclusively to securely host TO1 mission applications.

The Contractor shall not operate these task orders in silos. The Contractor must enforce continuous synchronization, communication, and joint change-management between the TO1 and TO2 operational teams across the following areas:

Integration Pillar	Synchronization Mandates
Coordinated Cybersecurity & Patch Management	The TO2 infrastructure team must strictly coordinate all network changes, vulnerability patching, and security updates with the TO1 applications team. All cybersecurity actions must be tested and phased to guarantee that platform updates do not disrupt, degrade, or disconnect active TO1 physical security devices.
Unified Platform	Both task orders share the responsibility for overall LSB platform health. Hardware

Health	degradation identified by TO2 must be communicated to TO1 to anticipate application impact, and application latency identified by TO1 must be analyzed by TO2 to optimize infrastructure routing or compute power.
Future Capability Alignment	All future task orders, technology insertions, or micro-purchases executed under this IDIQ must be validated against both TO1 operational requirements and TO2 cybersecurity constraints prior to integration.

1.5 PERIOD OF PERFORMANCE: The period of performance shall be for a five-year base ordering period, and five option period.

1.6 CONTRACT TYPE: The Government will award a Firm Fixed Price Performance Based IDIQ.

1.7 PLACE OF PERFORMANCE: PFPA provides protection for DoD facilities in the National Capital Region (NCR). This region extends from Northern Virginia through lower Pennsylvania. The current locations of DoD facilities protected by PFPA will be provided at the task order level and are listed in Appendix A. Facilities occupied by the Government change based on multiple factors and may increase or decrease throughout the duration of this contract. The Contractor is fully responsible for performing work at all facilities protected by PFPA.

1.8 TELEWORK: Unless otherwise specified/approved by the COR, the Contractor shall perform the work onsite or at the ISSC laboratory. In the case where the teleworking is approved, the work must be accomplished at no additional cost to the Government and with no negative impacts to contract performance. Telework will be provided at the Task Order Level.

1.9 HOURS OF OPERATION: Hours of Operation will be addressed at the task order level.

1.9.1 On-Site Working Conditions, Holidays, and other Closures: Due to the nature of the work, some 24/7 operations will continue during holidays or Government closures.

1.9.2 Washington Headquarters Services facilities are smoking restricted workplaces. Due to the nature of the work, facilities, and requirements, Contractor staff may only smoke outside in designated smoking areas.

1.9.3 The facilities are open 24/7, but the majority of the work will occur during business hours, between 0600 and 1900 *Eastern* Time (ET) Monday through Friday, but these hours are subject to the task order requirements.

1.10 RECOGNIZED HOLIDAYS: Government personnel observe the following holidays as governed by 5 U.S.C. § 6103. Government facilities will be closed and unavailable to Contractor personnel:

New Year's Day	Labor Day	Martin Luther King Jr.'s Birthday
Columbus Day	Washington's Birthday	Veterans Day
Memorial Day	Thanksgiving Day	Juneteenth
Independence Day	Christmas Day	

*If the date falls on a Saturday, the Government holiday is the preceding Friday. If the date falls on a Sunday, the Government holiday is the following Monday.

In addition to the days designated as holidays, the Government observes the following days:
- Any other day designated by Federal Statute
- Any other day designated by Executive Order
- Any other day designated by the President's Proclamation

1.11 QUALITY CONTROL/ASSURANCE:

1.11.1 Quality Control: The Contractor shall develop and maintain an effective quality control program 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 quality control program is the means by which it ensures that its work complies with the requirement of the contract. The quality control plan will be submitted with the first two task orders of the contract. After acceptance of the quality control plan, the Contractor shall receive the Contracting Officer's acceptance in writing of any proposed change to its quality control program.

1.11.2 Quality Assurance: The Government shall evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must 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 the minimum acceptable defect rate(s).

1.12 PERSONNEL MATTERS

1.12.1 Key Personnel: Key personnel will be addressed at the task order level.

1.12.2 Identification of Contractor Employees: All contract 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 in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed.

1.12.5 Special Qualifications: Based on the task order, contractors shall have appropriate certifications, relevant skill sets and experiences to perform the ISSC task orders and cybersecurity tasks.

1.12.6 The Contractor shall submit certificates of completion for each affected Contractor employee and Subcontractor employee, to the COR or to the Contracting Officer. This training shall be completed and reported to the COR within 30 calendar days of contract award and annual refresher training for the remaining contract duration.

1.13 SECURITY:

1.13.1 The security requirements are in accordance with the DD254.

1.13.2 Contractors are required to report to PFPA any derogatory information that may justify an unfavorable administrative action in a personnel security or building access determination.

Derogatory information includes, but is not limited to, criminal conduct, illegal drug involvement, or psychological conditions that impair judgment, reliability or trustworthiness. Derogatory information must be provided to the COR and Contracting Officer as promptly as possible, but in no event later than three (3) business days after the contractor becomes aware of the information.

1.13.3 PFPA reserves the right and prerogative to deny and/or restrict facility and information access of any Contractor employee determined by PFPA at any time during performance to be unsuitable for access and/or present a risk of compromising sensitive Government information to which they would have access under this contract.

1.13.4 A determination by PFPA that a person is not suitable to perform work under this contract is not a denial, suspension or revocation of a previously granted security clearance by another agency, nor shall it be interpreted as a direction or recommendation to the Contractor regarding the suitability of an affected individual for employment outside the scope of PFPA.

1.13.5 Due to the sensitive of the scope of the program and task orders and the wide variety of program assignments anticipated under the contract, personnel who have been previously denied or relieved of any security duties or other security-related duties for reasons of security violations, negligence, or nonperformance of duties will not be deemed acceptable unless specifically approved by the Government and an investigation into the circumstances surrounding the denial has been completed and information provided to the KO.

1.13.6 Key Control: The Contractor shall establish and implement methods of making sure all keys/Common Access Card (CAC) issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. **NOTE:** All references to keys include CACs. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the QCP. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/CAC to the COR.

1.13.7 The Contractor shall prohibit the use of Government issued keys/CAC 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 Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the COR.

1.13.6 Lock Combinations: The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. These procedures shall be included in the Contractor's QCP.

1.14 CONTRACT ADMINISTRATION

1.14.1 Post Award Conference/Periodic Progress Meetings: Post Award Conference/Periodic Progress Meetings will be addressed at the task order level.

1.14.2 Phase-in/Phase-out Period Phase in/Phase out Period will be addressed at the task order level.

1.15 OTHER DIRECT COST (T&M and LH):

Other Direct Costs will be addressed at the task order level.

1.16 CONFLICT OF INTEREST:

1.16.1 Organizational Conflict of Interest/Personal Conflict of Interest: Contractor and Subcontractor personnel performing work 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 Organizational Conflict of Interest (OCI) as defined in FAR Subpart 9.5 as well as personal conflicts of interest. Using the Contractor OCI/ COI Disclosure Form, the Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential conflict and shall promptly submit the conflict-of-interest disclosure form to the Contracting Officer to avoid or mitigate any such conflict.

1.16.2 The Contractor's mitigation plan will be reviewed and accepted/rejected solely at the discretion of the Government, and in the event the Government unilaterally determines that any such conflict cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the conflict.

1.16.3 In addition, Contractors shall conduct internal reviews as necessary to identify financial interests and determine if any personal conflicts of interest exist or may arise. The Contractor shall ensure that the organization has analyzed each financial disclosure to determine whether actual or potential conflicts exist. Information should be gathered and analyzed for all governing body members (e.g., board of directors, trustees, etc.) and principals of the organization as defined by FAR 52.203-13 and for each manager and key personnel who would be or are involved with the performance of the contract.

1.16.4 All Contractor and Subcontractor employees supporting this contract shall sign the WHS AD non-disclosure agreements.

1.17 SMALL BUSINESS UTILIZATION

1.17.1 Small Business Participation Reporting: The contractor shall submit semiannually, a small business participation progress report on their small business utilization (format as agreed upon between contractor and Government) to the Contracting Officer and will be shared with the Washington Headquarters Services Office of Small Business Programs (WHS OSBP).

These reports shall be submitted concurrently with the subcontracting periods, during contract performance for the periods ending March 31 and September 30. A report is also required for each contract within 30 days of contract completion. Reports are due 30 days after the close of each reporting period, unless otherwise directed by the contracting officer. Reports are required when due, regardless of whether there has been any small business participation activity since the inception of the contract or the previous reporting Period. When a contracting officer rejects a SBPCD report, the contractor is required to submit a revised SBPCD report within 30 days of receiving the notice of the SBPCD report rejection.

Report actual subcontracting dollars/percentages achievements relative to the accepted small business participation. The reports shall cover:
Quantitative achievements
Small Business subcontracts awarded during reporting period

Contractor name and socioeconomic category
Dollar value of subcontract
Type of product or service provided by subcontractor
Order number
Contract specific initiatives and tools employed to enhance small business utilization or capabilities.

The reporting requirement shall be incorporated into the contract with the Contracting Officer's ability to require corrective action plans from the contractor in the event of unsatisfactory progress during a semi-annual reporting period for the MQR and any other small business participation requirements.

Any modification to the Small Business Participation Commitment Document must be pre-approved by the contracting officer prior to implementation.

PART 2
DEFINITIONS & ACRONYMS

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. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. DELIVERABLE. Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

2.1.6. 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 Key Personnel listed in 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.

2.1.7. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8. QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.11. SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.12. WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.12. WORK WEEK. Monday through Friday, unless specified otherwise.

2.2. ACRONYMS:

ACC	Access Control Center
AAR	After Action Review
ACOR	Alternate Contracting Officer's Representative
ACS	Access Control System
AMP	Access Management Portal
APL	Approved Products List
APO/FPO	Army/Air Post Office / Fleet Post Office
AQL	Acceptable Quality Level
ATO	Authority to Operate
BMS	Balance Magnetic Switches
BVMS	Bosch Video Management System
C2	Command and Control
CAC	Common Access Card
CAD	Computer Aided Dispatch
CCB	Configuration Control Board
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CHUID	Cardholder Unique Identifier
CM	Configuration Management
CMDB	Configuration Management Database
CMP	Configuration Management Plan
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer's Representative
COTS	Commercial-Off-the-Shelf
CSCIP	Certified Smart Card Industry Professional
CSCIP-G	Certified Smart Card Industry Government
CSEIP	Certified Engineer ICAM PACS
CSSP	Cybersecurity Service Provider
CUI	Controlled Unclassified Information
DBU	Database Unit
DCO	Defensive Cyber Operations

DD254	Department of Defense Contract Security Classification Specification
DFAC	Dining Facility
DFARS	Defense Federal Acquisition Regulation Supplement
DHHQ	Defense Health Headquarters
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DPO	Diplomatic Post Office
DRMO	Defense Reutilization and Marketing Office
ECC	Error Correction Code
ELMS	Enterprise Logistics Management System
EM	Enterprise Management Directorate
ESS	Electronic Security Systems
FAR	Federal Acquisition Regulation
FASC-N	Federal Agency Smart Card Numbers
FFT	Future Fibre Technologies
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FTE	Full Time Employee
GAT	Government Acceptance Testing
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFM	Government Furnished Meals
GIS	Geographic Information System
GPC	Government Purchase Card
GUI	Graphical User Interface
GUID	Global Unique ID
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSPD	Homeland Security Presidential Directive
HSS	High Security Switches
IAVA	Information Assurance Vulnerability Alert
ICAM	Identity, Credential, and Access Management
ICD	Intelligence Community Directive
IDS	Intrusion Detection System
IED	Improvised Explosive Devices
IMESA	Identity Management Engine for Security and Analysis
IMMS	Inventory and Maintenance Management System
IPR	In-Progress Review
ISC	Interagency Security Committee
ISSC	Integrated Security Services Contract
IT	Information Technology
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
JSP	Joint Service Provider

KO	Contracting Officer
KO	Contracting Officer
LAN	Local Area Network
LCAT	Labor Category
LCR	Lifecycle Replacement
LiDAR	Light Detection and Ranging
LKM	Lockmasters Pedestrian Door Lock
LPR	License Plate Recognition
LPRPE	LPR for Parking Enforcement
LSB	Life Safety Backbone
MILAIR	Military Airlift
MMS	Maintenance Management System
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MWR	Morale, Welfare, and Recreation
NCCS	National Industrial Security Program (NISP) Contracts Classification System
NCR	National Capital Region
NIPR	Non-classified Internet Protocol Router
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OEM	Original Equipment Manufacturer
OGA	Other Government Agency
OGC	Office of General Counsel
OS	Operating System
OSW	Office of the Secretary of War
PA	Public Affairs
PACS	Physical Access Control System
PCU	Premise Control Unit
PDF	Portable Document Format
PFAC	Pentagon Facilities Access Card
PFPA	Pentagon Force Protection Agency
PIN	Personal Identification Number
PIPO	Phase In/Phase Out
PIV	Personal Identification Verification
PM	Program Manager / Preventative Maintenance
PMP	Privilege Management Program
PMR	Program Monthly Review
POAM	Plan of Action and Milestones
POC	Point of Contact
PoE	Power-over-Ethernet

PPD	Pentagon Police Department
PPSM	Ports, Protocols, and Services Management
PRS	Performance Requirements Summary
PSIM	Physical Security Information Management
PTZ	Pan-Tilt-Zoom
PVT	Performance Verification Test
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
RMS	Records Management System
RRMC	Raven Rock Mountain Complex
RSA	Rivest-Shamir-Adleman (cryptography algorithm)
SCC	Security Control Center
SCI	Sensitive Compartmented Information
SDD	System Design Document
SDK	Software Development Kit
SLA	Service Level Agreement
SLA	Service Level Agreement
SMA	Service Maintenance Agreement
SOFA	Status of Forces Agreement
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publication
SPOT	Synchronized Predeployment Operational Tracker
SQL	Structured Query Language
STA	Secure Technology Alliance
STIG	Security Technical Implementation Guide
SVSS	Under Vehicle Surveillance System
TAK	Team Awareness Kit
TDY	Temporary Duty Travel
TE	Technical Exhibit
TI	Technology Industries
TMA	Tenant Managed Access
TO	Task Order
TPOC	Technical Point of Contact
TS	Top Secret
TSI	Technical Solution Identification
UFC	Unified Facilities Criteria
UL	Underwriters Laboratories
UVSS	Under Vehicle Surveillance System
VACP	Vehicle Access Control Point

VCA	Video Content Analysis
VMS	Video Management System
VSS	Video Surveillance System
WHS	Washington Headquarters Services
ACS	Access Control System
ACOR	Alternate Contracting Officer Representative
AMAG	American Magnetics
ANSI/EIA	American National Standards Institute/ Electronic Industries Alliance
CFR	Code of Federal Regulations
COTS	Commercial off the Shelf
CO	Contracting Office
KO	Contracting Officer
COR	Contracting Officer Representative
DHHQ	Defense Health Headquarters
DoD	Department of Defense
ESS	Electronic Security System
GSA	General Services Administration
GFE	Government Furnished Equipment
GFI	Government Furnished Information
IDIQ	Indefinite Delivery Indefinite Quantity
ISSC	Integrated Security Services Contract
NCR	National Capital Region
OS	Operating System
OGA	Other Government Agencies
OGC	Other Government Contractors
PFPA	Pentagon Force Protection Agency
PWS	Performance Work Statement
POP	Period of Performance
QA	Quality Assurance
QC	Quality Control
RRMC	Raven Rock Mountain Complex
SCI	Secure Compartmentalized Information
SSD	Security Services Directorate
TS	Top Secret
WHS	Washington Headquarters Service

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED PROPERTY (GFP) AND SERVICES:

3.1. SERVICES: The Government will provide services and support when necessary for all installation projects. The Government will also provide available drawings for facilities and office spaces.

3.2. FACILITIES: The Government will provide limited office space. Office space will be limited to the access control center and security control center. The Government cannot guarantee office or storage space for technicians, key personnel or administrative personnel.

3.3. MATERIALS: The Government will provide the Standard Operating Procedures (SOP) for the Access Control Center. If GFP is provided, the Government will notify the contractor at the task order level. Contractor will provide all other materials for installation task orders as outlined in individual task orders.

3.4. PARKING: The Government shall provide the Contractor with limited parking at the Pentagon Reservation, Mark Center, and Raven Rock Mountain Complex on a space available basis. There is no Government provided parking at leased facilities. Parking is limited on the Pentagon reservation and restricted to only company labeled vehicles. The Contractor shall be fully responsible for procuring parking at all locations to perform work required under this Contract.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1. GENERAL: The Contractor shall furnish all supplies, equipment, facilities and services required to perform task orders under this contract that are not listed under Section 3 of this PWS.

4.2. TOP SECRET FACILITY CLEARANCE: The contractor shall possess and maintain a TOP SECRET facility clearance from the Defense Security Service. The DD254 is provided as Attachment 13 with the solicitation. Specific security requirements will be identified at the task order level.

4.3. MATERIAL: The Contractor shall provide, maintain, and be fully accountable for all tools necessary to safely and effectively perform the services required in this contract. The contractor will also provide all necessary safety equipment (glasses, hearing and head and foot protection) for use onsite.

4.4. EQUIPMENT: The Contractor shall provide lifts, ladders and any equipment needed to perform the tasks described in this PWS. Some work is performed on roofs, light posts, in confined areas and other locations in multiple Government facilities.

4.5 UTILITIES: The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

4.6 SERVICES: The Contractor will provide project leads, for all installation projects and personnel supporting task orders. The Contractor will also maintain and update available drawings for facilities and office spaces

PART 5
SPECIFIC TASKS

5. SPECIFIC TASKS:

5.1. BASIC SERVICES: The contractor shall provide services for this contract at the task order level. Each task order will have a PWS describing all the requirements for materials, installation, or support for security of the Pentagon or other PFPA supported facility.

The work to be performed on ISSC is divided into five major categories, which are:

a) System Support: The Contractor shall be responsible for sustainment support of electronic security systems. This support includes system monitoring, troubleshooting, patching and software updates, configuration, and administration.

b) Logistics: The Contractor shall be responsible for procuring, storing, and inventory of materials and supplies to deliver services under this contract.

c) Repair: The Contractor shall be responsible for responding to and repairing damaged, malfunctioning, or inoperable systems and their components as described in this PWS as well as any components installed during this contract unless specified in the individual task order PWS.

d) Maintenance: The Contractor shall be responsible for performing periodic preventative maintenance on all electronic and physical security systems identified in this Performance Work Statement (PWS) as well as any components installed during this contract unless specified in the individual task order PWS. Periodic preventative maintenance shall be performed at minimum in accordance with manufacturer recommendations and may require additional preventative maintenance work due to amount of use or ambient conditions. This includes patching on hardware, as well as ensuring systems, hardware, and applications are up to date.

e) Installation and Hardware: The Contractor shall be responsible for the complete requirement analysis, system engineering, detailed design development, programming, configuration, integration, shipment, installation, and testing of systems as outlined in future TOs.

- The Contractor shall provide a qualified team of installation professionals with the necessary experience to install equipment properly while having minimal effect on the day-to-day operations responsibilities outlined in preventative maintenance, repair, system support, and logistics sections of this PWS.
- All engineers and technicians working on ISSC systems shall have certification and training from OEM in their area of expertise. The Contractor shall provide best practices and adherence to applicable DoD regulation, industry standards, and local regulation on all installation efforts. Deviation from applicable regulations should be noted in TO proposals.
- Infrastructure installation should adhere to cabling standards ANSI-TIA-EIA 569-A, Unified Facilities Criteria (UFC) 3-580-01, and the Department of Army ITA Telecommunications Distribution Design Method SOP00385.
- The contractor shall propose solutions in compliance with the Pentagon Exterior Standards Manual (PESM). Deviation from PESM shall be approved in writing by Government.
- Installation TO's shall be designed and implemented in accordance with all applicable DoD regulations to include, but not limited to, the Office of the Director of National Intelligence, Intelligence Community Directives (ICD) 503, 705.1, DOD 5100.76M - Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E), and ICD 705.2, Protecting Sensitive Compartmented Information within Information Systems; DoD Manual, 5205.13, Defense

Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) Program Security Classification Manual; DoD Manual 5220.22M, National Industrial Security Program Operating Manual (NISPOM); DoD Manual 5200.01, Information Security Program; and Office Secretary of Defense Supplement to DoD 5200.1R.

- Contractor shall provide a performance verification testing plan for each TO that addresses the performance characteristics identified in section 5.5. This plan shall include a burn-in period of no less than 30 calendar days to demonstrate system performance through operational testing and include a testing checklist for Contractor completion and government validation. Procedures shall explain in detail, step-by-step actions and expected results, demonstrating compliance with the requirements specified.
- The Contractor shall complete installation of new systems or integrations between the existing systems and other ESS as part of individual TOs. The Contractor shall be responsible for the full lifecycle systems engineering process for these integrations, including requirements elicitation and analysis, detailed design, development, testing, integration, end user training, operationalization and go-live, and sustainment for all systems and sub-systems in this contract.

- Task Orders will be noted and awarded as either a Capital Improvement or Non-Capital Improvement:
    - Capital Improvement (This is a subcategory of Installation for accounting purposes): Capital improvements to general equipment must be noted and awarded as such when a task order performs the following: (1) the improvement increases the asset's useful life by two or more years, or increases the assets capability, or increases its capacity or size, and (2) the cost of the improvement equals or exceeds the capitalization threshold ($250K).
    - Non-Capital Improvement: These will be more common than the capital improvement projects. This includes projects or hardware that do not meet the capital improvement projects.

5.2. Task Order (TO) Management:

- The Contractor shall manage all issued TO as outlined in contract requirements. The Installation Manager shall serve as the focal point for all TOs and PoP Management.
- The Contractor shall maintain comprehensive tracking tools to manage TO schedules and to identify Government or Contractor delays to the critical path in advance, along with recommendations/options to mitigate delay in overall project schedule. Examples of these delays include, but are not limited to, network or electrical infrastructure, permits, material procurement, or construction delays.
- The Contractor shall provide appropriate staffing to address assigned task orders within the PoP defined on each TO. The Contractor shall identify when TOs may overlap, are duplicative, or conflicting and request clarification by the Government as part of proposal response.
- The Contractor shall insure that all equipment, configurations, and as-built drawings for the installation are loaded in the Maintenance Management System.

5.2. Proposal Response to TOs:

- The Contractor shall provide a comprehensive proposal identifying the Contractor’s approach and solution.
    - The Contractor shall identify how their proposal was shaped by specific Government’s PWS items and the Contractor’s assumptions.
    - Unless stated otherwise at the task order level, the Contractor shall provide detailed design of a proposed product and/or solutions. The design may include detailed drawing of solution overview, architecture, interconnect, elevation, The drawings shall be created in a computer aided design (CAD) software and file format shall be a DWG format. For each

TO, unless otherwise specified, the Contractor shall submit 30% with the proposal and later provide 60%, 90% and as-built drawings as deliverables.
    - The Contractor shall include detailed costs for prime and sub-contractor labor hours and categories, materials, other costs.
    - The Contractor is encouraged to identify trade space that may provide quantifiable improvements in cost, schedule, or performance.
    - Contractor will provide labor hours labor category responsibilities will be to complete the task order, and the role of the personnel in that labor category
- The Contractor shall return proposals within the below response times.
    - Routine Proposals: Returned within three (3) business days.
    - Surge or Emergency Proposals: Returned within one (1) business day.
    - Complex Proposals, such as those involving extensive amounts of integration, construction, multiple stakeholders, or new systems shall be returned within seven (7) business days.
    - Deviations from outlined proposal response times should be requested in writing to Government and are subject to approval.
- Proposal responses shall include site survey data including sketches, photographs, survey sheets, and annotated site drawings. The responses shall include details about the current site conditions as well as conditions/considerations that may impact ability of proposed system performance or schedule for consideration by government.
- For complex projects, joint scoping sessions may be requested.

5.4 Technical Design Packages: For complex system designs not yet developed, the Government may request as a TO, a Technical Design Package (TDP) that details complete system, design, installation approach, testing, and full lifecycle costs for installation and sustainment. Specific Technical Design Package requirements will be defined on an individual TO basis.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)

6.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. This includes but is not limited to ICD 705, DoD 52001.01 Volume 3, and DoD 5100.76.

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING

7. ATTACHMENT/TECHNICAL EXHIBIT LIST:

7.1 Technical Exhibit 1 – Performance Requirements Summary

7.2 Technical Exhibit 2 – Deliverable Schedule

TECHNICAL EXHIBIT 1
PERFORMANCE REQUIREMENTS SUMMARY

7.1 Performance Requirements Summary

Performance Requirements Summary will vary by task order and will be defined in specific task orders.

TECHNICAL EXHIBIT 2
DELIVERABLE SCHEDULE

7.2 Deliverable Schedule

Additional deliverables may be identified and defined in specific task orders.

All deliverables shall be submitted using Microsoft Office suite of tools (for example, MS Word, MS Excel, MS PowerPoint), or Adobe PDF format, unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR.

The COR has the right to reject or require correction of any deficiencies found in the deliverables. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection.

The following table specifies the deliverables for this requirement. The Contractor is expected to adhere to the due dates for reference item. However, schedules for reference items become dependent on a number of factors beyond the Contractor's control including, but not limited to; force protection constraints, accessibility to Command locations, and availability of key stakeholders. The Contractor shall account for external schedule complications and will adjust staffing, billing and due dates of deliverables accordingly. Delays in scheduling should not influence the labor hours required to complete a comprehensive strategic evaluation. Before any reimbursable expenses (i.e., travel costs) are incurred by the Contractor as a result of schedule delays shall be reimbursed by the government, provided all reimbursable expenses were previously approved and COR is notified of any increased costs due to external scheduling delays.

Para Reference	**Deliverable**	**Frequency**	**# of Copies**	**Medium/Format**	**Submit To**
	Executive Compensation FAR Clause 52.204-10	Annually, NLT 5 business days following the Contractor's submission to the FFATA Sub-Award Reporting System (FSRS)	1 original	PDF	KO & COR
1.17	Small Business Participation Reporting	Semi-annually, congruent with the subcontracting reporting periods.	1	Electronically (spreadsheet or PDF)	KO & COR & Small Business Professional

TECHNICAL EXHIBIT 3

ESTIMATED WORKLOAD DATA

Firm-Fixed-Price Contracts: Technical Exhibit 3 provides estimated data for completing the Performance Work Statement (PWS) requirements. The Contractor is responsible for determining appropriate staffing levels using sound judgment and business practices to meet all PWS requirements. This will be based on the task orders issues under this ISIQ

CLIN #	**Labor Category**	**Key or Non-Key Personnel**	**PWS Task reference(s)**	**Estimated Hours**	**FTEs**
CLIN TBD	Program and Project Leads	TBD based on Task Order	PWS Part 5	37,440	20
CLIN TBD	System Admins and Technical Points of Contact for Systems/Applications	Non-Key Personnel	PWS Part 5	56,250	30
CLIN TBD	Maintenance and Repair Technicians	Non-Key Personnel	PWS Part 5	37,440	20
CLIN TBD	Installation Leads and	Non-Key Personnel	PWS Part 5	56,250	30
CLIN TBD	Project and Support Personnel	Non-Key Personnel	PWS Part 5	74,880	40