ADAP TEMPLATE 211-002 PERFORMANCE WORK STATEMENT (PWS)

INTEGRATED SECURITY SERVICES CONTRACT (ISSC)

Task Order 1

PART 1
GENERAL INFORMATION

1.1 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. The Pentagon Force Protection Agency (PFPA) Integrated Security Services Contract (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 leased facilities in the National Capital Region (NCR), and Raven Rock Mountain Complex (RRMC) in Adams County, PA and Washington County, MD.

1.2 DESCRIPTION OF SERVICES:

The Contractor shall provide Integrated Security Services as defined in this PWS except for those items specified as government furnished property and services. The Contractor shall perform to the standards in this contract.

1.3 BACKGROUND:

Previous contracts for this requirement, awarded in 2007, 2012, 2017, and 2021 provided comprehensive security integrator services to PFPA. Since inception, contract scope has expanded to include additional facilities, new systems, and increased security capabilities.

1.4 OBJECTIVES:

The primary objective is to ensure the Pentagon Force Protection Agency's (PFPA) security systems are robust, reliable, scalable, compliant, and continuously available to support the critical security operations of multiple Security Operations Centers. The Contractor shall provide all necessary services to design, implement, and maintain these systems and applications in a manner that is high-performing, user-centric, and cost-effective, while strictly adhering to all contractual requirements

These systems covered by this PWS shall be designed, implemented, and maintained to meet the following critical characteristics:

Resilience: The system must be capable of withstanding and recovering from disruptions, whether accidental or malicious. This includes built-in redundancies and failover mechanisms to ensure operational continuity.

Availability: The ESS shall achieve a minimum of 99.9% operational uptime, outside of scheduled maintenance windows. The system must be accessible and fully functional to support 24/7 security operations.

Reliability: The system shall perform its specified functions consistently and without failure under stated conditions for specified periods. All components must meet or exceed industry standards for reliability and mean time between failures (MTBF).

Scalability: The ESS architecture must be scalable to accommodate future growth in the number of users, facilities, connected devices, and data volume without degradation in performance. The design should allow for seamless expansion of capacity and functionality.

Interoperability: The system must be fully interoperable with all designated PFPA legacy and future systems, as well as with external partner systems as required. It shall adhere to open standards and protocols to facilitate seamless data exchange. The Contractor is expected to keep abreast of changes to existing integrations and connectors that all involved vendors within that integration.

Affordability: The total cost of ownership, including acquisition, implementation, maintenance, and support, shall be managed to provide the best value to the government. The Contractor shall proactively identify and propose cost-saving measures throughout the period of performance.

1.5 SCOPE: The ISSC consists of four main capabilities: Electronic Security systems, Physical Security, Passive and Active Barriers, and Mission Applications. Systems and services under each capability include but not limited to the following:

a) Electronic security systems - access control; intrusion detection; video surveillance; networked video recorder and intelligent video analytics; physical security information management (PSIM); license plate recognition (LPR); gunshot detection; under vehicle inspection; identity, credential, and access management (ICAM); mass notification; biometric and multi-modal authentication; computer aided dispatch and other law enforcement mission applications; chemical, biological, radiological detection and mitigation; operations center collaboration visualization systems; LiDAR.

b) Physical security, personnel, vehicle, cargo, and parcel screening systems; passive and active barriers, turnstiles, fencing, bollards, gates, traffic control; ballistic rated glass, booths, kiosks, and mobile shields; blast-resistant waste receptacles, doors (sound-rated and force protection), window film, locks, and door hardware. Software applications in support of Electronic Security, Physical Security, Law Enforcement, and Emergency Management.

c) Infrastructure supporting the above systems, software configuration, custom code, cabling for electrical and information technology; trenching, grading, utilities, conduit placement, and other civil types of work. For TO1, Contractor shall be responsible for

maintaining the infrastructure of existing systems. However, new installations will be addressed at the task order level.

To successfully execute these requirements, the Contractor shall provide personnel possessing demonstrated subject matter expertise in the following areas:

- Electronic Security Systems (ESS): In-depth knowledge of access control, intrusion detection, video surveillance (CCTV), and other related electronic security technologies and the nuances of the various vendors and platforms, with knowledge on the integration of these technologies with each other and those within the other areas listed.
- Physical Security Systems: Expertise in the principles and application of physical security measures, including barriers, locks, and lighting, and their integration with electronic systems.
- Mission Support Systems: Understanding of the ancillary systems that support the primary security mission, ensuring their proper integration and operation.
- Command and Control (C2) Systems: Expertise in C2 platforms and situational awareness tools used to monitor, manage, and respond to security events, including their integration with underlying ESS.
- 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.
- 3rd 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.
- Preventative Maintenance: The Contractor shall be responsible for performing periodic preventative maintenance on all electronic and physical security systems identified in this PWS as well as any components installed during this contract. An estimated amount of components installed per year is included in Appendix- A Table 15. 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. Preventative maintenance will be performed on the assets described in Appendix for Systems and Device Counts and Attachment 1b5 Task Order 1 Appendix D, as well as assets installed under other task orders under this IDIQ.

- 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. This includes assets described in Appendix for Systems and Device Counts and Attachment 1b5 Task Order 1 Appendix D.
- Logistics Management: The Contractor shall be responsible for procuring, storing, and inventory of materials and supplies to deliver services under this contract.
- Quality Management: The Contractor shall be responsible for tracking, baselining, and identifying deviations from ISSC and manufacturers standards for quality and performance.
- 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. Use of Artificial Intelligence in ESS and Physical Security systems
- Training: The Contractor shall be responsible for developing and maintaining training modules for all ISSC systems. The modules will include instructor's slides deck and end-user training manuals; the Contractor will provide initial and annual training to existing and new Government and Contractor personnel.

1.5.1 Engineering Support: The Contractor shall be responsible for the creation, modification, and maintenance of a complete and accurate library of all system documentation required to define, operate, maintain, and decommission the ESS. This documentation library is a critical Government asset and must be kept current and accessible to the Government and Contractor personnel throughout the period of performance. All documents shall be delivered in both a native editable format (e.g., Microsoft Word, Visio, AutoCAD) and a portable format (e.g., PDF). The Contractor shall perform the following engineering services throughout the system lifecycle:

- Requirements Analysis: Elicit, analyze, document, and manage system requirements from all stakeholders. Perform trade studies and analysis of alternatives to inform technical solutions.
- System Design & Development: Maintain detailed system designs, network architecture, and "as-built" documentation. Ensure designs adhere to all relevant DoD, Federal, and industry standards, including support for Task Order 2 cybersecurity and Zero Trust principles/requirements
- Continuous Testing and Evaluation: Develop and execute comprehensive test plans, including integration, stress, and user acceptance testing. Validate that all system patches and upgrades are fully tested in the ISSC Laboratory prior to production deployment.
- Configuration & Integration: Maintain configuration of all system components in

accordance with approved design specifications. Continually ensure integration of disparate systems to ensure seamless interoperability and data exchange as versions and upgrades occur

Deliverables: (these documents shall be maintained and available on NIPR and the MMS throughout the length of the contract)

System Design Document (SDD) - A comprehensive document that details the system's architecture and design. It describes how the system will meet the requirements. It includes hardware/software selections, detailed network diagrams, data flow diagrams, system interfaces, and security architecture. The primary blueprint for building the system and the foundational document for planning future upgrades.

As-Built Drawings - The definitive record of the final, installed state of the system, including physical locations, cable pathways, network connections, and power distribution. Essential for troubleshooting physical connectivity, performing maintenance, and understanding the real-world layout.

System Administrator's Guide - A detailed technical manual for system administrators. It covers advanced configuration, system backup and recovery procedures, user account management, performance monitoring, and advanced troubleshooting. The primary "how-to" guide for the technical staff responsible for the day-to-day health and maintenance of the system's backend.

Standard Operating Procedures (SOPs) / Operator's Manual - A user-focused manual detailing the step-by-step procedures for performing all day-to-day operational tasks (e.g., acknowledging alarms, generating reports, reviewing video). This document is the basis for the end-user training curriculum. The primary guide for the security operators who use the system 24/7 to perform their mission. Ensures consistent and correct actions.

Decommissioning Plan - A plan that details the procedures for the orderly retirement of a system at the end of its life. It must include steps for data sanitization and archival in accordance with DoD standards, and the proper disposal or turn-in of all hardware components. Ensures that systems are disposed of securely and that no sensitive data is compromised during the retirement process.

1.5.2 System Status: The Contractor shall provide a comprehensive monthly report detailing the status and progress of all systems under its purview. This report shall be delivered to the designated Government representative. At a minimum, the report shall include:

- Lifecycle Progress: An executive summary of all significant lifecycle activities, milestones achieved, and any variances from the project plan for each major system.

- System Health and Status**:** A detailed assessment of the operational health, availability, and performance of each production ESS, including any identified deficiencies or risks

- Sustainment Activities**:** A summary of all preventive and corrective maintenance activities performed, progress against sustainment plans, and an overview of ticket and service request trends.

- Actionable Next Steps: A clear outline of all outstanding tasks, planned activities for the upcoming reporting period, and any required Government decisions or actions

Deliverables:
System Lifecycle Report – *Due monthly after contract award.*

Lifecycle Replacement Plan – *Due annually as an overview of systems, expected end of life and estimated cost*

1.5.3 Configuration Management: The Contractor shall establish and maintain a robust Configuration Management (CM) process for all hardware, software, and documentation associated with the ESS. The Contractor shall develop, maintain, and execute a Configuration Management Plan (CMP) that details the processes for:

- Configuration Control: A formal process for proposing, evaluating, approving, and implementing changes to the established baseline. This includes the role of a Configuration Control Board (CCB).
- Configuration Status Accounting: Recording and reporting the status of CIs and change requests.
- Configuration Audits: Conducting formal audits to verify that the system configuration matches the documentation.
- Configuration and Coordination with Task Order 2 requirements to ensure alignment between application and infrastructure

1.5.4 Firmware and Software Management: Within 60 days of award, the Contractor will provide an initial Application Version Report to establish a starting baseline for ISSC5 TO1 that details:

- The current software versions for the applications listed in Section 5.2 and the Systems and Device Count Appendix sheet, as well as any other applications in this document.
- For each of the responsible vendors of the applications listed, provide the most current versions available of the respective software at the time of award. Include compatibility and any hardware or operating system constraints, if not compatible.
- Any software listed will show the associated end-of-support date by the responsible vendor, if applicable. The Contractor will provide the Government an upgrade plan to the most current vendor offering for all applications.
- For each of the applications listed in this PWS, provide details on the most current versions of supporting software, operating systems, and databases. Include compatibility and any hardware or operating system constraints, if not compatible.

- Any supporting software/application listed will show the associated end-of-support date by the responsible vendor, if applicable.

Deliverable:
Configuration Management Plan – *Due 60 days after contract award.*
Application Version Report - *Due 60 days after contract award, updated annually*

1.5.5 System Support: The Contractor shall provide baseline system administration support of all systems. System support shall include the following services:

System Monitoring: The Contractor shall be responsible for continuous monitoring and oversight of ESS. The Contractor shall establish an automated, continuous method to electronically track the status of ISSC systems, devices, and end points and record statistics on uptime and availability. The Contractor shall provide monthly reports on system and endpoint uptime and reliability. The Contractor shall report to the Government unplanned infrastructure, network, power, or ISSC system interruptions that impact or degrade ISSC Systems. The Contractor shall fully participate in planned and unplanned network outages, including participation in outage teleconferences, on-site coverage, response, remediation to restore systems to pre-outage conditions, and after-action reports on outages. The Contractor shall maintain an active database of equipment across the enterprise to include all devices and their associated location information (address, suite, door(s)), security managers and lessor contact information (where applicable) when made available to PFPA for ISSC use. The Contractor shall integrate this information with geo-spatial databases to ensure consistent records and information for both installation and maintenance.

Contractor shall provide database information within 48 hours of request and shall provide database access to the Contracting Officer (KO), Contracting Officer Representative (COR) and COR-approved personnel for use in more frequent/tailored data queries.

Software Updates: The Contractor shall receive and apply all software and firmware updates as they are released by the vendor. Further detail on this Contractor responsibility is located in Section 1.5.3 and 1.5.4.

Configuration Changes: The Contractor shall perform configuration changes to ISSC systems upon Government approval. These configuration changes include, but are not limited to, changing alarm priorities, schedules, parameters; system and device attributes, rule sets, camera home positions, reader group changes; PSIM response workflow adjustments; add, change, and remove ISSC system users; and documenting all system configuration activities. The Contractor shall perform configuration changes within two (2) business days of the approval. Any situations where the configuration changes that cannot be performed within two (2) business days, the Contractor shall provide to the requestor and the COR a written explanation as to the reason and the estimated date of completion. The Contractor shall record all configuration changes for each system in a database.

Reports: The Contractor shall provide to the Government both periodic and ad hoc reports from all ISSC systems. These reports include, but are not limited to, alarm activity; time to acknowledge and clear an alarm by an Operations Center; highest frequency alarms for a specified period; daily turnstile status reports; number of personnel passing through a specific card reader, reader group, entrance, or facility; reports on number of personnel granted access to a specific card reader, reader group, or facility; errors and failures; number, location, and type of outages and impairments; mean time to repair; and lists of sensors, devices, card readers, reader groups; summary of system configuration changes The Contractor shall provide these reports within one (1) business day of request.

Urgent more immediate reports will be submitted by the COR for only emergency situations.

Security Control Center (SCC)
The Contractor shall provide 24/7 on-site support services, referred to as the SCC, serving as the focal point for security systems health monitoring, preemptive identification of system failures and degradations, technical support and inquiries, repair coordination and dispatch of technicians, making system configuration changes, system administration, nuisance alarm reduction, system support as described above, and receiving customer service requests.

Key Personnel: Operations Manager

Staffing: No less than two (2) system administrators will be present and on-site with the capabilities of performing at least Tier 2 level of support (see Tier Support definition) explicit to operations and maintenance. The Contractor will staff appropriate to the operational tempo of the ongoing mission, e.g., recalling additional administrators to support an ongoing system outage while also still being able to execute scheduled outages for STIG remediation and patching, or adding administrators to support Task Orders outside of TO1 "base" requirements.

Location: the SCC will operate from the Pentagon, Room 4B556, comprising of nine (9) seats with both NIPR and LSB workstations. 4B556 will be the primary location of the SCC. A secondary location comprising of two (2) hotseats, will also be provided at the Suffolk Building, 6th Floor, to support building-wide power or network events, or to support Tiers 3 and 4 level troubleshooting with vendor representatives.

Operating Hours: The SCC shall be manned on-site, staffed 24 hours per day, 365 days per year, including Government holidays and during Government closures, to include support during inclement weather and other closure-inducing incidents.

The SCC will be the focal point and the first line to issue outage notifications for the systems of ISSC responsibility.

Outage Definitions: there are three (3) types of notifications the SCC will publish to PFPA's stakeholders.

- **Scheduled Outage:** These are recurring outages that are planned at least one (1) calendar week in advance to the outage occurring.

Success of recurring outages is determined by zero-net changes or added capabilities to the security application being services.

Any unforeseen issues stemming from a scheduled outage will result in an Unscheduled Outage or Service Degradation.

- **Unscheduled Outage**: Non-scheduled outages that impact end users' ability to utilize PFPA's security systems in its full capacity, to include integration capabilities from sub-system to PSIM.

Large-scale impacts of significant portions servicing the Pentagon and Mark Center, e.g. the entirety of a Pentagon wedge, floor, or site like HRP or PSOC.

System-wide impacts of security applications at any PFPA-protected Delegated Facility, e.g. all cameras at One Liberty Center or inability for the Mark Center SOC to receive alarm notifications from the Suffolk Building.

Impacts to any "mission critical" camera or "VIP" access panel and associated readers, as defined by the Government.

- **Service Degradation:** Categorized as a partial impact regarding capability that does not fall within the definition of an "Unscheduled Outage."

Deliverables:
Turnover Log: SCC will conduct a turnover from shift to shift report to fully brief the incoming staff members that detail the following. Formatting and delivery of the turnover must be approved by the assigned Government oversight. Log will be kept on NIPR and readily accessible by the Government to quickly report the operational status of each system and any ongoing outages. (Daily)

Manpower Report: Identification staff members who are being relieved and who are assuming SCC duties, identifying locations of each person (Weekly)

System Operations Report: Operational status of each system, ongoing issues, and actions still needing to be taken in relation to ongoing outages. Report will be kept on NIPR and readily accessible by the Government to quickly report the operational status of each system and any ongoing outages (Daily)

Contacts of WHS FOSD or DISA J6 counterparts involved in troubleshooting (Maintain updated record)

List of Maintenance Management System (MMS) tickets that were worked on and what tickets were closed. (Maintain updated record)

List of Task Orders worked on and what actions were taken by SCC staff, e.g. programming access panels for PACS LCRs, cameras for VSS LCRs, Performance Verification Tests (PVTs) and Government Acceptance Testing (GATs). (Maintain updated record)

1.5.6 Information Technology, Network, and Cybersecurity: TO1 doesn't not provide the manpower to perform cybersecurity requirements, but system application leads are the technical points of contact (TPOC) for the Task Order 2 cybersecurity team, and support, PFPA and Defense Information Systems Agency (DISA) Joint Service Provider (JSP). DISA/JSP is responsible for the vast majority of IT delivery to PFPA, to include user accounts, cabling, switches, routers, virtual private networks, firewalls, cybersecurity service provider (CSSP) and defensive cyber operations (DCO), assessment and authorization and issuance of authority to operate (ATO), workstations, and workstation operating system and 3rd party non-ISSC application patching. JSP and higher level DoD information technology/cybersecurity organizations periodic cybersecurity compliance inspections are a key barometer by which ISSC quality is judged.

The Contractor is responsible for application level troubleshooting of ISSC software on servers and workstations. The list of network services is located in the Systems and Devices Appendix.

Cybersecurity Services: The Contractor shall support cybersecurity configuration, documentation, and software update support for all ISSC servers and security devices (e.g., PACS panels, cameras, etc.) in order to maintain their Authority to Operate (ATO).

These requirements are described in detail in Task Order 2, but personnel on this task order will support these requirements from a system/application standpoint.

ACTIVITY	DESCRIPTION	FREQUENCY/REQUIREMENT
Software Patching	Applying Microsoft Windows, Linux, Unix, and 3rd party software updates on ISSC servers in coordination with the IT Service Provider.	Applied IAW with CYBERCOM/JFHQDODIN/DISA specified orders or IAVA notifications prior to suspense date. The IT Service Provider performs vulnerability compliance scans of all services and network devices at least weekly.
Security Technical Implementation Guides (STIG)	Automatic and manual DISA STIG implementation and documentation for all servers and devices. These STIG remediations and documentation include the following at a minimum when they are on ISSC servers: • IIS and Web Server STIG • Application STIG • Microsoft SQL Server	Continuously maintained IAW individual STIG frequency.

	STIG • Redhat Server STIG	
Plans of Objectives and Milestones (or similar)	Narrative description of cybersecurity requirement, operational impact, cybersecurity risk, and plan/schedule for compliance	As needed to document required patch or STIG deviations for continued compliance/accreditation
Cybersecurity Documentation	• Ports, Protocols, and Services • Hardware/Software Lists • System Design Documentation • System Architecture • System Security Categorization • Privacy Impact Assessment • System Security Plan • Compelling body of evidence (e.g., screenshots, logs, scan results) that empirically demonstrate cybersecurity compliance	As needed for periodic cybersecurity compliance inspection and re- accreditation
Authority to Operate	Collection of STIG, POAM, and cybersecurity compliance documentation necessary for Authorizing Official approval	Every one to three years dependent on system type and accreditation ATO documentation shall be submitted at least 100 calendar days prior to ATO termination date

1.5.7 Technical Solutions Identification: At the request of the Government, the Contractor shall provide written technical solutions identification on up to 24 separate topics per contractual year. Technical solutions identification shall be aimed at improving system performance, reducing vulnerabilities, closing gaps associated with current security measures,

or identifying new or replacement materiel solutions. These technical solution identification submissions are typically in a 5-15 page white paper format that describes the issue/requirement and the proposed solution also provides a rough cost estimate for solution.

The Contractor may submit unsolicited technical solutions identifications based on their identification of emerging trends in the security industry or capability and performance gaps. If the Government accepts the Contractor's suggestions, the Contractor-initiated technical solutions identification shall count towards the 24 separate solutions required per year.

Deliverables:
TSI Documents

1.5.8 Lab Support: The Contractor shall establish, operate, and maintain a dedicated ISSC Laboratory environment within the National Capital Region (NCR) 20 miles radius from the Pentagon Reservation. This facility is critical for supporting the lifecycle management of the PFPA's ESS and shall be utilized for a range of activities, including, but not limited to:

Technology Evaluation: Assessing new and emerging security solutions and technologies to determine their suitability for the PFPA enterprise.

System Testing: Conducting comprehensive design, stress, integration, and regression testing for all ESS components and configurations.

Patch and Upgrade Validation: Rigorously testing all system patches, updates, and upgrades in a non-production environment before deployment to mitigate risks to the operational environment.

Diagnostics and Troubleshooting: Replicating and diagnosing issues identified in the production environment to develop and validate effective resolutions.

Software Pre-Installation Testing: Verifying the functionality and security of all OGC (Office of Government-wide Policy) software prior to installation.

Support Personnel: Lab Manager, who shall meet with the appropriate Government POC at least weekly to brief lab-related activities, to include a look ahead of scheduled activities. A copy of the brief and subsequent actions items resulting from the briefing shall be made available to the Government.

The Contractor will ensure only personnel supporting PFPA's ISSC will have both physical and logical access. If the software or hardware are co-located on appliances, virtual or physical, the Government must be aware and give explicit approval that is contingent on the Contractor demonstrating proper controls to maintain integrity of PFPA's systems and information.

The laboratory shall replicate the Government's production environment to the maximum extent feasible. This is to provide empirical evidence of system performance and to reduce the risk associated with changes, thereby ensuring the stability and integrity of the production environment.

At all times, the laboratory shall be in a ready state, where basic physical security systems' functions for PFPA's vendors can be accessed, configured, and used to replicate issues, test follow-on repairs, and establish remedies. For example, each of PFPA's PACS vendor's software, access panels, and reader hardware shall be operational and available to, not only emulate the endurance of the production system from being constantly online, but to ensure PFPA can demonstrate/confirm fundamental PACS' capabilities without delay and need for set-up or reconfiguration.

The Contractor is responsible for maintaining all laboratory facilities and systems under stringent physical and logical access controls to prevent unauthorized access and protect all Government-furnished and proprietary information.

Furthermore, the laboratory shall be made available to support Government-led training initiatives on modifications to existing ISSC Systems, as well as on associated maintenance and logistics software.

The Contractor shall ensure the ISSC laboratory network is secure and adheres to all applicable Department of Defense (DoD) and Joint Service Provider (JSP) information technology (IT) and cybersecurity standards and practices, including the implementation of a Zero Trust Architecture and robust Identity, Credential, and Access Management (ICAM) controls.

Deliverables:

- Access Report (Monthly) - A comprehensive list of all personnel provisioned with Physical Access Control System (PACS) privileges for the ISSC laboratory, a log of any individuals added to or removed from the PACS privilege list, a detailed access log of all individuals who entered the laboratory, including the date, time, and reason for access.

- Master ISSC Laboratory Schedule (Monthly) - An accurate and forward-looking schedule that captures all planned activities, appointments, tests, and maintenance projected for the next six (6) months. Any changes from the previous month's schedule shall be clearly highlighted and explained.

- Asset Inventory Report (Quarterly) - A detailed report that accurately documents all assets added to or removed from the laboratory, including hardware, software, and any other government-furnished equipment. The report shall reconcile with the master asset inventory.

1.5.9 Logistics:

1.5.9.1 The Contractor shall be responsible for all logistics and warehouse management services, including:

- GFE Transition and Receipt - During the contract transition-in period, the Contractor shall be solely responsible for the planning, coordination, and physical transfer of all GFE from the outgoing Contractor's facility to their new warehouse.

- Inventory Management - The Contractor shall perform all receiving, storing, issuing, and tracking of GFE and previously ordered spare parts inventory.

- Transportation - The Contractor shall provide all necessary transportation and personnel required to move parts and equipment between the warehouse, the ISSC Laboratory, and all operational sites at no cost to the Government.

- Obsolescence Management - The Contractor shall conduct an annual review of all GFE in the warehouse and provide a formal recommendation to the Government for the disposal or turn-in of obsolete, unserviceable, or excess

- Spare parts - The Contractor shall have spare parts necessary to meet response times for Tier 1,2, or 3 incidents. These assets shall be tracked in the inventory system

- Licenses - The Contractor shall track licenses and dates for license of systems and applications and maintain the data in the inventory system

1.5.9.2 ISSC Warehouse: The Contractor shall provide and operate a secure warehouse and logistics facility at no direct line-item cost to the Government. The primary objective of this facility is to store, manage, and account for all Government Furnished Equipment (GFE), project equipment ordered for installation, and spare parts required to support the maintenance and repair objectives of this contract. The facility shall be managed in a manner that ensures rapid access to inventory, maintains 100% accountability of Government property, and supports efficient logistical operations, to include ensuring entry into the Enterprise Logistics Management System (ELMS), as appropriate. Asset details shall be noted as to their location and status in the Maintenance Management System and provided as a monthly deliverable.

The facility shall be located within a radius that allows for ensuring material can be delivered to the Pentagon Reservation or other PFPA site to ensure timely transport of parts and equipment and meet Repair SLAs. It must be easily accessible for both standard and large delivery vehicles.

The facility must be equipped with, at a minimum: a monitored Intrusion Detection System (IDS), an Access Control System (ACS) that logs all entries, and a video surveillance system covering all ingress/egress points and storage areas. Access shall be restricted to authorized personnel only.

The facility must have sufficient square footage to properly store the initial GFE transfer and accommodate future inventory fluctuations. It must also be able to support storage of equipment as it is prepared for DRMO. It must be organized with appropriate shelving and clear labeling to facilitate efficient inventory management and retrieval.

Deliverables:

Monthly Inventory Report (Monthly) - A comprehensive report generated from the IMMS detailing all GFE and Contractor-owned critical spare parts. The report must include quantities on hand, recent additions, recent issuances, and current status of all items.

Annual Obsolescence Report (Annually) - A formal report listing all GFE recommended for disposal or turn-in, including the rationale for each recommendation (e.g., obsolescence, non-repairable).

1.5.9.3 Maintenance Management System (MMS): The Contractor shall provide a commercial off-the-shelf (COTS) MMS. The MMS shall consist of a web based front end and a structured query language database that shall be able to download and upload to similar management systems.

The MMS shall capture the following data for all systems and their sub-components under ISSC. The Contractor shall be responsible for assuring the below data is captured and updated within three (3) business days following any procurement, testing, installation, preventative maintenance, configuration change, or repair activity. The Contractor shall adhere to government requirements, guidance, and industry best practices to ensure secure connectivity and storage of the sensitive data contained in the MMS.

Device type
ISSC details:
ISSC barcode number
Project procured under
Projects under which the device was moved, adjusted, or removed.
Manufacturer details:
Manufacturer
Device model
Value of component
Manufacturer serial number

Date of manufacture
Useful life
DPAS/ELMS Serial Number assigned to the asset by facility and type
Predicted end of service date
Device location:
Building or storage site/Floor/Suite or room number
Geospatial coordinates
DPAS/ELMS Serial Number
Pertinent configuration details, including but not limited to:
Software or firmware version
Device logical naming
Alarm priority
Parent and child device physical and logical connections
Device specific configuration parameters, such as home position
Licensing, warranty, service, and support agreement information, including terms and expiration and renewal dates
A complete cradle to grave chronological history of:
Device procurement, warehousing, pre-installation testing, installation, and placement in service

Preventative maintenance schedule and activities, history of preventive maintenances (PMs), and date of next scheduled PM
Break-fix repair history and corrective measures
System patch / hot-fix history
Time down and time returned to service per incident
Configuration changes
Removal, relocation, decommissioning, and final disposal
Editable field for Quality Assurance that can be queried

The MMS web based front end shall allow for the following capabilities for the Contractor and authorized Government personnel to:

Submitting repair tickets and getting ticket status
Tracking repair ticket lifecycle
Searching for a device by salient characteristic above
Printing standard reports for system metrics
Natural language, free form database querying
Export all or portions of the database in a file format compatible with Defense Property Accountability System/ELMS to enable effective audit readiness

The Contractor shall provide training on the Contractor's MMS solution to Government personnel.

Note: Government MMS. During the life of this contract the Government plans to transition from a Contractor owned and provided MMS to a Government owned and provided MMS. This Government MMS will satisfy all the features and requirements described through a commercial, CAC-required, DoD accredited, software-as-a-service offering. The Contractor shall transition all data and operations from the Contractor MMS to the Government MMS in accordance with the requirements described in and priced via Sample Task Order 1.

After transition the Government MMS shall become the official system of record for all contractual SLAs, tasks, and performance requirements under this contract. All reports to the Government shall be via export from the Government MMS. The Contractor shall be afforded administrator permissions within the Government MMS to configure workflows and other relevant options to satisfy the requirements of this contract.

1.5.9.4 Replacement and Spare Parts Equipment: The Contractor shall maintain a sufficient bench stock of spare parts and replacement components for equipment on the program to ensure quick reaction to emergencies and to ensure timely repairs are made to all the equipment on the program, as well as being able to fulfill service requests within contractual requirements. The Contractor shall submit a monthly report documenting spare and replacement part usage and inventory status. The report shall include at minimum the following:

a. Spare parts used in the previous month
b. Reason for the spare part use
c. Location where the spare part was deployed
d. Most up-to-date spare parts inventory
e. List of spare parts that need to be procured to maintain the inventory

The parts and supply inventory/bench stock shall be maintained in the Contractor's warehouse and procured by the Contractor as inventory gets below a level that allows the Contractor to meet repair time objectives specified in the PWS in Section 1.4.6.1. The determination of frequency of failure is based on the individual component, but shall be replaced if failing at least three times in a one-month period. This equipment and the maintenance plan shall be kept in the MMS. A list of these parts and equipment will be provided to the COR team on a monthly basis.

1.5.10 Repair: Should an application, system, subsystem, or end-point supported under this contract become inoperable or degraded, the Contractor is required to respond per the requirements detailed in this section. These repairs shall include repair and replacement batteries, card readers, cameras, turnstiles, and other end-point devices, as well as troubleshooting and resolution of software issues. The Contractor shall provide all required equipment to perform repairs, including but not limited to service lifts, specialized tools, and any other equipment needed to maintain and service all electronic security systems under ISSC. The Contractor may be required to coordinate with OGAs, OGCs, subcontractors, or internal resources to troubleshoot and resolve the issue(s).

Upon discovery of a system outage or degradation, the Contractor shall immediately, but not longer than one hour, notify the Government COR team, the Government system owner, and PFPA Operations Centers of system impact via e-mail and or phone, along with measures being taken to remedy.

After action reporting for system outages are required within 24 hours of identifying or troubleshooting the root cause of system issues and shall provide all-inclusive details of the event, to include, but not limited time, date, actions taken, root cause, next steps, and lessons learned, as well as other pertinent information.

Quality Control (QC) and Repair teams shall ensure system and environment data is accurate and updated. Deficiencies found during preventative maintenance shall be repaired.

The Contractor shall submit a monthly summary report of all repair activities performed, ESS Outages or Degradations and QC activities for the previous month and yearly trend analysis. The reports shall at minimum include:

Repair
1. Number of repairs performed
2. Repair types
3. Average time to complete the repairs
4. Longest time to complete the repairs
5. Observed trend analysis

Outages and Degradations
1. Number of outages or degradations
2. Outage/Degradation type
3. Average duration
4. Longest duration
5. Observed trend analysis

QC:
1. Total number of QC performed
2. System/Device/Sensor/Service that QC was performed on
3. Date and Location
4. QC findings/results

1.5.10.1 Response to Service Calls: The Contractor shall meet the following response and repair time objectives.

Tier 1 severity service calls reflect ongoing disruption to PFPA's core law enforcement, security, and force protection mission.

Table 1: Service Level Agreements

TIER 1 SEVERITY SERVICE DEGRADATION CRITERIA		
System	**SERVICE DEGRADATION**	**THRESHOLD**
Video Surveillance System	Outage	10% of live view inaccessible per each site
	Mission Critical	Any mission critical cameras and/or recordings not viewable
	Recording Availability	10% of cameras not recording per each site
	System Degradation	10% of cameras have diminished quality of video per each site
Perimeter Intrusion Detection System	Outage	Detections are reported as alarms, systems inaccessible
Perimeter Intrusion Detection System	Degradation	Detections reported are delayed by more than 5 seconds from the incident.
Physical Access Control Systems	Outage	Application or facility wide outage lasting more than 1 minute
Physical Access Control Systems	Degradation	Backup or delays in reporting or download of data lasting more than 5 minutes
Physical Security Information	Outage	Application or facility wide outage lasting more than

Management (PSIM) System		1 minute
Physical Security Information Management (PSIM) System	Degradation	Backup or delays in reporting or download of data lasting more than 5 minutes
Emergency Call Box	Outage	Device failure to communicate or operate as designed
VACP Under Vehicle Surveillance Systems and License Plate Readers	Outage	Any UVSS or LPR at the VACP's not viewing undercarriages or receiving license plate reads.
Caliber CAD	Degradation	System in DO for more than 20 minutes
Caliber CAD	Degradation	Other system capability is not working correctly for multiple users
Caliber CAD	Outage	Users can not access
LPR	Outage	Camera is not functioning or recognizing reader
Turnstile	Outage	More than 20% of the turnstiles at that specific entract is down for more than 30 minutes
Duress or Lockdown device	Degradation/Outage	Any delay or lack of function of device
Visitor Management System	Visitor check-in, Pre-Registration Portal, or Visitor Sponsor	Visitor enrollment/check-in kiosks down
Visitor Management System	Tenant lockout during business hours	Tenants are completely unable to access a suite

TIER 1 SEVERITY SERVICE DEGRADATIONS RESPONSE TIMES		
REQUIREMENT	**DEFINITION**	**RESPONSE**
Response Time	Time from customer service call submission until ISSC acknowledges and begins working or troubleshooting	5 minutes (Normal Duty Hours)
		10 minutes (Outside Normal Duty Hours)

Service Interruption Notification	Time from customer service call until ISSC sends an initial service interruption email to customers/stakeholders	Within 15 minutes of beginning response
		Every two hours thereafter until resolved
Repair/Recovery Time	Time from customer service call submission until system parameters are restored within threshold	120 minutes (Normal Duty Hours)
		180 minutes (Outside Normal Duty Hours)
After Action Review	Written summary of service degradation, operational impact to the Government, proximate cause, and short and long term corrective actions. AAR are required for all Tier 1 severity system degradations.	Preliminary report within four hours after repair/recovery time
		Final report within five (5) business days

TIER 2 SEVERITY SERVICE DEGRADATION CRITERIA		
System	**SERVICE DEGRADATION**	**THRESHOLD**
Video Surveillance System	Degradation	10% of cameras per site have diminished quality of video
Video Surveillance System	System-wide, unscheduled complete loss of alarm monitoring	Alarms/events interrupted over any 30 consecutive minute period
Video Surveillance System	Loss of active recording of video surveillance to disk	Cameras not recording any video to disk over any 60 consecutive minute period
Video Surveillance System	Global inability to retrieve recorded video	Non-perimeter cameras cannot have their corresponding live video retrieved
Physical Access Control Systems	Tenant cardholder download delay	Any individual site or PACS delayed by more than 90 minutes from provisioning in PMP until available at PACS panel
Physical Access Control Systems	Visitor cardholder download delay	Any delay of more than 90 seconds from provisioning at kiosk until available at PACS panel lasting more than

		ten minutes
Physical Access Control Systems	Tenant lockout during non-business hours	Tenants are completely unable to access a suite
TelesStaff	Degradation	Any capability is not responding normally for multiple users
TeleStaff	Outage	Users can not access
mLPR	Degradation	Any capability is not responding normally for multiple users
mLPR	Outage	Users can not access

TIER 2 SEVERITY SERVICE DEGRADATIONS RESPONSE TIMES		
REQUIREMENT	**DEFINITION**	**RESPONSE**
Response Time	Time from customer service call submission until ISSC acknowledges and begins working or troubleshooting	30 minutes (Normal Duty Hours)
		60 minutes (Outside Normal Duty Hours)
Service Interruption Notification	Time from customer service call until ISSC sends an initial service interruption email to customers/stakeholders	Within 60 minutes of beginning response

Outage or repair issues not falling into either Tier 1 or 2 shall be responded to within 60 minutes and the Government Lead or COR shall be notified. Based on the issue and impact on security, time for repair will be provided at that time.

Occasionally ISSC system service degradations are caused by a higher-level service disruption. These higher-level disruptions include interruption of electrical service by building management or IT/network disruptions. The Contractor is responsible for identifying when a higher-level service degradation is potentially causing the ISSC system disruption and opening a ticket with the responsible organization. The Contractor shall update or create any service interruption notification that the issue has been referred to others for resolution. The Contractor shall capture the ticket number and lifecycle within their MMS.

The Contractor's Repair/Recovery Time SLAs are placed on hold while the higher-level service disruption is resolved. Once the higher-level service disruption is resolved, the Contractor's Repair/Recovery SLA resumes. The Contractor's MMS shall track the complete ticket lifecycle including time "off the clock" waiting for resolution from another organization. This shall be tracked and maintained in the Service Ticket.

A service call is a verbal or written request by telephone or e-mail from the COR, PFPA Operations Center personnel, or other authorized representative reporting a malfunction

or maintenance problem. The information shall be entered by the Contractor into the MMS and tracked until completion. The Contractor shall commit the appropriate resources necessary to accomplish the repair, to include, but not limited to, system administrator for system issues as well as electronics technician for equipment repairs.

1.5.10.2 Completion of Service Calls: A service call shall be completed per the table above relating to Tier Level response from the time the service call is issued to the Contractor. If a service call cannot be resolved within the specified time period, the Contractor must notify the COR or one of his designated representatives. The Contractor shall submit a written notification that gives:

(1) an explanation of the delay
(2) the estimated time for completion of the service call
(3) evidence showing an effort to comply with the time requirement
(4) corrective measures to avoid repeated failures to meet response and repair time objectives

If immediate repairs cannot be made, the Contractor will coordinate with the tenant occupant/security manager to take all necessary actions or measures to protect the safety of the public and/or Government property.

Deliverable: Monthly report on Service calls and compliance with Tier Response Service Level Agreements

1.5.11 Preventative Maintenance:

1.5.11.1 Preventative Maintenance Plan: Preventative Maintenance Plan: Contractor Responsibilities
The Contractor is required to create, deliver, and continuously maintain a comprehensive, risk-based Preventative Maintenance Plan. This plan requires government approval and must be submitted as a formal deliverable according to the project schedule.

Plan Requirements
The plan must detail the following key areas:

Requirement	Description
Maintenance Details	Clearly document the frequency and type of maintenance for all systems and components.
Minimum Standards	The baseline maintenance frequency must, at a minimum, follow the recommendations of the Original Equipment Manufacturer (OEM).
Enhanced Maintenance	The plan must identify any systems or devices that require maintenance *more frequently* than the OEM recommendations. This is necessary for devices that are critical,

	heavily used, in harsh environments, or would impact security if they were offline.
Scheduling	Propose a maintenance schedule that is phased to cause the least possible disruption to tenant spaces.
Data Verification	Include a process to verify that all system updates and device information are correctly logged in the Maintenance Management System (MMS).
Inaccessible Spaces	A list of rooms/devices unable to access during the PM cycle and a request for support or remediation methods for access next cycle.

a. Baseline Plan is due within 60 calendar days of contract award
c. Final Plan is due within three months of contract award
d. Revised Plan is due within 30 calendar days of any option year award

Preventative maintenance shall also be performed on new systems installed during the life of this contract unless noted otherwise in the individual task orders.

1.5.11.2 Hardware Maintenance: The Contractor shall provide all parts, services required, and equipment necessary to maintain the ISSC equipment to manufactures specifications at an operational site as requested by the Government. Preventative maintenance shall be performed on all systems listed in Section 5.5 of this PWS Statement down to the lowest serviceable level identified by the vendor. The Contractor shall maintain a spare parts inventory and active logistics program to support the fielded equipment for the term of the contract. The contractor shall provide comprehensive Operations and Maintenance (O&M) support to ensure system stability, availability, and performance.

1.5.11.3 Software Maintenance Requirements: The Contractor is responsible for purchasing and managing all necessary software agreements with Original Equipment Manufacturers (OEMs) to ensure access to software and firmware updates for all systems managed under the ISSC.

- Exclusions: This responsibility does not include the operating system (OS) or database management system, unless a specific task order requires it.

Deliverables for Updates & Patches
Within 30 calendar days of an OEM releasing an update or patch, the Contractor must provide the following five items:

Deliverable	Description
1. Patch Overview	An explanation of the update, detailing its new features, capabilities, and bug fixes. The contractor must highlight any new features that address previously identified government needs.

2. Implementation Schedule	A timeline for rolling out the update in both the laboratory and the live production environments.
3. Stakeholder Dependencies	A list of any dependencies related to the patch that will require coordination with other technical or operational teams.
4. Lab Test Report	Documentation confirming that the update has been successfully tested in a controlled laboratory environment.
5. Deployment Recommendation	A formal recommendation from the integrator on whether the government should proceed with deploying the update.

1.5.11.4 PM Reporting Requirements: The Contractor shall deliver a monthly report on the software and hardware serviced the previous month that will include:

a. List of hardware systems maintained.
b. Description of maintenance actions taken.
c. Status of each system (e.g., operational, requires repair).
d. Photos of hardware components before and after maintenance.
e. List of software systems maintained.
f. Description of updates, patches, and optimizations applied.
g. Status of each system (e.g., operational, requires further action).
h. Summary of issues discovered during PM.
i. Severity and impact of each issue.
j. Recommended corrective actions.
k. Resolved issues over the past month of those identified from PMs.

Deliverable: Preventative Maintenance Plan

All licensing issues shall be routed to the Government COR.

1.6 Period of Performance: The period of performance shall be a base year and five option years. Proposal may be requested for additional IDIQ five years .

1.7 Program Management: Program Management Plan

The Contractor shall deliver and implement a detailed plan for the overall management of the ISSC contract. The plan shall be a comprehensive overview of all aspects of the program. Program Management Plan deliverables are outlined as follows:

- Draft Plan is due as part of the Contractor's proposal
- Baseline Plan is due within 30 calendar days of contract award
- Final Plan is due within 45 calendar days of contract award
- Revised Plan is due within 30 calendar days of any option year award

The Program Management Plan shall be the master plan over all individual plans as outlined in this PWS. The program management plan shall include personnel management, configuration management, QA/QC, maintenance, and overall service delivery under ISSC.

As part of the proposal and the final Program Management Plan, the Contractor shall identify potential cost efficiencies or trade-offs for consideration by the Government.

1.7.1 Program Schedule

The Contractor shall maintain an Integrated Master Schedule of all ISSC activity, including maintenance activities, installation work, programmatic review meetings, option year renewals, and warranty and license expirations. This schedule shall be updated on a regular basis to accurately reflect the current schedule.
The Contractor shall provide on-line access to the program schedules at all times. The Contractor shall use a program scheduling software solution that is commercial off the shelf and meets industry standards to develop and maintain schedules.

The Contractor shall use a program scheduling software package that is commercial off the shelf and meets industry standards to develop and maintain schedules.

1.7.2 Personnel Management (On-Site Contractor Support)

Personnel: Before replacing any Contractor employee designated as key or critical personnel, the Contractor shall notify the COR in writing at least 30 calendar days in advance. The Contractor's request shall include a written justification along with the resume/qualifications of the proposed personnel substitution. All proposed personnel substitutions shall possess qualifications that are equal to or exceed the minimum requirements of the PWS. The following personnel are considered key personnel by the Government:

Program Manager

Shall have at a minimum, 15 years of experience in the implementation and sustainment of complex security systems, and a Baccalaureate degree in Management, Engineering, Mathematics, Physics, Computer Science, operations management, business administration, or other related technical fields. The PM shall be certified as a Project Management Professional. The PM must have a TS clearance and be able to obtain and maintain SCI eligibility at the time of proposal.

Clearance must be maintained throughout the length of the contract.

Program Manager will ensure oversight and management of the entire IDIQ.

Be responsible for briefing a wide range of individuals to include United States Government personnel through the Senior Executive Service level on ISSC services, activities, and deliverables.

Ensure the right mix of management, technical, engineering, and maintenance personnel across all Task Orders on the IDIQ. Ensure all personnel have the necessary qualifications, including training, security clearance, badging, and access privileges, and limit the amount of multiple roles personnel have if it impacts execution of duties from TO1, TO2, or subsequent task orders.

Manage and de-conflict multiple ongoing baseline support and technical tasks

Be the lead for interfacing with industry and vendors on applicable systems installed, administrated, and maintained under ISSC.

Identify ISSC system dependencies or of non-ISSC systems dependent on ISSC systems. Document concerns and findings and present to the Government.

Communicate to the Government emerging trends and technologies in the security industry.

Operations Manager (SCC and ICAM Service Desks)

The Operations Manager must have, at a minimum, five (5) years of experience in the management and sustainment of complex security systems and five (5) years of experience in the general supervision and management of personnel or technical functions. The Operations Manager must possess and maintain at least a Top Secret clearance.

SCC lead and manager of systems and personnel in the SCC.

Be responsible for managing all aspects of the monitoring and support of electronic security systems, managed and supported by the SCC.

Oversee the execution and quality of all SLA and system repair activities.

Oversee the completion of all repair activities in accordance with contract requirements.

Track and report on system availability, operability, and any issues at monthly IPRs as requested.

Identify systems or system components reaching end of life, end of service, or requiring lifecycle replacement and notify the Government in writing.

Identify reoccurring causes of system or component failure and propose options to remedy.

Be responsible for the quality and integrity of the data in the MMS.

Senior System Engineers The Senior System Engineers are considered critical and shall be permanently staffed by distinct personnel without a single person managing more than one system:

(Technical Point of Contact (TPOC) for critical electronic security systems) - TPOC shall hold and maintain an active professional certification in at least one (1) of the seven (7) core systems listed below. The TPOC shall possess a minimum of three (3) years of direct, hands-on experience working with, administering, or maintaining the specific system(s) for which they are responsible. The Senior System Engineers must possess and maintain at least a Top Secret clearance.

TPOC Systems List:
1. Physical Security Information Management (PSIM) system

Everbridge Command Center

ESRI ArcGIS (2D Map)

Microsoft Azure map (2D)

Edge360 3D Map

2. Cardholder Identity Management, referred to as the Privilege Management Program (PMP)

Intellisoft Entrypoint

Technology Industries (TI) Entrypoint

Salesforce (Visitor Portals)

Lighthouse FIPSLink

3. Physical Access Control Systems (PACS), to include Intrusion Detection System (IDS)

Gallagher Command Center

Lenel OnGuard

Softwarehouse CCURE

AMAG Symmetry

Zenitel Emergency Call Box

TBS Enterprise Biometrics

4. Video Surveillance/Analytics System

Bosch Video Management System

MOOG Long Range Cameras

Briefcam Analytics

5. Perimeter Intrusion Detection Systems and Barriers Systems

Future Fibre Technologies

SICK LiDAR

Sightlogix

McQ sensors

6. Vehicle and Personnel Screening:

Genetec mobile License Plate Recognition (LPR)

Flock LPR

Gatekeeper LPR

Gate Keeper Under Vehicle Surveillance System (UVSS)

EVOLV screening system

7. Mission Applications:

WebEOC

CAD/RMS

E911

Telestaff

Mobile License Plate Reader (mLPR)

Team Awareness Kit (TAK)

Maintenance Manager

Candidates for the Maintenance Manager role must have a minimum of five years of experience in the management and sustainment of complex security systems. In addition, they must have at least five years of experience in a supervisory role, managing either personnel or technical functions. The manager is required to possess and maintain a Top Secret security clearance.

Responsibilities:

The ESS Operations and Maintenance Manager will perform the following duties:

- Maintenance and Repair: Oversee, track, and ensure the timely completion and quality of all preventative maintenance and repair activities for all Electronic Security Systems (ESS), in accordance with contract requirements.

- System Management: Be responsible for managing all maintenance and support activities for electronic security systems, including passive and active barriers, and screening systems.
- Preventative Maintenance Plan: Develop and maintain the official Preventative Maintenance Plan. This includes following manufacturer recommendations and identifying systems that require more frequent maintenance due to high usage or harsh environmental conditions.
- Lifecycle Management: Proactively identify systems or components that are approaching their end-of-life or end-of-service and notify the Government in writing.
- Failure Analysis: Identify recurring causes of system or component failures and propose effective, long-term remedies to the Government.
- Inventory and Data Management: Ensure that an adequate stock of frequently used spare parts and consumables is on hand to minimize system downtime. They are also responsible for the quality and integrity of all data within the Maintenance Management System (MMS).
- Reporting: Provide weekly and monthly Operations & Maintenance (O&M) summary reports to the Government. These reports will include system issues, mitigation plans, performance metrics, and the status of troubleshooting tickets. The manager will also track and report on all maintenance and repair activities during monthly program reviews.

The Contractor shall provide a workforce possessing the skills, knowledge, and training to satisfactorily perform the services required by this contract. The Contractor shall staff the management organization with qualified personnel for the positions described in the following paragraphs.

Certifications and Training – All Contractor personnel must be properly certified prior to being assigned to this contract work or to perform any work on the ISSC systems. The Contractor shall be responsible for each personnel maintaining the certification and for any training expenses required by the individual to meet certification requirements. The Contractor shall submit a personnel certification database at award of the contract and maintain the database throughout the contract. The personnel certification information shall provide at the request of the government.

Contractor Representatives - The Contractor shall provide an on-site person(s) who shall be physically present during normal duty hours to act as site supervisor(s), conduct total management coordination, and furnish liaison with the Government during system installation, maintenance, and repair. The supervisor(s) shall be the point of contact with the Government. The supervisor(s) shall have the authority to make technical decisions on-site on behalf of the Contractor.

Security Clearance - Contractor personnel performing work under this contract shall have a minimum Secret clearance at time of the proposal submission and shall maintain the level of security required for the life of the contract. The security requirements are in accordance with the attached DD254 (The unit security monitor is responsible for initiating this form).

Personnel supporting the NCC and database administration shall have a TS with SCI eligibility.

Identification of Contractor Employees - (If applicable) 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.

Operational Security:

All Contractor personnel shall be responsible for safeguarding all Government equipment, information and property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

The Contractor shall prohibit the use of Government issued access control 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 Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

Before replacing any Contractor employee designated as key personnel, the Contractor shall notify the COR and KO in writing at least 30 calendar days in advance. The Contractor's request shall include a written justification along with the resume) of the proposed key personnel substitution. All proposed personnel substitutions shall possess qualifications that are equal to or exceed the minimum requirements of the PWS. The Contractor shall not unilaterally change its key personnel without written approval from the KO

1.8 Programmatic Review Meetings: The Contractor shall hold the following meetings. The meeting location will be at the Government site, with date and time to be coordinated with the Government. The Contractor shall provide minutes of all meetings to the Government within one (1) business day of the meeting occurring.

TABLE 2: MEETINGS

MEETING DESCRIPTION	FREQUENCY / OCCURRENCE
ISSC Kickoff Meeting. The Contractor shall introduce key personnel, provide a description of key services and how they will be delivered under the contract, and schedule follow-ups with major system owners.	To be held within 15 calendar days of award.

	Program Monthly Review (PMR) Meeting. The Contractor shall present to the Government the current status of ISSC services and systems, to include all monthly reports, such as: Repair Reports, Installation Log, System Status, action items, and outstanding issues.	To be held monthly
	Coordination Meetings. The Contractor shall attend meetings held by others that affect ISSC systems. These meetings may include, but are not limited to, information technology and information assurance, construction, facility changes, and outages and schedule maintenance. The Contractor shall be expected to provide personnel with the qualifications and knowledge to answer questions and provide detailed information and minimize take backs. The Government shall provide notice of the meeting at least 24 hours ahead of time when possible and the expected role of the ISSC Contractor in the meeting.	Ad hoc

1.9 Contractor Personnel Qualifications: The Contractor shall provide a workforce possessing the skills, knowledge, and training to satisfactorily perform the services required by this contract. The Contractor shall staff the management organization with qualified personnel for the positions described in the following paragraphs.

1.9.1 Contractor personnel supporting systems and applications shall be appropriately certified in prior to being assigned to this contract work or to perform any work on the ISSC systems. The Contractor shall be responsible for any retraining expenses required by the individual to meet certification requirements. All applicable certifications must be submitted at award and kept up to date.

1.9.2 Contractor Representatives: The Contractor shall provide an on-site person(s) who shall be physically present during normal duty hours to act as site supervisor(s), conduct total management coordination, and furnish liaison with the Government during system installation, maintenance, and repair. The supervisor(s) shall be the point of contact with the Government. The supervisor(s) shall have the authority to make technical decisions on-site on behalf of the Contractor.

1.10 Contract Type: The Government will award a Firm Fixed Price Performance based Task Order.

1.11 Place of Performance: The PFPA currently provides protection for DoD facilities in the National

Capital Region (NCR) and RRMC as listed in Appendix A, Table 1. This list is for informational purpose and is not intended to be definitive or binding. 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.

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.

1.11.1 Site Conditions and Work Environment: Site Conditions and Work Environment: The Contractor shall anticipate the need to access confined spaces, which Occupational Safety and Health Administration requires appropriate permits/certifications and defines as roofs, roof hatches and access points; telecommunications closets and high voltage rooms; and areas of high traffic or criticality that may not be interrupted during peak access periods as part of installation, preventative maintenance, and repair activities. The Contractor shall provide installation, preventative maintenance, and repair activities throughout the year, in all weather conditions. The Contractor shall provide the appropriate tools, safety measures, and qualified personnel to accommodate the unique nature of these environments and ambient conditions.

The Contractor shall apply for and obtain any required building permits, including space use, confined space entry, hot work, excavation, electrical, above ceiling, and utility permits from the Building Manager's Office or appropriate authority having jurisdiction prior to performing the required work.

The Government shall provide the Contractor with limited parking based on availability at the Pentagon Reservation, Mark Center, Suffolk, and Raven Rock Mountain Complex. There is no guaranteed Government provided parking at leased facilities. The Contractor shall be fully responsible for procuring parking at all locations to perform work required under this Contract.

1.12 Telework: The COR will determine whether the work to be performed can be successfully accomplished offsite. Teleworking must be accomplished at no additional cost to the Government and with no detrimental impacts to contract performance. Contractor personnel may be required to report on onsite to a government facility to perform services at any time as required by the KO or COR.

1.13 Hours of Operation: (If applicable) The Contractor is responsible for providing services, between the hours of 0700-1800 Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. This does not include any 24/7 task orders and doesn't include the SCC, which is 24/7. For other than firm fixed price contracts, the Contractor will not be reimbursed when the government facility is closed for the above reasons. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

The Contractor shall establish normal operating hours under this contract between 7 a.m. to 6 p.m. Eastern Time (ET) Monday through Friday. The Contractor's Program Manager (PM) and the Government's Contracting Officer's Representative (COR) shall consult and coordinate on any proposed alternate work schedules that may be arranged depending on the operational tempo/needs of the mission.

1.14 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

1.15 Quality Control/Assurance:

1.15.1 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 (QC) shall be provided to the Government within 30 days of contract award. It shall ensure that QC is applied to existing equipment, installed equipment, MMS data, Preventative Maintenance, and Repairs.

- 1.15.2 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). The Government will perform existence and completeness testing monthly on all assets. Additionally, the QA program will follow the requirements of the QASP to include soliciting customer feedback on repairs and installations.
- **Deliverable -** QC Plan - *Due 60 days after contract award.*

1.16 Security: Contractor personnel performing work under this contract shall have a minimum Secret clearance at time of the proposal submission and shall maintain the level of security required for the life of the contract. The security requirements are in accordance with the attached DD254 (The unit security monitor is responsible for initiating this form). Personnel supporting the NCC and database administration shall have a TS with SCI eligibility.

1.16.1 Physical Security: The Contractor shall be responsible for safeguarding all Government equipment, information and property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

1.16.2 The Contractor shall prohibit the use of Government issued access control 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 Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.16.3 All Contractor personnel with a CAC and NIPR access shall maintain in compliance by completing all iCompass training annually as required.

1.17 Contract Administration:

Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The Contracting Officer, COR, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the Contracting Officer will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. These meetings shall be at no additional cost to the Government.

1.18 Transition Support:

1.18.1 Phase In: A smooth and orderly transition between the Contractor and the predecessor Contractor is necessary to assure minimum disruption to vital services and Government activities. The Contractor shall provide a plan for a 30-calendar day incoming transition from the outgoing contractor. The Contractor shall address a transition point of contact who will oversee the entire transition period and all deliverables outlined below and in the deliverables table in Technical Exhibit 2. The Transition Plan shall include, but is not limited to:

- Day-by-day transition schedule with key milestones identified.
- Review and evaluation of current supported systems/services.
- Transition of historic data to new contractor systems.
- Recruitment, onboarding, training, and identification of key personnel and contractor employees.
- Transfer of hardware/software warranties, license information, and service maintenance

agreements (SMAs). New licenses and SMAs shall be procured by the Contractor.

- Transfer of all necessary business and/or technical documentation.
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates, and patches.
- Orientation phase and program to introduce government stakeholders, programs, and users to the contractor team, tools, methodologies, and business processes.
- Transfer of GFE, GFI, and GFE inventory management assistance, to include obtaining, storing, and updating inventory within contractor's maintenance management system.
- On-boarding coordination with Government to account for badging of immediate personnel, system access, ID/access cards, and security codes.

Deliverable(s): Phase In Plan

1.18.2 Phase Out Plan and Continuity of Services: In accordance with this contract, the Contractor shall provide an Outgoing Transition Plan for a 30-calendar day outgoing transition for transitioning work from an active contract to a follow-on contract/order or Government entity. This transition may be to a government entity, another Contractor or to the awardee Contractor under a new contract/order. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this Contract and/or orders issued under this Contract to a successful provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall include, but is not limited to:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services,
- Transition of historic data to new Contractor system, to include maintenance and logistical data
- Government-approved training and certification process,
- Transfer of hardware warranties and software licenses (if applicable)
- Transfer of all necessary business and/or technical documentation, to include all drawings,
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable),
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
- Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
- Transfer of GFE, GFI, and GFE inventory management assistance,

- Applicable TMA debriefing and personnel out-processing procedures, and
- Turn-in of all government keys, ID/access cards, and security codes.

Deliverable(s): Phase Out Plan

1.19 Conflict of Interest:

1.19.1 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.

1.19.2 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.

1.19.3 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.

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

PART 2
DEFINITIONS & ACRONYMS

2.1 DEFINITIONS AND ACRONYMS:

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 assists in administering 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 required to be used in the performance of the contract as indicated in the Key Personnel section listed in the PWS.

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 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
DD 254	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
	National Industrial Security Program (NISP) Contracts
NCCS	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 ITEMS AND SERVICES:

3.1. Facilities: The Government will try to provide desk space in the Pentagon and other DoD Leased/Owned facilities. Space is limited and will be provided when available

3.2. Equipment: The Government will provide cell phones and laptops to certain authorized personnel as selected by the Government, but requested by the Contractor.

3.3. Information: The Government will provide Standard Operating Procedures, Regulations, and Documentation needed to support the ISSC mission at the request of the Contractor.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1. General: The Contractor shall furnish all supplies, equipment, facilities, Software and/or Software Licenses if applicable and services required to perform work under this contract that are not listed under Section 3 of this PWS.

4.2. Clearance: The Contractor shall possess and maintain a Top Secret facility clearance, as stated in the attached DD 254. The Contractor's employees, performing work in support of this contract shall have been granted a Secret security clearance from the DSCA office at time of award. Certain personnel will be required to maintain a Top Secret clearance with SCI eligibility. The DD 254 will be completed within the National Industrial Security Program (NISP) Contracts Classification System (NCCS) at contract award and attached by modification, if timing dictates. The DD 254 will be housed within the NCCS through the life of the contract. The Contractor can register within NCCS at time of award to gain electronic access to the DD 254 in order to submit Subcontractor DD 254s.

PART 5
SPECIFIC TASKS

5. SPECIFIC TASKS:

5.1 Basic Services: The Contractor is required to provide continuous Integrated Security Services throughout the life of the contract. These "static services" include:

- System Support – maintaining the systems, ensuring they are functioning properly, and that they remain online
- Logistics Support – Maintain a real time database of all assets, systems, and versions of each device and application
- Repair Services – Break/fix response to assets, applications, or systems when they are inoperable or not performing as intended
- Preventative Maintenance – manufacturer suggested maintenance, at a minimum of the assets, applications, and systems

These services apply to all current systems (as listed in PWS Section 5), all ongoing initiatives, and any new systems installed during the contract period. The Government will issue Task Orders for these continuous services at the start of each option period.

Separately, Task Orders for new Installation Services will be issued on an as-needed basis.

5.2 Physical Access Control Systems (PACS) and Intrusion Detection Systems (IDS):

5.2.1 Physical Access Control System:

System Description: The PACS provides automated control of doors, turnstiles, gates, and barriers and is integrated with the IDS at the system level. The PACS is augmented by visual intercom systems and integrated door releases that will be installed, maintained, and serviced under ISSC. The PACS is integrated with PSIM, where PSIM is the primary command and control interface for alarm and access notifications. The PACS native applications, however, will serve as a contingency to PSIM should PSIM become unavailable, allowing alarm notification and system administration functions to continue at both the local and Enterprise levels, requiring those applications to be installed at client workstations at varying geographic locations. The PACS is also integrated into the Privilege Management Program (PMP), which is a centralized repository of cardholder holder data and access privileges. In tandem with the data provisioned from PMP, the PACS allows access using 1 to 3 factors of authentication: CARD ONLY, CARD+PIN, CARD+BIO, or CARD+PIN+BIO.

The goal for the PACS and IDS is to have a system that provides a scalable and flexible architecture, uses open industry standards and best practices, and meets the demands for a growing and technologically advancing system. In addition to the current capabilities listed in the Key Performance Requirements, minimum additional requirements for the long-term system improvements to be funded under future individual TO include, but are not limited to, the following:

1. Shall support a minimum of 100,000 cardholders with expansion up to a maximum of 250,000.
2. Shall support PKI challenge and response using a Federal Information Processing Standards (FIPS) 201 approved algorithm to include Random Structures and Algorithms (RSA) 2048, Error Correction Code (ECC) 128 and 256 without a server connection.
3. Shall monitor and control at least 10,000 card readers. The system shall support the current access control card readers.
4. Support only approved card authentication methods.
5. Shall be able to read the full Federal Agency Smart Card Numbers (FASC-N) and adjudicate an access decision based on a change in one field of the FASC-N.
6. The System shall support reading the full 128bit Global Unique ID (GUID) in the Cardholder Unique Identifier (CHUID) of the PIV card and make control decision based on a change in one bit of the GUID.
7. The System shall support configurable multi-factor authentication, including Common Access Card; Common Access Card and personal identification number (PIN) code; Common Access Card, PIN, and biometric; Common Access Card and biometric; or biometric and PIN.
8. The System shall allow the intrusion detection system to be placed in a maintenance mode for testing without impacting alarm monitoring or system performance.
9. The System shall support anti-pass back across multiple field panels and shall function in the absence of server communications.
10. The System shall support granular control over the ability of operators to grant or revoke permissions to an area.
11. The system shall be supported with a data warehouse, which consists of aggregate identity data from PMP and swipe history from all PFPA PACS. Contractor shall maintain existing data as well as ensure new information is incorporated into the data warehouse.

Additional information on the PACS/IDS Systems is listed in Appendix: Systems and Devices

System Performance Requirements: The key performance requirements of the current system are:

1. The System shall support HSPD-12 compliant Personal Identification Verification (PIV) cards and other smart card technologies. The system shall be compliant with FIPS 201-2 and Federal Identity Credential and Access Management (FICAM).
2. All system components must be approved for use by the General Services Administration (GSA) Approved Products List (APL) per Office of Management and Budget (OMB) M-11-11. These components include card readers, biometric devices, door controllers, locking devices, balance magnetic switches (BMS), and other hardware devices.
3. Have the system capacity for a minimum of 100,000 cardholder records stored locally in the access control system (ACS) panel/database unit (DBU) with expansion possible to a maximum of 250,000.
4. Monitor and control at least 10,000 card readers.
5. ACS has the capability to track a minimum of ten (10) access control levels per individual.
6. Process, annunciate, and activate a single access control system status change within 1.2 seconds. Features shall include generating an alarm condition when tenants fail to secure alarmed zones within programmed “secure hours” or at the end of the occupied duty day.
7. Track and record every event transaction and assign a date, time, and location stamp.

8. Permit the minimum throughput processing time of ten (10) individuals per portal per minute. “Portals” are any doors, turnstiles, pedestrian gates, vehicle access control points, or other electronic devices installed to control access to a specific area.
9. Include capabilities for anti-pass back detection (to include timed-release anti-passback), strike release duration, and door open alarm condition.
10. Incorporate historical reporting of varying forms of access transactions, including specific “event” driven reports that pinpoint alarmed activity at specific door, portal, person, priority, or sensor location, and general logging reports that record all transactions combined.
11. Provide the capability for authorized users to control the access rights to the facilities that they control.
12. Provide for automatic voiding of selected individual cards from the system after the system administrator or Government-authorized manager has defined that duration for access has reached the permitted limit or that the individual is no longer authorized access.
13. Provide for a minimum of 256 operator logins and passwords.
14. Maintain a current file on each enrollee. System shall provide for user-defined and generated data fields and user-defined sorting capabilities.
15. Produce user-defined and generated data lists and other reports upon demand for security management purposes.
16. Use password controls and/or CAC to prevent unauthorized access to data and partitions within the database.
17. Prevent database files from being lost or damaged by power or equipment failures.
18. Report unauthorized entry attempts, by individual name and card number.
19. Automatically void selected cards that have been used for attempts of unauthorized entry.
20. Be capable of interfacing with biometric devices for controlling access.
21. Card readers shall be tamper and vandal resistant devices with a visual display to indicate status and optionally provide a keypad for the input of a PIN.
22. Support multiple means for enrollment, primarily performed by the Privilege Management Program and modification of personnel data, such as keypads, customer service terminals, and client stations over the local area network (LAN).
23. Enable the establishment of multiple access groups; groups of individuals assigned identical access privileges based on access portal, time, and day of the week.
24. Provide a Graphical User Interface (GUI).
25. Provide a wide variety of access control devices and associated hardware, including, but not limited to, card readers, keypads, turnstiles, mantraps, biometric personal identity verification devices, locking devices, egress devices, and passive and active barrier systems, using industry standard power and communications interfaces with controllers, communication networks, and workstations.
26. ACS shall meet all applicable Underwriters Laboratories (UL) standards listed in the References section
27. Provide ability to separate access rights based upon privileges (e.g., individual is a Contractor and only military reservists should have access to spaces based upon granted privileges).

Deliverable:

Contract shall provide a report to the Government confirming compliance of existing PACS and IDS, as it relates to the aforementioned requirements (within 6 months of award)

5.2.2 Intrusion Detection System (IDS):

System Description: The Intrusion Detection System (IDS) provides monitoring of alarm sensors, primarily by the PSIM and secondarily from dedicated alarm client workstations. At the periphery, the IDS is comprised of alarm initiating devices and associated hardware including, but not limited to, High Security Switches (HSS), motion sensors, video motion sensors, glass break sensors, tamper switches, duress switches, fence line sensors, LiDAR, and other perimeter IDS devices. These end devices report alarms to the IDS and from the IDS to the PSIM.

The Mark Center and Pentagon combined has over 8 miles of perimeter fence line. The Pentagon fence line is covered by SIGHTLOGIX video analytical sensors. The Pentagon Force Protection Agency also has installed perimeter IDS with dual sensor technology using a combination of Future Fibre Technologies (FFT) at the Pentagon and Mark Center. Utilizing FFT intrusion detection system in conjunction with the current SIGHTLOGIX system is done to mitigate nuisance alarms. All of the perimeter sensors are integrated into BVMS and the ACS. The vendor shall be responsible for maintenance and repairs of existing system as well as the additional future coverage. The installation of the additional sensors will be funded with a separate task order.

System Performance Requirements:

1. All IDS system design and installation shall meet the requirements of the space being protected per the applicable Federal and DoD regulatory requirements. These requirements include, but are not limited to, the Unified Facilities Criteria; ICD 705, DoD 5200.01-M, DoD 5100.76-M, and 32 CFR parts 2001 and 2004 for classified spaces; and Interagency Security Committee Standards for leased facilities.
2. The System shall provide the capability for monitoring personnel to enter comments upon acknowledgement of an alarm event. System shall provide space for a minimum of 250 characters.
3. The System shall provide a log of events and alarms, including comments on actions taken for each in a spreadsheet format.
4. The System shall provide administrators the capability to enter alarm instructions for each security zone. System shall provide a minimum 500 characters of space for alarm instructions.
5. The System shall provide administrators with the capability to enter security zone contact information in a standard database format (e.g., name, phone number, e-mail, etc.). System shall allow entry of, at minimum, ten (10) security contacts and contact information. System shall provide the capability to generate a database query and printable report for use in updating or verifying security contact information. Reports shall be scalable to allow for a full report of all zones or individual zones as necessary.
6. The System shall provide the capability to establish separate monitoring for intrusion detection and access control alarm events.
7. All intrusion detection equipment must be UL-listed (or equivalent) and approved by PFPA (ICD 705, DoD 5200.01, Volume 3, DoD 5100.76). All equipment shall maintain an active UL certification.
8. Failed sensors shall cause an immediate and continuous alarm activation until the failure is investigated and corrected (ICD 705, Chapter 7, Para 3.a.(3)).
9. The System shall provide the capability for installation of duress buttons that report to a local or off-site monitoring station (Interagency Security Committee (ISC), Level III).

10. The System shall detect an unauthorized penetration or entry into the secured area (DoD 5200.01, Volume 3, Para 2.(6)).
11. Each zone shall have a continuous probability of detection greater than 95% and shall be demonstrated with a confidence level of 99%. This probability of detection is defined as 45 successful detections out of 46 tests or 98 successful detections out of 103 tests (Unified Facility Criteria (UFC) 4-021-04A).
12. Each Exterior perimeter sensor/Zone, Nuisance Alarm Rate must not exceed three alarms per day.
13. Each IDS Sensor/Zone must not exceed one false alarm per day for per 30 day period.
14. Interior Sensors Nuisance Alarm Rare must not exceed three alarms per month, and the False Alarm Rate must not exceed one alarm per month.
15. Contractor shall provide personnel to accompany the Government on weekly perimeter IDS weekly testing in the field and personnel at a monitoring station to ensure that alarms are annunciating as required, to include camera slewing to an alarm event (SIGHTLOGIX, SICK, and FFT) Contractor shall conduct on the spot corrections to any perimeter sensor that requires zone adjustments to ensure there are no gaps in the detection field. If zone adjustments are made the sensor/zone will need to be retested to ensure any and all corrections are suitable with government concurrence.
16. Contractor shall conduct tamper switch testing on all Field Distribution Box that is in support of a perimeter sensor. If a tamper switch is found not operational for configuration or mechanical reasons the contractor shall ensure that it is corrected within 24 hours.
17. The System shall include a 30-second audible countdown upon valid entry to allow for an authorized occupant to disarm the system. Upon expiration of the 30-second period, the system shall transmit an alarm to the monitoring station (ICD 705, Chapter 7, Para. 3.a)(6)).
18. The System shall include a 30-second audible countdown upon a valid command at the security panel to arm the system. Upon expiration of the 30-second period, the system shall transmit an audible and visual indicator and generate an alarm to the monitoring station ((ICD 705, Chapter 7, Para. 3.a)(6)).
19. The System shall include a maintenance mode. When the alarm zone is placed in the maintenance mode, this condition shall be signaled automatically to the monitor station. The signal shall appear as an alarm or maintenance message at the monitor station, and the IDS shall not be securable while in the maintenance mode. The alarm or message shall be continually visible at the monitor station throughout the period of maintenance.
20. All maintenance periods shall be archived in the system. A self-test feature shall be limited to one second per occurrence (DoD 5200.01, Volume 3, Para 2.d.(4)).
21. Shunting or masking of any internal zone or sensor shall be appropriately logged and recorded in archive. A shunted or masked internal zone or sensor shall be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors (DoD 5200.01, Volume 3, Para 2.d.(5)).
22. Indications of alarm status shall be displayed at the monitoring station and optionally within the confines of the secure area (DoD 5200.01, Volume 3, Para 2.d.(6)).
23. The System shall provide an option for installation of an 8-hour operating power battery and an option for an 24-hour operating battery in the event an emergency power generator circuit is not available (DoD 5200.01, Volume 3, Para 2.d.(7)(a); ICD 705, Chapter 7).
24. Immediate and continued alarm notification shall occur for the following conditions (ICD 705, Chapter 7):
    1. Intrusion detection

2. Failed sensor
3. Tamper detection
4. Maintenance mode (a maintenance message may display in place of an alarm)
5. Zones that are shunted or masked during maintenance mode
6. Duress alarms (PFPA operating requirement)

25. The System shall transmit one event for each intrusion zone alarm regardless of the number of sensors/conditions triggered. The system shall provide the monitor with the capability to expand each alarm event to determine the conditions begin triggered.
26. Failed/changed power status shall be indicated at the Premise Control Unit (PCU) and the monitoring station (ICD 705, Chapter 7).
27. Tamper circuits and emergency exit door circuits shall remain in the secure mode of operation (ICD 705, Chapter 7).
28. The system shall report when communications to a PCU has been lost or interrupted (ICD 705, Chapter 7).
29. The System shall provide a standard IDS labeling scheme for all alarm conditions and types to prevent inconsistent queries and/or monitoring practices. (PFPA Operational Requirement based on design intent established in ESS Device Naming Nomenclature, June 24, 2013).
30. The System shall provide a method for alarm monitors to expediently identify the building/location, floor, suite, tenant, security contact information, and unique instructions.
31. All signal or data transmission lines between sensors and the alarm annunciation console shall be supervised by the system. The system shall supervise the signal lines by monitoring changes in the direct current that flows through the signal lines and a terminating resistor. The system shall initiate an alarm in response to a current change of five percent or greater. The system shall also initiate an alarm in response to opening, closing, shorting, or grounding of the signal and data transmission lines (Unified Facilities Guide Specification 28, Electronic Security System).
32. The System shall provide the capability for a GUI that displays IDS devices in a map or floor plan display and provides a color-coded representation of each sensor's operating status (Unified Facilities Guide Specification 28, Electronic Security System).
33. The System shall provide monitors the capability to observe, acknowledge, and dispatch to all alarm conditions within two minutes of annunciation during peak alarm system traffic levels.

Key Services:

System Support: The Contractor shall provide overall system support as defined in Section 1.5.5. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.

The Contractor shall produce system reports in response to requests for information.

The Contractor shall take an active effort in alarm reduction efforts. This effort includes routinely visiting tenant spaces to identify the cause of nuisance alarms, maintaining a list of offending spaces, system configuration strategies to reduce the burden of high frequency nuisance alarms, tenant and Operations Center training on responsibilities and proper system use, and recommendations for improvement. On-site Pentagon Operations Center

support shall be consistent for PSIM, BVMS, AMAG, Gallagher, C-Cure, DMP, Avigilon, and other applications.
The Contractor shall advise PFPA on the top 10 offending spaces in order for the PFPA Alarm Reduction Team to visit the offender spaces to provide remedial training. This report of the top 10 offending spaces shall be provided monthly to PFPA.
The Contractor shall provide a scheduled twice-yearly system "clean-up", to include, but are not limited to, the purge of obsolete system configuration, system overlap, and verification of standard programming configurations. All proposed changes will be presented to the Government for approval prior to implementation.

The Contractor shall ensure access control system records are maintained in accordance with the approved System of Records Notice (SORN). The Contractor shall be able to track and report on the lifecycle of a PACS/IDS alarm, including, but not be limited to, the following:

1. Time of receipt of alarm.
2. Name(s) of security or response force personnel.
3. Dispatch time.
4. Arrival time of responding personnel.
5. Nature of the alarm.
6. Follow-up actions that were taken

The Contractor shall support 3rd party system integrations to include hardware / software, associated connections, and applicable integration testing of third party system.

The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations per Section 1.5.8.

Logistics: The Contractor shall supply adequate materials to meet the requirements for repair and maintenance.

Repair: The Contractor shall provide repair of the system.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability. During scheduled PM, contractor shall ensure that the batteries are up to date and maintained or replaced as necessary.

5.2.3 System Description: PFPA's Physical Security Information Management (PSIM) system is a commercial-off-the-shelf (COTS) enterprise solution designed to enhance command and control, security management, and overall situational awareness for its security operations centers. The system plays a critical role in surveillance, alarm, and incident management, ensuring streamlined security operations across the Pentagon and National Capital Region (NCR) facilities. As an integration platform, the PSIM system connects over fifteen disparate electronic security systems, enabling them to function collectively. It automates the application of business rules and operational procedures, assisting security operators in managing alarms and incidents effectively.

Additionally, the PSIM system integrates seamlessly with PFPA's Identity, Credential, and Access Management (ICAM) solution, known as the Privilege Management Program (PMP) system, to provide comprehensive and easily accessible personnel data.

PFPA's PSIM system is built on a robust infrastructure consisting of two server chassis located in geographically separate locations. Each chassis houses three blade servers, ensuring high availability and load balancing through VMware High Availability, Site Recovery Manager, and Distributed Resource Scheduling. The system, identified as Everbridge Control Center, was deployed in 2021 and has since been a cornerstone of PFPA's security operations.

PFPA's PSIM integrates over fifteen subsystems, including 2D and 3D Geographic Information System (GIS) capabilities and a data warehouse. The number of subsystem integrations is expected to grow, reflecting the system's scalability and adaptability. Currently, the PSIM system incorporates over 150 business logic implementations, which are regularly adjusted in coordination with the Security Operations Centers to meet evolving operational needs. Furthermore, there are more than 70 PSIM client applications deployed across PFPA's enterprise, serving security operators and end users in at least three security operations centers.

System Performance Requirements: Systems shall be maintained per DoD requirements (DoDM 5200.08, DoDM 5200.01, and ICD705), UFGS 28 10 05, and UFC 4-021-02, vendor guidance, or industry best practice, whichever is the highest standard.
System MTBF: 10,000 hours (Minimum)
Applies to the aggregate head-end system acting as a single unit (servers and software)
System Availability: 99.9% up time. Achieved through implementation of the following:
Clustering and Failover
Hardware Redundancy
MTTR (Mean Time to Repair) – defined in SLA

Potential System Enhancements:

- Expand Subsystem Integration and Management - As the number of integrated subsystems is expected to increase, prioritize the integration of emerging technologies such as artificial intelligence (AI)-powered analytics and advanced threat detection systems. This would further enhance situational awareness and proactive incident management. Enhance subsystem management capability to monitor subsystem and connectivity health, detect failures/malfunctions, and inform stakeholders for quick resolution.
- Enhance Data Analytics Capabilities - Incorporating advanced data analytics tools and solutions into the PSIM system could provide deeper insights into security trends and patterns, enabling predictive analysis and more informed decision-making.
- Improve User Interface - Regularly evaluate the user interface of the PSIM client applications to ensure they remain intuitive and user-friendly.
- Strengthen Cybersecurity Measures - Given the critical nature of the PSIM system, it is essential to continuously assess and enhance cybersecurity measures to protect against potential threats and vulnerabilities.

- Disaster Recovery and Redundancy - While VMware High Availability and Site Recovery Manager provide robust disaster recovery capabilities, conducting regular tests and simulations of disaster recovery plans can ensure readiness in the event of a system failure. Implement enhanced redundancy to support automatic failover between designated locations.

Services:

- System Support: The Contractor shall provide system support for the following:
  - Perform configuration changes, systems administration, software and firmware updates/ patching, system health monitoring, and information assurance compliance.
  - Provide an annual geospatial information system update of building floor plans, aerial imagery, and regional data.
  - Provide real-time updates of sensors and devices in PSIM from connected sub-systems as those sub-system components are changed.
  - Create or make changes to response workflows, business logic, and alert thresholds.
  - Produce system reports in response to requests for information.
  - Maintain an active Laboratory environment to test system configuration changes, software updates, and integrations.
  - Provide End User Training for government and contractor personnel to maximize the system's capabilities and ensure efficient usage.
- Logistics: The Contractor shall supply adequate materials to meet the requirements for repair and maintenance.
  - Spare parts - The Contractor shall have spare parts necessary to meet response times for Tier 1,2, or 3 incidents. These assets shall be tracked in the inventory system
  - Licenses - The Contractor shall track licenses and dates for license of systems and applications and maintain the data in the inventory system

- Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan. These Preventative Maintenance services shall include, but not be limited to, system/UI/component/services testing, routine diagnostics and cleaning, maintaining licensing and vendor hardware/software/firmware support agreements, and routine administrative tasks necessary to maintain system operability.
  - Maintain system backup and redundancy capabilities.
  - Annual system assessment and evaluation by OEM.
  - Maintain subsystem connectors using the latest and bug free versions. Track new release, inform the government systems owners and deploy in accordance with the preventive maintenance plan.

- Repair: The Contractor shall provide repair of the system. When systems experience malfunction or failure, the Contractor shall work with PSIM and subsystem manufacturers to identify root cause of the issue and collectively resolve the problem. The Contractor shall manage the coordination and ensure complete resolution of the problem within time frame identified in SLA described in the Maintenance and Operations section of this document.

5.2.4 Video Surveillance System (VSS):

System Description: The current employed VSS at the Pentagon Reservation is Bosch Video Management System (BVMS), version 11 and consists of both analog cameras on encoders and full IP cameras. Cameras are both fixed and pan-tilt-zoom (PTZ) and employ both visible and non-visible light technologies. All video is recorded on a two- tier system utilizing NetApps single and dual controllers, expansion units where needed, and a disaster recovery network architecture all managed by Bosch's Video Recording Manager (VRM). Tier 1 response is for critical is a high quality, low retention time solution operating in close physical proximity to the camera or encoder in order to minimize bandwidth consumption and provide core network outage resilience. Tier 2 is both logically and physically centralizes video storage at a lower frame rate, but is archived for a longer duration. Both Tier 1 and Tier 2 storage is covered by a full NetApp hardware/labor warranty that allows for replacement of hard-drives without turn in of the failed drive.

The perimeter at the Pentagon Reservation uses a combination of Bosch advanced video content analysis (VCA), SightLogix sensors, Briefcam Video Analytics, and Future Fibre Technologies fibre optic intrusion detection all integrated into the VMS via Bosch's Software Development Kit (SDK). Each sensor has associated fixed cameras, while groups of sensors have an associated PTZ. When pre-programmed alarm conditions are met, associated auto calls are initiated, and reported in BVMS both locally and in the Operations Center.

The entire Pentagon system resides on a redundant 10 GB/s, OGC/OGA managed multicast network, with Power- over-Ethernet (PoE) available in most locations.

Presently, a single tiered approach to storage is deployed throughout the Leased Facilities. Viewing both live and recorded video is based on accounts assigned via Active Directory and user rights assigned via the VMS. Storage devices located in leased facilities currently do not have warranties on hard-drives or cameras. SightLogix, FFT, and various BVMS VCAs are also deployed at the Leased Facilities. The alarms from these devices are integrated into the operations centers of these sites.

It is further anticipated/expected that PFPA will continue with an enterprise approach for visual surveillance. New VSS equipment and systems requested will be completed through individual task orders.

In the event that a site is not added to the enterprise system, it is anticipated to be installed in such a way that is compatible with the enterprise solution.

Additionally, mobile, field deployable VSS platforms shall be maintained by the Contractor.

Additional VSS details are identified in Appendix Systems and Devices.

System Performance Requirements: The Contractor shall maintain and repair all VSS in accordance with Section 1.5.10 and 1.5.11. For planning purposes, the current ratio of non-mission critical to mission critical cameras at the Pentagon is a 4:1 ratio. Additionally, all perimeter SightLogix cameras are considered mission critical and considered Tier 1 (See Table 1).

Systems shall be maintained per DoD requirements (DoDM 5200.08, DoDM 5200.01, and ICD705) and UFC 4-21- 02, vendor guidance, or industry best practice, whichever is the highest standard.

The System shall support no less than the VMS's manufacturer suggested maximum number of connections. Enterprise system shall maintain interoperability across the three primary locations (The Pentagon, Mark Center, and DHHQ) at a minimum. Non-enterprise system scenario shall work independently from the system's enterprise solution.

Key Services:

System Support: The Contractor shall provide overall system support as defined in Section 1.5.5. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.

The Contractor shall provide system performance validation, verification of that video storage and retention requirements are met, rule-set programming for auto-calls and camera schedules, video content analysis programming, reports/analysis on VSP related assets, home position programming, camera number changes, routine reporting on system, system training, bandwidth consumption reports, and other tasks related to system administration of visual surveillance assets.

The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations per Section 1.5.8.

Logistics: The Contractor shall supply adequate materials to meet the requirements for logistics per section 1.5.9 of this PWS.

Repair: The Contractor shall provide repair services as defined in section 1.5.10 of this PWS.
Repair and replacement of equipment shall include but are not limited too; monitoring hardware substitutions, defective hardware and camera replacement, hard-drive and recording device replacement, and camera dome replacement.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan as described in section 1.5.11 of this PWS. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability, camera firmware upgrades, verification of camera fields of view (pass/fail camera testing; pixels on target verification), and connection point verification and validation.

5.2.5 Identity, Credentialing, and Access Management (ICAM)/ Privilege Management Program (PMP):

System Description: PMP provides identity and access management of cardholders within the various Physical Access Control Systems (PACS) deployed at the Pentagon Reservation and delegated Leased Facilities throughout the National Capital Region (NCR). It is supported explicitly by a team referred to as "ICAM," or Identity, Credential, Access Management." ICAM, as it relates to the ISSC, is specific to support of cardholder and visitor management applications and systems.

PFPA-protected facilities are subjected to Homeland Security Presidential Directive (HSPD) 12, Federal Information Processing Standard (FIPS) 201-2, relevant National Institute of Standards and Technology (NIST) Special Publications (SPs), and relevant DoD Instructions, Regulations and Manuals related to identity and access management using approved credentials. To achieve compliance with the regulations, PFPA has deployed PMP, an enterprise solution designed to provide ICAM services across the PFPA protected facilities.

System Support

The Contractor shall provide project management, systems engineering, information technology support, cybersecurity support, consulting and advisory services to ensure operations, maintenance to support ICAM-relevant applications, systems, subsystems, and devices. The Contractor shall update the Government on a weekly basis, or as needed due to urgency, on other ICAM-related Task Orders, system health, system outages and degradations, and instances where Government involvement is required.

The Contractor shall provide a dedicated team to the PFPA ICAM program, consisting of project management, engineering, and field technician personnel to successfully manage and support applications, interfaces, web services, databases, integrations, and peripheral equipment relevant to ICAM programs. The Contractor shall be responsible for maintaining an appropriate quantity of skilled and qualified personnel who hold an appropriate mix of clearances and certifications to successfully fulfill the ICAM mission.

The Contractor shall produce and provide to the Government a roster of personnel and description of his or her role to the ICAM program, and with each add or removal of personnel, an up-to-date roster shall be provided. The Contractor shall make available a mix

of personnel who are appropriately skilled and certified to staff the ICAM Help Desk in order to field requests and issues related to ICAM applications, systems, subsystems, and devices from the Government and end users.

The Contractor shall monitor, maintain, and, for applicable locations, ensure the delivery of newly created PFACs to the respective Pass Offices. Network transport, switching, routing, firewalls, computer network defense, and general network services for ICAM systems will be provided by the responsible IT Service Provider of networks used by ICAM programs. The Contractor shall be responsible for troubleshooting, maintaining, and providing system administration support for ICAM programs, including software updates and configuration of the Operating System, middleware, associated databases, PMP and VMS applications, services, and integrations.

IT Service Requests: The Contractor shall be responsible for requesting and escalating any issues with ICAM programs to the responsible IT Service Provider and continued coordination until the restoration of the degraded ICAM service. The Contractor shall submit all required forms, data, and diagrams to enable services, accounts, and exceptions to ensure proper operation of ICAM servers, workstations, and devices.

System Health and Monitoring: The Contractor shall coordinate with the IT Service Provider the most up-to- date system information to maintain continuous monitoring of applicable ICAM server, workstation, and device health via Solar Winds or similar monitoring platform.

Workstation and Server Patching: The Contractor shall be responsible for ensuring ICAM-related servers are patched and up-to-date by coordinating with the IT Service Provider. The Contractor is not responsible for workstation patches, but shall advise on optimal maintenance windows to minimize operational impacts, ensuring system availability as well as cybersecurity compliance.

Personnel Requirements: In addition to baseline support, the following requirements are needed to support the ICAM System:

- At least one (1) Project Management Professional (PMP) certification, who will be considered the CTR lead.
- At least two (2) STA Certified Smart Card Industry Professional (CSCIP) or STA Certified Smart Card Industry Government (CSCIP-G) personnel

- At least one (1) Senior Database Administrator and one (1) Junior Database Administrator. These positions will be independent of DBAs supporting other areas of both Task Order 1, 2, or 3.
- At least three (2) shall hold a Top Secret Clearance with SCI access
- All personnel shall, at a minimum, meet DoD IAT II requirements
- All personnel shall hold vendor certifications relevant to PMP and its web portals, (e.g. ICEWARE and Technology Industries)
    - All personnel are expected to be able to make application-level configuration changes, to include relevant reporting services.
- All personnel shall possess the Secure Technology Alliance (STA) Certified Engineer ICAM PACS (CSEIP) certification

Maintenance: The Contractor shall provide personnel and licensing/agreements to support all applications, interfaces, web services, databases, integrations, and peripheral equipment relevant to the following PFPA ICAM programs. The Contractor shall procure, track, and ensure the availability of system documentation relevant to ICAM programs, to include, but not limited to, hardware, software, licenses, integrations, and Service Level Agreements (SLAs) with vendors and developers. All equipment in inventory shall be tracked in the maintenance management system.

- Privilege Management Program (PMP)
- Cardholder Management System
- Visitor Management System
- PMP Web Portals
    - Access Management Portal (AMP)
    - Visitor Registration, Sponsor, and Approval portals
    - OSW PA Pentagon Tours visitor portal
    - PFPA Special Events Unit visitor portal
- Identity Management Engine for Security and Analysis (IMESA)
- PMP hardware and physical licenses (dongles) used to support the above mentioned programs and systems; See data in Appendix for Systems and Devices

Training: The Contractor shall provide training support to personnel identified by the Government as part of deployments of current programs and periodic refresher training to end users of ICAM programs

5.2.6 Emergency Call Boxes:

System Description: Mark Center and One Liberty Center utilize a Zenitel based call box systems provide a method for personnel to identify or initiate duress activation, including instant communication to an Operations Center.

Communication devices are currently located in Mark Center and One Liberty Center parking lots, garages and other pedestrian locations. These boxes are used to assist in providing life safety and security on facility grounds. DHHQ utilizes a Commend International system with similar capabilities.

System Performance Requirements: The Emergency Call boxes shall operate in accordance with Manufacturer Recommendations.

Additional Call Box information is identified in Appendix Systems and Devices.

System Support: The Contractor shall provide overall system support as defined in Section 1.5.5. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.
The Contractor shall produce system reports in response to requests for information.

The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations per Section 1.5.8.

Logistics: The Contractor shall supply adequate materials to meet the requirements logistics as described in Section 1.5.9 of this PWS.

Repair: The Contractor shall provide repair of the system per Section 1.5.10.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan as described in Section 1.5.11 in this PWS. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability.

5.2.7 License Plate Recognition (LPR):

System Description: The License Plate Reader (LPR) uses optical character recognition to read license plates at Vehicle Access Control Points (VACP). The LPR captures an image of the front and rear license plates on all vehicles traversing the screening area at the VACP. The LPR cameras perform OCR on the images to identify the state of origin and plate number information. The system queries the license plate data the Microsoft Structured Query Language (SQL) Server database in order to detect adverse information for the history of that vehicle which may indicate a warning to officers at the VACP. ELSAG LPR and Operations Center software is the current system in place at the Pentagon Reservation and RRMC.

Additionally, the Flock Safety License Plate Readers system consists of a network of cameras (currently nine) that capture images of the rear of passing vehicles. These cameras are designed to record not just the license plate number, but also other identifying details such as the vehicle's make, model, color, and even unique features like bumper stickers or roof racks. The system employs machine learning and computer vision to analyze the captured images and compares them against various national and local law enforcement watchlists. Annual License Renewals: The contractor shall provide written notification to the governments Contracting Officers

Representative no later than 90 days prior to the expiration of the annual service/licensing period. Contractor shall include the expiration date, a detailed quote for a one-year renewal period, and any proposed changes to the terms of the service or systems capabilities from FLOCK.

FLOCK Warranty and Lifecyle replacement: The contractor shall provide a warranty and lifecycle replacement plan as part of the annual subscription fee to ensure that the systems operated a peak performance.

Information gathered is integrated with the following information sources:

1. PFPA Parking Database
2. Virginia State Police (VSP). The VSP data also contains National Crime Information Center (NCIC) records
3. PFPA and DoD Counter-Intelligence Data Sources
4. PFPA Be on the Lookout (BOLO) Watch lists

Additional information on the License Plate Reader (Fixed) is identified in Appendix Systems and Devices.
System Performance Requirements: Systems shall be maintained per vendor guidance, or industry best practice, whichever is the higher standard. The System shall correctly maintain at least 90% accuracy in plate recognition. The System shall support up to 20 simultaneous operators across all workstations and monitoring locations at the VACPs and security operations centers.

Unit Locations: FLOCK and other VACP LPR locations and devices are located in Appendix Systems and Devices

Services:
System Support: The Contractor shall provide overall system support. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.

The Contractor shall perform in place adjustments to LPR hardware or software to improve character recognition accuracy.

The Contractor shall produce system reports in response to requests for information.

The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations.

Logistics: The Contractor shall supply adequate materials to meet the requirements for repair and maintenance.

Repair: The Contractor shall provide repair of the system as described in Section 1.5.10 of this PWS.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan as described in Section 1.5.11 of this PWS. These Preventative

Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability.

For this System, the Contractor shall conduct at least four quarterly visits per year. The System includes the server hardware, LPR cameras, storage, backup/archival components, and server and client applications. The Contractor shall maintain the integration between the LPR System and the Under Vehicle Surveillance System (UVSS) interface.

5.2.8 Under Vehicle Surveillance System (UVSS):

System Description: PFPA currently utilizes Gatekeeper as the UVSS solution to inspect the underside of vehicles entering the various VACP on the Pentagon Reservation and at the RRMC. The triggering mechanism for the UVSS is a traffic loop sensor embedded in the pavement at the VACP. As vehicles drive over, the system scans and compiles two high-resolution images of a vehicle's undercarriage to create the vehicle's "fingerprint." The Gatekeeper and ELSAG System (Section 5.6.3) are integrated such that the ELSAG provides the license plate information and images captured by the LPR cameras to the Gatekeeper System. The system is able to detect irregularities on the underside and post a threat warning to officers at the VACP. The images are stored in a Microsoft SQL Server database. The LPR and UVSS systems operate independently to capture the license plate and undercarriage images respectively but combine the data images into one record. Remote viewing and control capabilities are provided in the standard Gatekeeper product.

Additional UVSS information is identified in Appendix Systems and Devices

System Performance Requirements: Systems shall be maintained per vendor guidance, or industry best practice, whichever is the higher standard.

The system shall support up to 20 simultaneous operators across all workstations and monitoring locations at the VACPs and security operations centers.

Unit Locations:

Current equipment quantities for the UVSS equipment on the Pentagon Reservation are as followed:

- Five UVSS units located at RRMC
- Two UVSS units located at the North Rotary and Fern VACP
- Two UVSS units located at Boundary Channel Drive VACP
- Two UVSS systems located at the Mall VACP
- One UVSS system located at the River VACP
- One UVSS system at the Heating and Refrigeration Plant VACP
- One UVSS system at the North Village VACP
- One UVSS unit at RRMC located at the screening facility

Services:

System Support: The Contractor shall provide overall system support as defined in Section 1.5.5. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.

The Contractor shall perform in place adjustments to UVSS hardware or software to improve anomaly detection. The Contractor shall produce system reports in response to requests for information.
The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations per Section 1.5.8.

Logistics: The Contractor shall supply adequate materials to meet the requirements for logistics as described in Section 1.5.9 of this PWS

Repair: The Contractor shall provide repair of the system per Section 1.5.10 of this PWS.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability.

For this System, the Contractor shall conduct at least four quarterly visits per year. The System includes the server hardware, cameras, storage, backup/archival components, and server and client applications. The Contractor shall maintain the integration between the LPR System and the UVSS interface (See Section 5.2.7).

5.2.9 Turnstiles:

System Description: PFPA currently utilizes a range of half, ¾, and full height turnstiles located in the interior and exterior of the Pentagon Reservation, Raven Rock Mountain Complex, Mark Center, Suffolk Building, One Liberty Center, and Defense Health Headquarters. All turnstiles use PACS to grant entry or exit.

Additional Turnstile information is identified in Appendix Systems and Devices

System Performance Requirements: The Contractor shall ensure that all turnstiles in the Pentagon, RRMC, Mark Center, Suffolk Building, One Liberty Center, and DHHQ are operational. This includes but is not limited to the access control function of accept or deny based on card access, remote operation as well as the cabling and wiring into the turnstile, internal components and physical external components of each turnstile. Turnstile services shall be done in a manner that does not limit entrance and egress and shall not be completed during high traffic times.
Turnstiles are located internal to the facilities as well as in certain external locations. Installation, maintenance, and repair of turnstiles at facilities other than those listed above may be required under individual TO.

Key Services:

System Support: The Contractor shall deliver a daily turnstile report identifying all turnstiles covered under the ISSC contract along with system availability for each turnstile. In the event that a turnstile is not operationally ready, an estimated timeline for repair should be included within the report.

Logistics: The Contractor shall supply adequate materials to meet the requirements for repair and maintenance per this PWS. The Contractor shall maintain an adequate bench stock of high fail/long lead-time parts in order to meet recovery time objectives. All parts and material used to perform repairs shall be new and be of the same or better capacity of the original manufacturers' component.

In the event damage occurs to a turnstile as a result of misuse (e.g., glass break), the Government is liable for the replacement of the parts associated with misuse; however, the Contractor is still responsible for providing at its own expense the labor for turnstile repairs resulting from the misuse up to five incidents per year.

Repair: The Contractor shall provide repair services as defined in sections 1.5.10 of this PWS.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability. In instances where increased use, environmental, or other factors affect operation of turnstiles, the Contractor shall address increased preventative maintenance in an effort to increase system performance and availability.

5.2.10 Locking Hardware:

System Description: Locking hardware is the physical security device preventing entry into an area protected with an access control and intrusion detection system. This hardware is electronic and connected to the ACS. Some devices such as the mortise locks, Lockmasters Pedestrian Door Lock (LKM) and panic bars have built in request to exit switches, while maglocks and electric strikes do not.

There are approximately 4500 mortise locks installed in the Pentagon and in leased facilities. The Contractor is responsible for repair or replacement of all broken devices, to include devices at end of life or failure. If damaged by negligence, the Government will be responsible for a project to replace it.

Contractor is responsible for integration and connection of LKM locking devices, but not maintenance or replacement of the physical device, unless specified in a separate project.

System Performance Requirements: The Contractor shall also be responsible for the installation, maintenance and repair of all electronic door hardware connected to the access control systems. This includes electric strikes, magnetic locks, panic bars, touch sense bars, electrified mortise and cylindrical locks. This also includes any FF-L- 2890 approved lock, such as the LKM7003. The Contractor is not responsible for the keys, cylinders combination lock on this device (X-09/10 or S&G 2740). The Contractor shall be responsible for maintaining a bench stock of commonly

replaced locks or their components. Maintenance of these devices should include but not be limited to function checks as well as ensuring all screws are tightened.

Logistics: The Contractor shall supply adequate materials to meet the requirements for logistics per Section 1.5.9 of this PWS.

Repair: The Contractor shall provide repair of the system per Section 1.5.10 of this PWS.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan. These Preventative Maintenance services shall include, but not be limited to, device testing, adjustments, and routine cleaning.

5.2.11 EVOLV Weapons Detection Systems:

System Description: The EVOLV system, is an advanced weapons detection system that uses a combination of artificial intelligence (AI), advanced sensors, and extremely low-frequency radio waves (ELF) to screen people for concealed threats like firearms and metallic improvised explosive devices (IEDs). It is designed to be a touchless, seamless experience, allowing individuals to walk through at a natural pace without needing to empty their pockets of common items like keys, wallets, or cell phones.

Warranty Renewal: contractor shall be responsible for renewing and maintaining the manufacturer's comprehensive warranty and all associated software/data subscriptions for each individual EVOLV unit for the entirety of the warranty.

Prior to the expiration of the manufacturer's warranty, the contractor shall advise the government no later than 180 days prior to the expiration of any EVOLV systems end of warranty services. Contractor shall provide the government with a renewal cost of warranties that the government is required to procure and activate a four-year extended warranty and maintenance subscription renewal directly from Evolv Technology, Inc. for each unit

EVOLV End of Life: The contractor shall advise the government if EVOLV Technology, Inc. declares a EVOLV model as 'End-of-Life' or 'End-of-Support' during the four-year warranty period. The contractor shall notify the government point of contact immediately. The contractor shall notify the government, within sixty (60) days, and present a cost proposal to replace the EOL unit(s) with the then-current, manufacturer make and model. The proposal shall include any trade-in value for the old equipment.

5.2.12 Mission Applications:

System Description: The ISSC Mission Application portfolio currently includes the following PFPA applications hosted on DISA's NIPR network (known as "Resource"): Caliber's Computer Aided Dispatch (CAD), Workforce TeleStaff, and the Mobile License Plate Recognition (LPR) system. These applications are separate from PFPA systems on the Life Safety Backbone.

CAD is critical to PFPA's Life Safety and Law Enforcement missions. All police dispatches use the CAD, which passes (or "spills") the critical aspects of each police dispatch event into another

system.

Workforce TeleStaff is an application that allows police superiors and administrators to schedule and track post assignments, as well as scheduled and unscheduled leave for all PFPA's officers.

Mobile LPR allows the Pentagon Police to scan the parking lots and detect violators much more efficiently than the traditional manual method.

Contractor shall configure the software and its environment to maximize the inherent capability of all systems in order to deliver the best customer experience to the PFPA users (e.g. PPD, POC). Note: Contractor may not have account permissions to all aspects of the system (e.g. database servers), as JSP controls these items. Additionally, any hardware requirements on the above Mission Application systems to be fulfilled by the Contractor will be codified via separate task orders. Contractor shall maintain up-to-date architectural drawings of all systems and other content (e.g. Ports, Protocols, and Services Management (PPSM), hardware software lists) needed for the Risk Management Framework submittals. Note: because these systems are housed by JSP, most cyber related activities that touch systems, such as scans and OS patches, are JSP responsibilities.

In the case of Salesforce, the contractor will configure and maintain the Orchard module coding within Salesforce to ensure functionality, make any adjustments and add new features as required by PFPA Recruitment, and work with Salesforce, JSP and DISA to ensure that the environment continues to be connected appropriately.

Maintenance: The Contractor shall acknowledge system outages 24/7/365 within 15 minutes of being reported to the desk. Systems shall be in line with ISSC Tier 1 support. AAR shall be completed for system outages within 24 hours of restoration of services, which shall include an event log showing time, date, actions taken, and root cause.

Each month a "State of the System" overview will be produced that reviews issues and mitigations with the system (if any) that have occurred that month and goals for the next month with respect to enhancements.

5.2.13 LPR for Parking Enforcement:

System Description: The LPR for Parking Enforcement (LPRPE) System provides parking permit enforcement and hot list recognition of wanted vehicles through IP cameras with optical character recognition mounted on vehicles. LPRPE System is integrated to receive permit data from the PFPA Parking System and hot list updates from Virginia State Police.

The System is Genetec AutoVu.
System Performance Requirements:

1. The System shall perform parking permit and hot list enforcement for the Pentagon Reservation.
2. The System shall be maintained per DoD, vendor, or industry standard best practice.
3. The System shall scan a minimum of 500 license plates per minute with at least 95% accuracy.

4. The System shall automatically periodically synchronize permit and hot list data from the authoritative sources with the field unit, and the field unit shall provide up to date enforcement data.
5. The System shall be expandable to at least five vehicles.
6. The System shall protect data-in-transit and data-at-rest.

Additional LPRPE information is identified in Appendix Systems and Devices

Services:
System Support: The Contractor shall provide overall system support as defined in Section 1.4.4. The Contractor shall perform configuration changes, systems administration, software updates/patching, monitoring, and information assurance compliance.

The Contractor shall perform in place adjustments to LPRPE hardware or software to improve character recognition detection.

The Contractor shall produce system reports in response to requests for information.

The Contractor shall maintain an active Laboratory environment to test system configuration changes, software updates, and integrations per Section 1.5.8 of this PWS.
Logistics: The Contractor shall supply adequate materials to meet the requirements for logistics per Section 1.5.9.

Repair: The Contractor shall provide repair of the system per Section 1.5.10 of this PWS.

Maintenance: The Contractor shall maintain the system in accordance with their approved Preventative Maintenance Plan per Section 1.5.11 of this PW. These Preventative Maintenance services shall include, but not be limited to, device testing, routine cleaning, maintaining licensing and vendor hardware/software support agreements, and routine administrative tasks necessary to maintain system operability.

PART 6
APPLICABLE PUBLICATIONS *(If applicable)*

(In this section list any publications, manuals, and/or regulations that the contractor must abide by. See example provided below.)

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS) *(If applicable)*: *(In this section list any publications, manuals, and/or regulations that the contractor must abide by. See example provided below.)*

6.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. (For example, insert AR 25-2, AR 530-1.)

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING *(If applicable)*

(Under this section list all attachments and technical exhibits that will be useful for the contractor to submit an appropriate proposal.)

7. Attachment/Technical Exhibit List:

7.1. Attachment 1/Technical Exhibit 1 – Performance Requirements Summary *(This document is required for every PWS. See attached example for format.)*

7.2. Attachment 2/Technical Exhibit 2 – Deliverables Schedule *(This document is required for every PWS. See attached example for format.)*

7.3. Attachment 3/Technical Exhibit 3 – Estimated Workload Data *(This document should be made available if historical data exists. For FFP contracts, the PWS needs to provide information on the extent of the required tasks (information as appropriate on exact amounts of tasks, estimates of amounts, etc.) and not just the estimated manning hours. This information should be meaningful enough to provide a legally adequate description of the quantity of work. This information can either be included in the body of the PWS, alongside the specific tasks listed in section 5, or it can be listed in a Technical exhibit such as Technical Exhibit 3,*

TECHNICAL EXHIBIT 1

PERFORMANCE REQUIREMENTS SUMMARY

1. Performance Requirements Summary

The Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

TABLE 4 – PERFORMANCE REQUIREMENTS TABLE

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
System Availability	**1.4**	All production ESS and associated components shall maintain operational availability.	99.9% availability, measured monthly, excluding Scheduled Maintenance.	System monitoring tools; analysis of outage reports.
Mean Time to Repair (MTTR)	**Table 1**	The average time taken to restore service after a system outage.	For Priority 1 incidents, MTTR shall not exceed 4 hours. For Priority 2 incidents, MTTR shall not exceed 8 business hours for 95% of tickets.	Analysis of service ticket data (from incident opening to resolution).
System Reports	**1.5.5**	**Respond to Government requests for tailored reports of ISSC system information within one business day of request.**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
System Components	**Appendix**	**System, sensor, or device meets standards and performs per functional and technical requirements**	**100%**	**100% Government review of all installed system, sensors, or devices**

	1.4	**Technical documentation to be delivered by the Contractor is technically acceptable**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**
Cybersecurity	**1.4.4**	**Cybersecurity configuration changes and application patches shall be completed within three calendar days of vulnerability notification**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
	1.4.4	**Notification shall be made per the PWS within three (3) calendar days of any patches or configuration updates**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
	1.4.4	**Systems shall meet applicable DoD standards for cybersecurity or have an approved Plan of Action and Milestones from the Approving Official**	**100%**	**Random and periodic inspection of system security posture**
Outage Notifications	**1.4.4 & 1.4.6**	**Outage notifications to the Government shall be within one hour of outage recognition**	**95%**	**100% Government review of time to complete actions**

System Support	**1.5.5**	**System administration services are completed per the requirements of the PWS**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
System Performance	**1.4.4**	**Systems operate per the requirements of Section 2.0 and meet applicable regulatory requirements for sensor detection and alarm annunciation**	**95%**	**Periodic and random Government review of system performance**

Visual Surveillance System Support	**1.4.4**	**Video pulls, configuration changes, and system reports shall be acknowledged within one (1) business day of Government request and completed within three (3) business days**	**95%**	**100% Government review of time to complete actions**
Technical Solution Identification	**1.4.4.3**	**Technical Solution Identification reports are completed per the requirements of the PWS**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**
Configuration Changes	**1.4.5**	**Within two business days of receipt**	**95% of the time**	**Random sampling and customer input**
Configuration Management Plan	**1.4.5**	**The Configuration Management Plan shall meet the stated requirements of the PWS**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**
Maintenance Management System	**1.4.5.1**	**The data fields required in MMS per the PWS shall be complete for each system, sensor, or device**	**95% of the time**	**Random inspection**
	1.4.5.1	**Updates to MMS shall be completed within three (3) business days of any procurement, testing, installation, preventative maintenance, configuration change, or repair activity.**	**95% of the time**	**Random inspection**
After Action Review	**1.4.6**	**After Action Reviews shall be completed within 24 hours of an outage per the requirements of the PWS**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
Replacement and Spare Parts Equipment	**1.4.6**	**Sufficient supplies and bench stock shall be maintained to meet requirements of the PWS**	**95%**	**Random inspection**
Repairs are performed on all	**1.4.6**	**Tier 1 Service Calls are responded to within one hour hours and repaired**	**95% of the time**	**Random sampling**

		within two hours during ISSC Service Desk hours		

ISSC systems, devices, and sensors	**1.4.6**	**Tier 1 Service Calls are responded to within two hours and repaired within four hours outside of ISSC Service Desk hours**	**95% of the time**	**Random sampling**
	1.4.6	**Tier 2 Service Calls are responded to within four hours and repaired within 48 hours during ISSC Service Desk hours**	**95% of the time**	**Random sampling**
	1.4.6	**Tier 2 Service Calls are responded to within 24 hours and repaired within 48 hours outside of ISSC Service Desk hours**	**95% of the time**	**Random sampling**
ISSC Service Desk	**1.4.6.3**	**On-site and off-site Service Desk services are provided as specified in the PWS**	**99.5%**	**100% Government review of Contractor staffing**
Requests for Access Control Adds or Changes	**1.4.6.3**	**Within two (2) business days of receipt**	**95% of the time**	**Random sampling and customer input**
Request for Personal Identification Numbers	**1.4.6.3**	**Within two (2) business days of receipt**	**95% of the time**	**Random sampling and customer input**
Request for Access Information	**1.4.6.3**	**Within two (2) business days of receipt**	**95% of the time**	**Random sampling and customer input**
Access Control Center Procedural Compliance	**1.4.6.3**	**Contractors shall comply with the Government's SOP**	**95% of the time**	**Periodic sampling**
Preventative Maintenance	**1.4.7**	**Preventative maintenance services are performed to the quality level and time intervals stated in the approved Preventative Maintenance Plan.**	**95% of the time**	**Random sampling**
Preventative Maintenance Plan	**1.4.7.1**	**The Preventative Maintenance Plan shall meet the stated requirements of the PWS**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**
Software Upgrades	**1.4.7.3**	**Application patch update overview, testing, and deployment recommendation is made within 30 days of OEM vendor release**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the**

				Contractor
Quality Assurance/Quality Control Plan	**1.6.1**	**The Quality Assurance/Quality Control Plan shall meet the stated requirements of the PWS**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**

Facility Clearance	**1.6.7.1**	**The Contractor shall maintain a facility clearance per the requirements of the PWS**	**100%**	**100% Government review of Contractor's facility clearance documentation**
Personnel Security Clearances	**1.6.7.2**	**All Contractor personnel shall meet the security clearance requirements of the PWS**	**100%**	**100% Government review of all Contractor personnel**
Program Management Plan	**1.8.2**	**The Program Management Plan shall meet the stated requirements of the PWS, complete, and technically acceptable**	**100%**	**100% Government review of all technical documentation delivered by the Contractor**
Meeting Minutes	**1.8.4.2**	**Meeting minutes shall be provided to the Government within one business day of the meeting occurring**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**
Key Personnel	**1.9**	**All Key Personnel shall meet the requirements of the PWS**	**100%**	**100% Government review of all Key Personnel**
Permit Compliance	**5.4**	**All permits shall be applied for and received prior to commencing work**	**100%**	**100% Government review of permit compliance**

System Information	**5.5**	**Respond to Government requests for information for ISSC system information within 48 hours of request**	**95%**	**100% Government review of time to complete actions and all technical documentation delivered by the Contractor**

TECHNICAL EXHIBIT 2

DELIVERABLE
SCHEDULE

1. Deliverable Schedule

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 6.1-6.2. However, schedules for reference items 6.3-6.5 and beyond 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) 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.

TABLE 5 – DELIVERABLE SCHEDULE

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Alarm Report & System Health Report	1.5.5	Contractor Determined Format	Daily	Standard Distribution
After-Action Reports	1.5.10	Contractor Determined Format	Within one (1) calendar day of issue identification	Standard Distribution
Task Order/ Installation Status Report	1.5.5	Contractor Determined Format	Monthly	Standard Distribution*

Training	1.7	Contractor Determined Format	As Requested	Standard Distribution*
System Report	5.0	Contractor Determined Format	Within one (1) calendar day of request	Standard Distributio n
Technical Solutions Identification	1.5.7	Contractor Determined Format	24 submissions per contract year	Standard Distributio n
Configuratio n Management Plan	1.5.4	Contractor Determined Format	Draft: To be evaluated as part of proposal Fin al: 60 calendar days after award	Standard Distributio n
Preventative Maintenance Plan	1.5.11	Contractor Determined Format	Draft: To be evaluated as part of proposal Fin al: 60 calendar days after award	Standard Distributio n
System Design Document	1.5.1	Contractor Determined Format	Draft: Completed within 90 days of award. Maintained throughout the contract	Standard Distributio n
As-Built Drawings	1.5.1	CAD	Updated as changes occur	MMS
System Administrato r's Guid	1.5.1	Contractor Determined Format	Draft: Completed within 90 days of award. Maintained throughout the contract	Standard Distributio n (Maintaine d on NIPR)
Standard Operating Procedures (SOPs) /	1.5.1	Contractor Determined Format	Updated as changes occur	Standard Distributio n

Operator's Manual				(Maintained on NIPR)
System Lifecycle Report	1.5.2	Contractor Determined Format	Due monthly after contract award.	Standard Distribution
Lifecycle Replacement Plan	1.5.2	Contractor Determined Format	Annually	Standard Distribution
Application Version Report	1.5.4	Contractor Determined Format	Due 60 days after contract award, updated annually	Standard Distribution
Turnover Log System Operations Report	1.5.5	Contractor Determined Format	Daily	Standard Distribution (Maintained on NIPR)
SCC Manpower Report	1.5.5	Contractor Determined Format	Weekly	Standard Distribution
Laboratory Access Report and Schedule	1.5.8	Contractor Determined Format	Monthly	Standard Distribution
Laboratory Inventory Report	1.5.8	Contractor Determined Format	Quarterly	Standard Distribution
Monthly Inventory Report (all assets)	1.5.9	Contractor Determined Format	Monthly	Standard Distribution
Annual Obsolescence Report	1.5.9	Contractor Determined Format	Annually	Standard Distribution
Service Calls Report	1.5.10	Contractor Determined Format	Monthly	Standard Distribution
Patching Report	1.5.11.3	Contractor Determined Format	Within 30 calendar days of an OEM	Standard Distribution

			releasing an update or patch	
Quality Control Plan	1.15	Contractor Determined Format	Due 30 days after contract award	Standard Distributio n
Phase In Plan	1.18	PDF	Final: To be evaluated as part of proposal	In proposal response to solicitation
Phase Out Plan	1.18	PDF	Draft: To be evaluated as part of proposal Final: At execution of final option year	Standard Distributio n
PACS and IDS Compliance	5.2.1	Contractor Determined Format	Due 6 months after contract award	Standard Distributio n

TECHNICAL EXHIBIT 3

ESTIMATED WORKLOAD DATA

1. Estimated Workload Data

The data (labor categories and hours) provided below is an estimate of what it may take to perform the major categories of requirements listed in the Performance Work Statement. The Contractor is not required to propose the data listed below for the FFP CLINs, and is encouraged to use sound judgment and business practices when preparing its proposal.

Firm-Fixed-Price Contract: 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.

One Full Time Equivalent (FTE) for the Firm Fixed Price CLIN is equivalent to 1872 hours.

Base Period

	FTEs	Base Period 1: 12 Months	Base Period 2: 12 Months	Base Period 3: 12 Months	Base Period 4: 12 Months	Base Period 5: 12 Months
Labor Category		**Hours**	**Hours**	**Hours**	**Hours**	**Hours**
Program Manager (Key)	1	1872	1872	1872	1872	1872
Maintenance Manager (Key)	1	1872	1872	1872	1872	1872
Administrative Specialist	1	1872	1872	1872	1872	1872
Operational Manager (SCC) (Key)	1	1872	1872	1872	1872	1872
Senior System Engineers (Key)	7	13,104	13,104	13,104	13,104	13,104
Junior System Administrator (ISSC Service Desk)	8	14,976	14,976	14,976	14,976	14,976
Database Administrator	2	3,744	3,744	3,744	3,744	3,744
Engineer 1	8	14,976	14,976	14,976	14,976	14,976
Engineer 2	8	14,976	14,976	14,976	14,976	14,976
Engineer 3	8	14,976	14,976	14,976	14,976	14,976
Logistics Manager	1	1872	1872	1872	1872	1872
Logistics Specialist	2	3,744	3,744	3,744	3,744	3,744
CAD Operator	2	3,744	3,744	3,744	3,744	3,744
Technical Writer	1	1872	1872	1872	1872	1872
Electrician 1	12	22,464	22,464	22,464	22,464	22,464
Electrician 2	12	22,464	22,464	22,464	22,464	22,464
Electrician 3	6	11,232	11,232	11,232	11,232	11,232
Safety Officer	1	1872	1872	1872	1872	1872
Quality Control Manager	1	1872	1872	1872	1872	1872
Labor Total	**83**	**155,376**	**155,376**	**155,376**	**155,376**	**155,376**

Option Period

	FTEs	Base Period 1: 12 Months	Base Period 2: 12 Months	Base Period 3: 12 Months	Base Period 4: 12 Months	Base Period 5: 12 Months	FAR 52-217-8
Labor Category		**Hours**	**Hours**	**Hours**	**Hours**	**Hours**	**Hours**
Program Manager (Key)	1	1872	1872	1872	1872	1872	936
Maintenance Manager (Key)	1	1872	1872	1872	1872	1872	936
Administrative Specialist	1	1872	1872	1872	1872	1872	936
Operational Manager (SCC) (Key)	1	1872	1872	1872	1872	1872	936
Senior System Engineers (Key)	7	13,104	13,104	13,104	13,104	13,104	6,552
Junior System Administrator (ISSC Service Desk)	8	14,976	14,976	14,976	14,976	14,976	7,488
Database Administrator	2	3,744	3,744	3,744	3,744	3,744	1872
Engineer 1	8	14,976	14,976	14,976	14,976	14,976	7,488
Engineer 2	8	14,976	14,976	14,976	14,976	14,976	7,488
Engineer 3	8	14,976	14,976	14,976	14,976	14,976	7,488
Logistics Manager	1	1872	1872	1872	1872	1872	936
Logistics Specialist	2	3,744	3,744	3,744	3,744	3,744	1872
CAD Operator	2	3,744	3,744	3,744	3,744	3,744	1872
Technical Writer	1	1872	1872	1872	1872	1872	936
Electrician 1	12	22,464	22,464	22,464	22,464	22,464	11,232
Electrician 2	12	22,464	22,464	22,464	22,464	22,464	11,232
Electrician 3	6	11,232	11,232	11,232	11,232	11,232	5,616
Safety Officer	1	1872	1872	1872	1872	1872	936
Quality Control Manager	1	1872	1872	1872	1872	1872	936
Labor Total	**83**	**155,376**	**155,376**	**155,376**	**155,376**	**155,376**	**77,688**

Estimated Task Orders

PFPA executes about 240-260 separate task orders per year averaging about $18M-22M annually
Approximately 165-190 of these projects fall under the GPC threshold of $25K

In general, approximately 60-70 on-site FTEs have been providing support (operations, help desk, maintenance, task orders, etc.) daily since mid-2023.