ADAP TEMPLATE 211-002 PERFORMANCE WORK STATEMENT (PWS) JUL 2025

INTEGRATED SECURITY SERVICES CONTRACT (ISSC)

Task Order 2

PART 1

GENERAL INFORMATION

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

1.1 **Introduction/Description of Services:** The Pentagon Force Protection Agency uses multiple mission applications and technology to complete its mission for Life Safety and Security of the Pentagon Reservation and Leased Facilities throughout the National Capital Region (NCR). These mission applications and technologies function on the PFPA Life Safety IT Platform known as the Life Safety Backbone or LSB. The LSB platform provides the foundation of the technology required for Video Surveillance, Access Control, Intrusion Detection, and other critical mission services also known as PFPA's Electronic Security Systems (ESS). The LSB platform consists of an on-prem physical and virtual IT environment as well as mission applications in the cloud and on the internet. PFPA requires operations and maintenance support to sustain the use of technology as a force multiplier to its physical security mission

The service expectation is the operations, sustainment, and security of the Life Safety Backbone (LSB) systems architecture. The LSB, which consists of desktops, virtual and physical servers, and network components, serves as the foundation for PFPA's Electronic Security Systems (ESS) and other core mission functions. PFPA has a host of Mission Applications and Systems used to perform their Life Safety and Security mission. These applications and systems reside on an on-prem Platform as a Service environment, and in the Cloud. These systems communicate on the DISA J6 managed NIPRNet, and the Coral Transport network. In addition to the operations and sustainment of the LSB, the contractor is responsible for the cybersecurity certification and accreditation of all PFPA-owned mission systems and applications. The daily technical oversight of this contract is provided by the PFPA Innovation Management Office (PIMO) and the DISA J6 Joint Provider PFPA (JPP) office.

The Government will award a Firm Fixed Price (FFP) Task Order, and the Contractor shall abide by all contractual and PWS requirements defined within. The Contractor shall provide personnel, transportation, tools, supervision, and other items and non-personal services necessary to perform IT Support Services – Service Delivery 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.

1.2 Objectives: The Government's objectives for this requirement include:

- **LSB Platform Operations and Availability** - Ensure the PFPA Life Safety Systems infrastructure is operational through daily systems monitoring and reporting, Available to allow PFPA to meet their mission goals using technology, and Secure and reduce risk to the PFPA mission systems using the cybersecurity defense lifecycle to identify, protect, detect, respond, and recover from any vulnerability or threat.

- **Engineering and Technology Integration** - Provide continuous engineering oversight for the LSB architecture to ensure its integrity, security, and alignment with future mission requirements. This includes establishing a formal process for the evaluation, testing, and integration of new technologies, systems, and projects into the LSB environment. The contractor shall manage the lifecycle of new initiatives from conception through deployment to ensure seamless interoperability, minimize operational disruptions, and maintain the established security posture.

- **LSB Network Availability** - Ensure availability through monitoring and maintenance all LSB network devices connected to CORAL network. The Coral transport network falls under the responsibility of DISA J6. Some of these devices are legacy LSB network devices within the PFPA Server room 3B559 and other locations throughout the Pentagon reservation to include Raven Rock Mountain Complex (RRMC). CORAL network devices located at the Defense Health Headquarters (DHHQ) are included in the requirements of this PWS.

- **Cybersecurity Compliance -** Maintain a Cybersecurity compliance posture of the LSB systems architecture that meets requirements as defined by the Department of Defense Chief Information Officer (DODCIO), National Institute of Standards Technology (NIST), Joint Forces Headquarters DoD Information Network (DODIN) and United States Cyber Command (USCC).

- **Scalability and Interoperability** – The contractor shall ensure that systems are capable of scaling to accommodate additional users, sensors, capabilities, and facilities. Similarly, systems shall be able to adjust down as facilities are closed, suites are decommissioned, or requirements adjusted. Systems and their components shall, to the maximum extent possible, utilize open standards and commercial-off-the-shelf (COTS) technology. Standard network protocols shall be used to traverse the Government's network.

- **Availability and Resiliency** – PFPA requires system availability at or near a 100% operational level to execute and complete its Life Safety and Security mission. Systems shall be designed and implemented to be resilient to failure such that a failure of a single component should not incapacitate the entire system. To achieve this goal, the Contractor shall leverage industry best practices for assuring resiliency and availability.

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

- **Accountability and Customer Satisfaction** – Systems and services shall be designed and implemented to be user friendly, mindful of the impact and sensitivities of the customer workspace, high performing, and to meet contractual service requirements.

1.3 Scope: The scope of this requirement is specific to the LSB Platform and Mission Systems. See Appendix "A", Environment Document for complete list of LSB Mission Application and Systems. The work to be performed is in accordance with (IAW) the Defense Information Systems Agency (DISA) J6 processes, policies and program management specific to eight major service areas:

- Program Management
- Project Management
- Engineering Projects
- Operations and Maintenance
- Cybersecurity
- Configuration Management
- Change Management
- Continuity of Operations (COOP)

1.3.1 **Program Management (PM)**:
The Contractor shall implement a Program Management structure to efficiently and effectively administer, report and oversee the Force Protection Technology Support (FPTS) Contract. Program Management must include a central point-of- contact (POC) responsible for the management, oversight, administration, risks, and substantive communication of all activities performed by Contractor personnel, including subcontractor personnel, to satisfy the requirements in this PWS. The Primary POC (Program Manager) shall provide the program management leadership authority to respond to all types of requests, critical or standard, and deploy the appropriate resources to address any issue pertaining to the scope of support for this requirement.

The Contractor shall provide a monthly Program Management Review (PMR) of the overall performance status of all FPTS service categories. The Contractor shall provide a breakout of, but not limited to achievements, monthly

metrics summary, deliverables, risk management, projects, and any updated program information. This status report shall be given in the form of a monthly PMR presentation by the Contractor to the COR and Contracting Officer.

1.3.1.1 **Program Management Plan**:
The Contractor shall deliver and implement a detailed Program Management Plan (PMP) within 90 calendar days of date of award. The Program Management Plan must be a comprehensive overview and living document describing all aspects as required of the overall contract. It will provide the Contractor's overall approach to the management of the FPTS program requirement. The goal of the plan is to fuse the functional activities and human resources into one program oversight and communication strategy. The PMP shall identify Key Personnel team members' roles and responsibilities, identifying the key activities the Contractor will focus on and specify how all program objectives will be met. Additionally, the plan will provide a summary of the appropriate level of quality assurance and risk mitigation as part of the program oversight, this document will be critical to effective management of the FPTS program.
The PMP shall include, but not limited to, the following:

- **Program Description**: Description specifically the FPTS program objectives and the eight major service categories.
- **Project Scope**: Provide a scope statement or guidelines to the scope of the Program Management Plan.
- **Roles and Responsibilities**: Define the roles and responsibilities of the FPTS program key personnel and describe their mission objectives as they pertain to the major support categories.
- **Roles and responsibilities of support personnel**: Define the roles and responsibilities of the FPTS program support personnel and describe their mission objectives as they pertain to the major support categories.
- **Staffing Strategy**: Includes key personnel, staffing matrix aligned with this PWS to include roles and description; subcontractors; resource backup plan; attendance reporting as described within the COOP or during emergencies; and any additional information deemed relevant.
- **Risk Management Strategy**: Describe risk management to include, but not limited risk register, risk assessment, root cause analysis, corrective action, reporting, monitoring, and communication.
- **Communications Strategy**: Define the Program Manager's role in managing communication. Include the type and frequency of communication, escalation procedures, backup procedures, and other guidelines or expectations.
- **Document Management Strategy**: Define the documentation management strategy.
- **Quality Assurance and Risk Strategy**: Acknowledge all contract deliverables for the FPTS program and define how contract deliverables will be met and how risk will be managed for the FPTS program.
- **Integrated Battle Rhythm**: Maintain, status, and report all FPTS program activity including maintenance activities, patching, updates, Authorized System Interruptions (ASIs) or other activity that would have an impact to the LSB. Ensure all projects are resourced and that no scheduled or unscheduled activities will conflict with other ongoing projects or tasks. The Contractor shall document and report action items relevant to tasks.

MEETING(S):
- Monthly Programmatic Review Meetings

DELIVERABLE(S):
- Program Management Plan
- Monthly Program Management Review (PMR)

1.3.2 **Project Management**
The Contractor shall provide professional Project Management (PM) oversight for all engineering, lifecycle refresh, technical refresh, and modernization projects executed under the IDIQ relating to this FPTS contract. The contractor will successfully manage and execute all project phases, from initiation through closure. The PM methodology shall align with industry best practices, such as those defined by the Project Management Institute (PMI), to ensure projects are delivered on time, within scope, and to the required quality standards.

Project Management Responsibilities
For each project initiated, the Contractor's Project Manager shall be the designated point of contact and is responsible for the following:

- **Project Planning**: Develop and maintain a comprehensive Project Management Plan (PMP) for each Government-approved project. The PMP shall, at a minimum, define the project scope, schedule, resources, communication plan, risk management approach, and key milestones.
- **Execution and Control**: Proactively manage and control project execution to ensure that milestones and objectives are met. This includes managing the project schedule, tracking progress against the baseline, and controlling changes to scope using a formal change control process.
- **Risk and Issue Management**: Identify, analyze, and document project risks and issues. The contractor shall develop and implement risk mitigation strategies and actively manage issues to resolution, escalating to the Government COR as necessary.
- **Stakeholder Communication and Reporting**: Facilitate clear and consistent communication between the project team, government stakeholders, and other relevant parties. The contractor shall provide regular, detailed project status reports and conduct periodic project review meetings to keep the Government informed of progress, risks, and financial status.
- **Quality and Resource Management**: Ensure all project activities and deliverables meet the quality standards defined in this PWS and the individual PMP. The contractor shall manage all technical and personnel resources assigned to the project to ensure effective and efficient execution.
- **Project Transition**: The Contractor shall ensure a formal transition from the project team to the Operations and Maintenance (O&M) team. A project will not be considered complete until the Government accepts all final deliverables, including Transition Documentation. This documentation must include, at a minimum, any Standard Operating Procedures (SOP), "as-built" diagrams, and any relevant configuration files or technical manuals required for successful sustainment of the new implementation.
- **Project Closure**: Upon project completion, the contractor shall conduct a formal closure process. This includes verifying that all objectives have been met, all deliverables have been accepted by the Government, and all project documentation is finalized and archived in a project repository.

DELIVERABLE(S):

- Project Management Plan
- Integrated Master Schedule (IMS)
- Weekly Project Status Report
- Project Transition Documentation
- Project Closure Report

1.3.3 **Engineering Projects**

This section defines the formal process for executing new projects and implementing new capabilities that are outside the firm-fixed-price (FFP) Operations & Maintenance (O&M) scope of this FPTS contract. All such work shall be initiated through the development of a Technical Solution Identification (TSI) document. The TSI will serve as the basis for a potential Government Request for Proposal (RFP), to which the Contractor shall respond with a detailed FFP proposal. If accepted, the work will be authorized via a separate formal Task Order. To be considered an eligible project requiring a TSI and separate funding, a proposed effort must be a discrete, non-recurring activity that meets one or more of the following criteria:

1. Introduction of new services, modernized technology, or capabilities: The project delivers a new functional service that is not currently provided or described within the scope of this PWS.
    - *Example:* Implementing a new cloud-based data analytics platform; deploying a new mobile application for field agents.
2. Addresses a New Strategic or External Mandate: The project is required to comply with a new or unplanned Presidential, Federal, DoW, DISA, or agency-level directive, policy, or security mandate that was not in effect at the time of contract award.
    - *Example:* Engineering a solution to comply with a new Zero Trust Architecture (ZTA) implementation mandate.
3. Involves Significant Re-architecture or Integration: The project requires a fundamental change to the existing enterprise architecture or involves complex integration with a new, external third-party system.
    - *Example:* Migrating a legacy, on-premise application to a government-approved cloud environment (IaaS/PaaS)

For the avoidance of doubt, the personnel and labor hours needed to execute the following activities are considered part of the firm-fixed-price O&M services for this contract and do not qualify as projects. The vendors cost for the following work shall be included in the TO2 proposal.

Life Cycle Replacement (LCR): The planned refresh and replacement of each component in Appendix A LSB Infrastructure, to include workstations, servers, network devices, and other IT assets as they reach end-of-life or end-of-support no more than once per device throughout the length of this contract.

1. Life Cycle Replacement of existing hardware or software assets as defined in the contractor's Technology Refresh Plan, regardless of the number assets involved.
2. Routine Sustainment and Maintenance: All activities associated with the ongoing management of the existing environment, including patching, configuration changes, user account management, system monitoring, and break-fix support.
3. Incremental Feature Updates: Minor enhancements, or configuration changes to existing systems that do not introduce a new capability.
4. Efforts to Meet Existing Service Level Agreements (SLAs): Work performed to correct performance deficiencies or to bring a service back into compliance with the performance metrics defined in Technical Exhibit 1.

DELIVERABLE(S):

- Technical Solution Identification (TSI) recommendations with a rough estimate on cost to implement submitted to COR and Government Lead.

1.3.4 **Pending Modernization Projects**:

Upon Task Order Award, the Contractor shall review and validate the existing project Technical Solution Implementations (TSI's) documents for projects that have not yet been awarded. For each TSI, the Contractor shall deliver a Project Validation Briefing (PVB), either concurring with the existing approach or providing a formal recommendation for an alternative solution, including a justification for the change. Upon completion of the Project Validation Briefing, the Government will decide a way forward

DELIVERABLE(S):

- Project Validation Briefings

1.3.5 **Operations and Maintenance (O&M)**:
The Contractor shall provide all personnel, processes, and tools required to deliver comprehensive Operations and Maintenance (O&M) for the Pentagon Force Protection Agency Platform as a Service (PaaS) environment. The Operations and Maintenance (O&M) team is responsible for the complete lifecycle of services required to ensure the availability, integrity, and security of the LSB system, its network, and all capabilities that support the PFPA mission. The Contactor shall provide O&M services necessary to ensure the LSB Platform and Mission Systems are resilient, secure, and continuously available. The architecture must be sustained to exhibit key attributes including, but not limited to, built-in redundancy, automatic failover, and fault tolerance. To achieve this, the Contractor is responsible for the complete management of, at a minimum, the following core service areas:

- **System & Network Administration**: Full lifecycle management of all physical and virtual servers, network devices, and operating systems.
- **System & Network Monitoring**: Continuous monitoring of all infrastructure and services to proactively detect, analyze, and respond to alerts and performance degradation. Monitoring will be done via applications and personnel. While on-site support is not 24x7, applications, such as Solarwinds will monitor the infrastructure by the Security Control Center through TO1 personnel. Response for incidence found shall meet the SLA requirements of this PWS.
- **Patching & Updates**: A comprehensive program for testing and deploying all required security patches, updates, and configuration changes to all systems and applications.
- **Data Management & Protection**: Execution of all data backup, restoration, and archival procedures to ensure data integrity and recoverability.
- **Lifecycle Management**: Proactive identification and notification of all hardware and software approaching end-of-life or end-of-service.
- **Tiered Service Desk Support**: Providing Tier 2 and Tier 3 incident response and service request fulfillment.

For the avoidance of doubt, the O&M responsibilities in this section do not include the day-to-day operational support, systems administration, or database administration for the applications hosted on the DISA J6 NIPR network. These operational duties are managed by other entities, however the cybersecurity responsibilities for these applications are defined in the Cybersecurity section of this contract.

1.3.6 **Operations and Maintenance Staffing and Availability**:

Staffing and Expertise:
The Contractor shall provide a properly skilled and trained workforce to perform all O&M services required by this PWS. The O&M team shall be composed of personnel with demonstrated advanced knowledge and experience supporting an IT infrastructure of similar size and complexity to the LSB.

Hours of Operation and Support Posture:
The Contractor shall provide support services aligned with the following schedule:

1. **On-Site Support**: The Contractor shall provide on-site O&M personnel during core business hours, defined as 0600 to 1800, Monday through Friday, excluding Federal holidays. The primary work location will be the Suffolk Bldg., 6th & 7th Floor, Falls Church, VA
2. **On-Call Support**: Outside of core business hours, the Contractor shall provide an on-call rotation of qualified Tier 2/3 personnel available 24 hours per day, 7 days per week, 365 days per year.
3. **Service Desk Escalation**: The Contractor shall serve as the Tier 2/3 escalation point for all tickets routed from the DISA J6 Tier 1 Service Desk related to the LSB Platform and its applications.

1.3.7 **System Availability and Resiliency**
The Contractor shall operate and maintain the LSB environment to ensure the highest levels of system availability and resiliency for the PFPA Mission.

Requirements: Availability
The Contractor shall be responsible for meeting or exceeding the uptime targets defined in the Performance Requirements Summary (PRS). These targets, not including scheduled maintenance approved by the Government in advance, are the official measure of performance.

System Resiliency
The Contractor is responsible for operating and maintaining all existing resiliency features within the LSB architecture (e.g., executing failover procedures, managing redundant components). This responsibility does not include the architectural redesign or engineering of new resiliency capabilities into the Government-

Furnished environment. Any effort to engineer new resiliency features shall be considered a new requirement eligible for the TSI process defined in Section 2.2

1.3.8 **System and Service Monitoring**:
The Contractor shall be responsible for the continuous monitoring of the health, performance, and security of the entire LSB Systems Architecture. The primary goal of this function is the proactive detection of events that could lead to service degradation or an outage.

Core Responsibilities:

- The Contractor shall actively monitor all alerts and events using the suite of Government-provided monitoring tools (e.g., SolarWinds).
- The Contractor shall analyze all alerts to determine their priority and potential impact on mission services.
- Upon identifying a qualified incident, the Contractor shall immediately initiate the Incident Management process as defined in the Incident Management section (1.3.9) of this PWS.

Performance Standard:

- All "critical" or "down" alerts generated by the monitoring system must be acknowledged by the Contractor, both in the monitoring tool and by creating a corresponding incident ticket, within 15 minutes of the alert's generation. The "start time" for this 15-minute requirement is defined differently based on the time of day.
    - During Core Business Hours (0600-1800 M-F): The clock starts at the moment a "critical" or "down" alert is generated by the Government's monitoring tool.
    - Outside of Core Business Hours: The clock starts at the moment the Contractor's on-call representative receives a direct verbal notification (i.e., a phone call) from the DISA J6 Service Desk or another designated 24/7 Government entity.

Tool Management:

- The Contractor shall be responsible for the basic administration and maintenance of the Government-provided monitoring tools, including ensuring all in-scope assets are correctly configured to report to the system. The Contractor shall document and report any discovered inaccuracies in accordance with the Asset Management Section.

1.3.9 **Incident Management and Response**:
The purpose of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on the PFPA mission. The Contractor shall be responsible for the full lifecycle of incident management for all in-scope systems.
The Contractor shall adhere to the following process and performance standards:

Incident Detection and Acknowledgement:

- The Contractor shall continuously monitor all systems for alerts that may signify an actual or potential incident or unauthorized access.
- The Contractor shall formally acknowledge all new incidents—whether received from a monitoring alert or as an escalation from the DISA J6 Service Desk—within fifteen (15) minutes of notification.

Initial Response and Triage:

- Immediately upon acknowledgement, the Contractor shall triage the incident to determine its priority level (Mission Critical, Mission Essential, Mission Support) in accordance with the definitions in the IT Environment Document (Appendix B).
- For any incident categorized as Mission Critical, or any incident projected to have widespread impact, the Contractor shall notify the designated Government On-Call Manager within 30 minutes of acknowledgement. This initial notification shall consist of both a direct phone call to establish immediate awareness and a follow-up email to document the event.

After-Hours Incident Response Process:
The Contractor shall provide an on-call rotation of qualified Tier 2/3 personnel to respond to critical after-hours incidents. Due to the requirement for all system management to be performed on-site, the after-hours response process shall adhere to the following multi-stage Service Level Agreement (SLA):

Stage 1: Initial Notification and Verbal Acknowledgement

- The after-hours response process is initiated only by a direct phone call from a designated 24/7 Government entity (e.g., DISA J6 Service Desk, Pentagon Operations Center) to the Contractor's on-call representative.

- The Contractor shall provide verbal acknowledgement of the notification by answering the call and confirming receipt of the incident details within 15 minutes of the initial call.

Stage 2: On-Site Arrival

- Upon verbal acknowledgement of a Mission Critical incident, the on-call representative shall immediately begin procedures to deploy a technician to the required on-site location.
- A qualified Contractor technician shall arrive on-site and be prepared to begin work within 90 minutes of the initial verbal acknowledgement.

Stage 3: Technical Engagement and System Acknowledgement

- Within 15 minutes of arriving on-site, the Contractor technician shall log into the necessary systems.
- The technician will then perform the first technical actions: formally acknowledging the corresponding alert in the monitoring tool (if applicable) and updating the service management ticket to reflect that work has begun on-site.

Summary of After-Hours Critical Incident SLA:

Action	Requirement	Maximum Time
Verbal Acknowledgement	Contractor answers phone and confirms receipt	15 minutes (from initial call)
On-Site Arrival	Technician arrives at the physical work location	90 minutes from verbal acknowledgement
Technical Engagement	Technician logs in and updates system/ticket	15 minutes (from on-site arrival)

Service Restoration:

- The Contractor shall take all necessary actions to resolve the incident and restore normal service. All restoration efforts must meet the specific time-to-resolve targets defined for each priority level in the Performance Requirements Summary (PRS).

Communication and Escalation:

- Throughout the lifecycle of an incident, the Contractor shall provide regular status updates to the Government throughout the lifecycle of an incident. All updates shall be documented in the corresponding service ticket and through a SITREP email notification. The minimum required frequency is determined by the incident's priority level:
  - Mission Critical – Every 60 minutes until service is restored
  - Mission Essential and Mission Support – Every 4 hours during core business hours until service is restored.
- The Contractor shall immediately notify the Government if it is anticipated that the time-to-resolve target for an incident will be breached.

Post-Incident Activity:

- The Contractor is responsible for documenting all activities performed during the incident in the corresponding service ticket.
- Following any incident resulting in a service outage exceeding the response posture times defined within the Environment document, the Contractor shall deliver an AAR within three (3) business days of service restoration. The report shall detail the event timeline, root cause analysis, lessons learned, and a list of actionable follow-up items to prevent recurrence

Process Improvement:

- The Contractor shall follow the current Incident Management SOP. Within 90 days of contract award, the Contractor shall deliver an assessment of this SOP, providing any recommendations for improvements to streamline and improve the incident response process.

DELIVERABLE(S):

- After-Action Report (AAR)
- Incident Management SOP Assessment

1.3.10 **Tiered Support Structure**:

The Contractor shall provide Tier 2 and Tier 3 support for all incidents and service requests related to the LSB environment and its Mission Applications. The support structure is defined as follows:

Tier 1 (DISA J6 LSB Service Desk):
Tier 1 is responsible for initial incident intake, basic diagnostics, and resolving common, well-documented issues within their area of responsibility. The Tier 1 Service Desk will escalate all other incidents to the FPTS Contractor's Tier 2 team.

Tier 2 - Technical Support (Contractor Responsibility):
The Contractor's Tier 2 team shall serve as the primary escalation point for all technical issues. This is a "hands-on" support tier. Responsibilities include, but are not limited to:

- Performing detailed diagnostics on incidents escalated from Tier 1.
- Resolving all server and workstation hardware and software issues.
- Executing system re-imaging, software installations, and approved configuration changes.
- Fulfilling standard service requests (e.g., account creations, permissions changes).
- Providing "remote hands" support for network and cybersecurity teams as needed.
- Escalating complex, systemic, or novel issues to Tier 3.

Tier 3 - Engineering & Advanced Support (Contractor Responsibility):
The Contractor's Tier 3 team shall consist of senior engineers and subject matter experts (SMEs) who handle the most complex issues. This tier is focused on problem resolution and architectural stability. Responsibilities include, but are not limited to:

- Troubleshooting complex issues requiring deep architectural knowledge (e.g., cross-domain integration problems, systemic performance degradation).
- Performing root cause analysis (RCA) on major or recurring incidents.
- Developing and testing solutions for novel problems for which no SOP currently exists.
- Liaising with OEM vendors to resolve bugs in hardware or software.
- Providing expert consultation to the Government and other project teams as needed.

1.3.11 **End User Service Requests:**
The Contractor shall be responsible for fulfilling all authorized service requests and performing standard operational tasks. All work performed shall be tracked via a ticket in the Government-provided service management system.

Scope of Standard Service Requests (O&M):
The following activities are considered routine and are included within the scope of firm-fixed-price O&M services:

- Workstation & Peripheral Support: Deployment, configuration, or removal of workstations and peripherals for individual users or groups.
- Account Management: Creation, modification, and deletion of all user accounts.
- Software Installation: Installation or removal of approved baseline applications on individual workstations.

Image Management:
The Contractor shall create, test, and manage the deployment images for all server, workstation, laptop, and tablet assets. All images will be built using the latest approved DoD Secure Host Baseline (SHB) repository, configured for the LSB environment, and must receive Government approval prior to use in production.

Transition Support:
The Contractor shall participate in Change and Release Management activities by providing technical support for the transition of new services into the production environment. The Contractor's specific duties and level of effort for each transition will be defined within the Government's formal Change Management Plan for that release.

1.3.12 **Access Management**:
The Contractor shall manage the full lifecycle of user and privileged account access for all in-scope LSB systems and applications. All access management activities will be performed in accordance with Government-provided policies and procedures.
The Contractor's responsibilities shall include, at a minimum:

- Account Administration: Creating, modifying, disabling, and deleting all user accounts as required by policy or in response to authorized Government service requests. All account administration tasks shall be completed within the timelines specified in the Performance Requirements Summary (PRS).
- Order, receipt, and delivery of LSB token to users for access.
- Privilege and Rights Management: Maintaining an accurate registry of user rights and privileges within Active Directory and other applicable systems, ensuring adherence to the principles of least privilege.
- Audit Log Management: Ensuring that all systems are configured to generate auditable records of access attempts and providing these logs to authorized Government personnel upon request.

- Access Incident Response: Detecting and responding to any instances of unauthorized access in accordance with the incident response procedures outlined in the Incident Management and Response section.
- Access Control Audits: Performing a documented audit of all privileged user accounts on a quarterly basis to validate that access is still required and appropriate. A summary of this audit's findings shall be included in the Monthly O&M Performance & Health Report.

1.3.13 **Security Patching and Vulnerability Management:**
The Contractor shall execute a comprehensive Security Patching and Vulnerability Management program to maintain the security posture of the LSB architecture. The Contractor is responsible for the full lifecycle of vulnerability remediation, from identification and testing to deployment and verification. The Contractor's performance will be measured against the specific compliance metrics defined below.

Core Performance Metrics:
- Credentialed Scan Rate: The Contractor shall maintain a credentialed scan success rate of 98% or greater for all in-scope assets as measured by ACAS.
- CCRI Score: The Contractor shall maintain a Command Cyber Readiness Inspection (CCRI) Weighted Average Score of 2.5% or lower for all in-scope systems as defined in the IT Environment Document.

Performance Standards and Timelines:
To achieve the above metrics, the Contractor shall remediate all identified vulnerabilities according to the following Government-mandated timelines, unless a different timeline is specified by a superseding directive (e.g., a USCYBERCOM order):
- Critical Risk Vulnerabilities: Remediate within 14 calendar days of discovery or vendor patch release.
- High Risk Vulnerabilities: Remediate within 30 calendar days of discovery or vendor patch release.
- Medium Risk Vulnerabilities: Remediate within 90 calendar days of discovery or vendor patch release.

Core Responsibilities:
To meet these requirements, the Contractor's duties shall include, but are not limited to:
- Continuously monitoring all applicable security sources (e.g., USCYBERCOM, DISA, OEM vendors) for vulnerability announcements, IAVMs, and security directives relevant to the LSB environment.
- The Contractor shall deploy, manage, and monitor enterprise patch management tools (e.g., SCCM, MECM) to automate patch deployment wherever possible.
- The Contractor shall test all patches and configuration changes prior to production deployment to ensure they do not adversely affect mission system functionality.
- The Contractor shall ensure all systems are hardened and configured in accordance with the latest applicable DISA Security Technical Implementation Guides (STIGs).

Reporting and Verification:
The status of all metrics defined in this section (Scan Rate, CCRI Score, and remediation timelines) shall be reported in the Monthly O&M Performance & Health Report. This report shall include, at a minimum, overall patching compliance rates, the status of any overdue vulnerabilities, and a Plan of Action & Milestones (POA&M) for each.

1.3.14 **System Backup and Restoration**:
The Contractor shall provide comprehensive Backup and Restoration services to ensure the integrity and availability of all in-scope LSB data.

Plan Management and Review:
- Within 30 calendar days of contract award, the Contractor shall review the existing Government-provided Backup and Restoration Plan and deliver a Backup Plan Assessment Report. This report shall either validate the current plan's adequacy or provide specific, actionable recommendations for improvement.
- The Contractor shall maintain and execute all backup and restoration activities in accordance with the final, Government-approved plan

Core Responsibilities:
- Execute all scheduled daily system backups (full and incremental) and verify their successful completion.
- Perform data and system restorations in response to authorized Government requests, meeting the recovery time objectives defined in the PRS.

- The Contractor's responsibility is strictly limited to the systems and data defined in the IT Environment Document. Support for systems managed by Other Government Agencies (OGAs) or Contractors (OGCs) is not included in the scope of this PWS.

Restoration Testing:

- The Contractor shall perform a documented data recovery test on a quarterly basis. The test shall validate the integrity of the backup media and the viability of the restoration process.

Reporting:

- The Contractor shall configure the backup system to provide automated email alerts directly to the Government for any backup job failures.
- A summary of backup performance, including the overall success rate, details on any failures, and a summary of the quarterly restoration test results, shall be included in the Monthly O&M Performance & Health Report.

DELIVERABLE(S):

- Backup Plan Assessment Report (One-time, 30 days after award)
- Quarterly Data Recovery Test Results

1.3.15 **Failover Testing**:

The Contractor shall plan, execute, and document a failover test of the LSB environment's primary resiliency features on a quarterly basis. The purpose of this test is to validate the functionality of all automated and manual failover mechanisms and to verify that Mission Critical systems remain available during a simulated site failure. A Quarterly System Failover Test Report shall be delivered to the Government no later than five (5) business days after the completion of the test. The report must contain:

- Executive Summary
- Test and Plan Objectives
- Execution
- Chronological Log of actions
- Test Results and Performance Metrics
- Findings and Recommendations

DELIVERABLE(S):

Quarterly System Failover Test Report

1.3.16 **Event Management**:

Event Management is the process of planning for, coordinating, and providing support to planned activities that may impact the LSB IT infrastructure. This includes, but is not limited to, Authorized Service Interruptions (ASIs) from DISA J6, building-wide power outages managed by PBMO, Government-led Integrated Systems Tests (ISTs).

Baseline Support (Firm-Fixed-Price):

The Contractor shall provide resources to support a baseline level of planned event activity as part of its firm-fixed-price services. This baseline is defined as a total of 10 events (each lasting a full day up to 10 hours) per contract year of event support occurring outside of core business hours. The Contractor shall track all such hours and report them in the Monthly O&M Performance & Health Report.

Surge Support (Over and Above):

Should the Government's requirement for event support exceed the 10 event annual baseline, the COR may authorize additional support. This "surge" support may be funded either through a separately priced Labor-Hour CLIN (if available) or as a new requirement via the TSI process. The Contractor shall not perform work exceeding the annual baseline without prior written authorization from the COR.

Contractor Responsibilities:

- Act as the central point of coordination for all planned technical events affecting the LSB.
- Ensure Government stakeholders are notified of upcoming events, their potential impact and risks.
- Generate and update a “Runbook” identifying actions for graceful shutdown and restorations of services
- Develop contingency and roll-back plans for major technical events.
- Schedule and provide the necessary technical personnel to support the execution of the event.

1.3.17 **Asset Management and Logistics Management**:

The Contractor shall provide comprehensive IT Asset Management (ITAM) and logistics services for all in-scope LSB hardware and software, from initial receipt to final disposal.

Asset Tracking System of Record:

- The Contractor shall use the Government-provided Enterprise Logistics Management System (ELMS) as the single, authoritative system of record for all IT assets. All assets shall be tracked electronically in ELMS, and data shall not be maintained in standalone spreadsheets or databases.

Core Responsibilities:

- Receiving and In-processing: The Contractor shall be responsible for the full in-processing lifecycle of all new IT assets. This includes coordinating with the DISA J4 Asset Management team to schedule and conduct joint receiving activities. Within two (2) business days following a joint session with the DISA J4 team where new assets are inspected and approved, the Contractor shall complete all subsequent tasks, including affixing asset tags and entering all required attributes into ELMS.
- Contractor-Acquired Property: In cases where the Contractor is directed to purchase equipment or software on behalf of the Government through a separately funded Task Order or project, all such items are considered Contractor-Acquired Property (CAP). The transfer of title for CAP to the Government shall be handled in strict accordance with Federal Acquisition Regulation (FAR) 52.245-1, Government Property.
    - Inspection and Acceptance: Upon receipt of CAP, the Contractor shall prepare and submit a DD Form 250, Material Inspection and Receiving Report, to the designated Government representative for inspection and formal acceptance.
    - Title Transfer: Title for the property shall officially pass to the Government only upon the signature and acceptance of the DD Form 250 by an authorized Government official.
    - In-processing: Following Government acceptance via the signed DD Form 250, the Contractor shall then follow the standard in-processing procedures as defined in this section to tag the asset and enter it into the ELMS system of record.
- **Logistics and Transportation:** Manage the physical storage and transportation of IT assets between Government facilities within the NCR. The Contractor shall provide their own vehicle for transportation.
- **Disposal Preparation:** Process all end-of-life assets for disposal including data sanitization in accordance with DoD 5220.22-M and NIST SP800-88 standards, preparing all necessary documentation for turnover to the Defense Reutilization and Marketing Office (DRMO) in accordance with DoD and PFPA policy, and physically preparing and transporting the assets to the designated DRMO collection point in accordance with all applicable PFPA and DoW policies.
- **License Management:** Maintain a complete inventory of all Commercial off the shelf (COTS) and Government off the shelf (GOTS) software licenses, including quantities, expiration dates, and renewal information. This inventory shall be delivered as a formal report within 90 days of award and updated annually thereafter.

Inventory and Verification:

- The Contractor shall conduct a full 100% wall-to-wall inventory of all IT assets annually, to be completed no later than August 31st.
- To support this annual requirement, the Contractor shall perform a cyclical inventory count, auditing approximately 25% of the asset baseline each quarter.
- The results of all inventory activities, including a list of any discrepancies found and their resolution status, shall be summarized in the Monthly O&M Performance & Health Report.

Planning and Process Documentation:

- Asset Management SOP: The Contractor shall review the existing property accountability procedures and deliver a consolidated Asset Management SOP within 90 days of award. This SOP shall document all processes for receiving, tracking, inventorying, and disposing of assets.

DELIVERABLE(S):

- Asset Management SOP (One-time, 90 days after award)
- Initial Software License Report (One-time, 90 days after award)
- Annual Software License Report
- Annual 100% Inventory Report

1.3.18 **Technology Refresh and Lifecycle Management**:

The Contractor shall be responsible for the complete lifecycle planning and execution of technology refresh activities to ensure the LSB environment remains modern, supportable, and cost-effective.

Technology Refresh Plan:

The Contractor shall develop, maintain, and deliver annually a Technology Refresh Plan. This plan is the foundational document for all LCR activities and must identify all major hardware and software components, their expected end-of-life dates, and a proposed, prioritized replacement schedule for the upcoming years through the length of this contract. This includes the life cycle replacement (LCR) of workstations, servers, network devices,

PaaS, and other IT assets described in the Appendix A Systems and Devices LSB Infrastructure tab as they reach end-of-life or end-of-support no more than once during the length of this contract. The Contractor will provide labor to support the LCR of the above components in this proposal and those mentioned in the Systems and Devices Appendix Tab 18 LSB Infrastructure. Material will be purchased by a separate task order.

Scope of Execution:
The execution of the Government-approved Technology Refresh Plan, including the physical replacement of workstations, servers, network devices, and other assets as they reach end-of-life, is a required activity. For the avoidance of doubt, all activities defined within the approved Technology Refresh Plan are considered part of the firm-fixed-price O&M services and shall not be billed as separate projects.

DELIVERABLE(S):
- Annual Technology Refresh Plan

1.3.19 **System Diagrams and Documentation**:
The Contractor shall create, maintain, and manage a complete and accurate set of technical documentation for the LSB Systems Architecture, including but not limited to network diagrams, server rack elevations, data flow diagrams, and hardware/software lists.
Event-Driven Updates:
The Contractor shall update all relevant "as-is" diagrams and documentation within ten (10) business days following the closure of any Change Request or project that alters the production environment's configuration, architecture, or inventory.
Annual Baseline Delivery:
The Contractor shall perform a full review of all documentation annually. Following this review, the Contractor shall deliver a complete, consolidated set of the current baseline documentation to the Government. This delivery shall occur no later than the end of the first quarter of each contract option year.
Format and Accessibility:
All documentation shall be maintained in a Government-accessible electronic repository (e.g., SharePoint) in standard, editable formats (e.g., Microsoft Visio, Word, Excel). The Contractor shall also provide large-format, plotter-sized prints for display in Government operations centers upon request.

DELIVERABLE(S):
- Event-Driven Updated Technical Documentation
- Annual Baseline Documentation Set

1.3.20 **O&M Standard Operating Procedures (SOP) and Work Instructions (WIs)**: The Contractor shall create SOPs and WIs for new, revised, or missing requirements; ensure continuous review and maintenance of all O&M SOPs and WIs to ensure content remains current; and accurate.
The Contractor's Operations and Maintenance (O&M) team shall be the central owner and custodian of all Standard Operating Procedures (SOPs) and Work Instructions (WIs) related to the operational environment.
Responsibilities shall include:
- Transition from Engineering: Taking ownership of the " Operations and Maintenance SOPs" delivered by the engineering team at the conclusion of each project.
- Continuous Review and Updates: Reviewing and updating all existing documentation on at least an annual basis to ensure it remains current, accurate, and reflective of the production environment.
- As-Needed Creation: Developing new SOPs or WIs as required for existing processes that are found to be undocumented or have changed over time due to system modifications or new operational requirements.
- Centralized Repository: Maintaining a single, authoritative, and government-accessible repository (e.g., SharePoint) for all operational documentation.

DELIVERABLE(S):
Annual Documentation Review Report: A report submitted annually to the Government certifying that all documentation has been reviewed and updated, noting any major changes.

1.3.21 **Operations and Situational Reporting**
The Contractor shall keep the Government informed of the operational status of the LSB environment through a combination of routine check-ins and event-driven situational reports. This approach is designed to provide timely, relevant information to leadership without creating unnecessary administrative overhead.
Routine Operations Check-in:

- The Contractor shall participate in a brief Operations Synchronization Meeting with Government leads at 0730 on Mondays and Thursdays.
- To support this meeting, the Contractor shall present a single-page "Ops Sync" briefing slide. This slide shall provide a high-level visual summary of key activities and statuses since the last meeting.
- The content of the slide is meant to be a conversation starter and shall include, at a minimum:
- Status of any significant ongoing incidents.
- Key accomplishments completed (e.g., major tickets closed).
- A look-ahead at major planned activities for the next 48-72 hours (e.g., scheduled changes, patching windows).
- This briefing slide is considered a meeting artifact, not a formal, archival deliverable.

Consolidation of Data:
All routine operational metrics, including ticket statistics, system health, and planned activities, will be documented and delivered in the Monthly O&M Performance & Health Report.

MEETING(S):
- 0730 Operations Synchronization Meeting (Mondays and Thursdays)

1.3.22 **Monthly Performance and Health Reporting**
The Contractor shall provide a comprehensive Monthly Operations and Maintenance (O&M) Performance & Health Report. This report shall consolidate all key performance metrics and operational data into a single, cohesive document. It serves as the primary formal mechanism for the Government to assess the overall health of the LSB environment and the contractor's performance against the standards set forth in this PWS.
This single monthly report replaces the need for separate, ad-hoc reports on topics such as daily backups, weekly patching, or daily operations. It is intended to provide a trend-based, analytical view of performance.
Submission and Review:
- The report shall be delivered to the Government no later than the 5th business day of the month following the reporting period.
- The contents of this report will be a primary topic of discussion during the Monthly Program Management Review (PMR).

Required Content:
The Monthly O&M Performance & Health Report shall include the following sections at a minimum:
1. Executive Summary: A high-level dashboard view of the reporting period, including an overall status (Green/Yellow/Red), a summary of major accomplishments, and a brief description of any significant challenges or major incidents.
2. Service Availability: A summary of system availability metrics, measured against the targets defined in the Performance Requirements Summary (PRS), with details on any unplanned outages.
3. Incident Management Summary:
    - Statistics for the period (e.g., number of P1, P2, P3 incidents opened vs. closed).
    - A summary of all After-Action Reports (AARs) completed during the month.
    - Analysis of any recurring incidents that may indicate an underlying "Problem" requiring root cause analysis.
4. Security and Compliance Posture:
    - Current Credentialed Scan Success Rate (as a percentage).
    - Current CCRI Weighted Average Score.
    - Summary of patching compliance, including the total number and age of any overdue Critical or High vulnerabilities, along with their associated POA&Ms.
5. System Health and Resiliency:
    - A summary of backup performance, including the overall job success rate and details on any critical backup failures and their resolution.
    - A summary of the results of any Data Recovery or Failover Tests conducted during the reporting period.
    - Analysis of system capacity and performance trends (CPU, memory, disk), highlighting any systems projected to exceed 85% utilization within the next 90 days.
6. Event Management:
    - A log of all planned events supported during the period (e.g., ISTs, power downs).

- An accounting of the "Baseline Support" hours consumed during the month and the cumulative total for the contract year.

DELIVERABLE(S):

- Monthly O&M Performance & Health Report

1.3.23 <u>Pentagon Shield/C-sUAS/MMS Cybersecurity and Operating System (OS) Sustainment Support:</u>
The Contractor shall perform services, in coordination with the PFPA CPD CBRN Systems Branch, to maintain cyber security compliance, operating system functionality, network configuration, as necessary, to sustain connectivity and system operations.

- The Contractor shall perform cyber security scanning, monitoring, patching, updates, and upgrades for the devices to maintain a CCRI score below 2.50 for those devices lists in Systems and Devices Appendix A, System Devices Overview, as having a non-proprietary operating system; valid exceptions (e.g., a score above 2.5 due to extended mitigation requirement in the case of a Microsoft driven "bad patch") shall be brought to the COR upon identification of issue. The CCRI score shall be reported weekly as part of the ISSC Task Order 2 FPTS standard CCRI Scorecard report distribution.
- The Contractor shall maintain a 98% or greater credentialed scan rate for devices with an OS, as identified in Systems and Devices Appendix A. The credentialing percentage shall be reported as part of the ISSC Task Order 2 FPTS standard CCRI Scorecard report distribution.
- The Contractor shall conduct routine twice-weekly ACAS scans on network connected systems to identify operating system/software application vulnerabilities; non-network connected systems shall be scanned every other week and shall require the system Functional/Application Technical Point of Contact (TPOC) to be present.
- The Contractor shall participate in the FPTS Vulnerability Management Program and perform remediation in accordance with the distributed Vulnerability Plan of Action (POA).
- The Contractor shall execute automatic and manual DISA STIG implementation and documentation for all servers and devices; STIG remediation and documentation include but are not limited to the following when they are on ISSC servers: IIS and Web Server STIG; Application STIG; Microsoft SQL Server STIG; Redhat Server STIG. STIGS should be maintained in accordance with individual STIG frequency.
- The Contractor shall conduct routine semi-annual SCAP scans to validate operating system/software application STIG compliance.
- The Contractor shall perform operating system maintenance for CPD systems connected to the LSB network and virtual lab to include installation, updates, patching, upgrades, and troubleshooting in accordance with devices identified as having an OS in Systems and Devices Appendix A; supporting activities include:
- Implement operating system updates to unsupported/vulnerable operating systems identified for upgrades in ACAS scans for compatible hardware.
- Implement non-mission application software (e.g., Tumbleweed, Google Chrome, etc.) updates to unsupported/vulnerable software applications identified for upgrade in ACAS scans; applied IAW with CYBERCOM/JFHQDODIN/DISA specified orders or IAVA notifications prior to suspense date.
- Validate implementation of operating system software patches before equipment (pre-production) is added to network and apply monthly updates and necessary.
- The Contractor shall implement weekly antivirus signature updates released by DISA.
- The Contractor shall perform network configuration activities to connect, troubleshoot, and repair network connections related to both configuration and physical network connectivity for all devices listed in Systems and Devices Appendix A.
- The Contractor shall support CPD in the JSP Standard Product List (SPL) approval process, including actions such as Business Requirement Document (BRD) development and JSP ticket submission/tracking.
- The Contractor shall respond to requests for service within three (3) hours for routine issues, and (1) hour for critical issues during regular weekly business hours (Monday through Friday 0600 to 1700).
- The Contractor shall respond to requests for service within twenty-four (24) hours for routine issues and six (6) hours for critical issues outside of normal weekly business hours (Monday through Friday 1700 to 0600) and weekend hours (Friday 1700 through Monday 0600).
- The Contractor shall support development of Plan of Actions & Milestones (POAMs) in support of system accreditation and Acceptance of Risk (AOR) exception requests; POAMs

and AORs shall be created in accordance with the latest JSP POAM Standard Operating Procedure (SOP) and AOR guidance/form.

- The Contractor shall provide OS-related support to the JSP Risk Management Framework (RMF) system accreditation process to achieve/maintain JSP Authorizing Official (AO) approval and Authority to Operate (ATO); support includes providing required ACAS and SCAP scans, providing compelling evidence to support cybersecurity control implementation/compliance, and developing and/or contributing to RMF artifact development (Ports, Protocols, and Services; Data Call [asset baseline audit] and Hardware-Software Lists; System Design Documentation; System Architecture; System Security Categorization; Privacy Impact Assessment; System Security Plan; Information Security Contingency Plan). This support shall be delivered in accordance with the agreed upon RMF Project Management Plan and JSP RMF multi-step submission process; it will also be done in coordination with the FPTS assigned Information System Security Officer (ISSO) and CPD's assigned system functional/application Technical Point of Contact (TPOC). RMF support shall be provided on a yearly cycle.

- **Laboratory Information Management Systems (LIMS)** – Monitor Only. The Contractor shall perform cyber security scanning and reporting of cyber security status for LIMs.
- The Contractor shall conduct cyber security scans at weekly intervals and report the findings to the CPD Laboratory for appropriate action to ensure compliance with cyber security requirements.

- **MMS Cloud Services Support.** The Contractor shall provide services necessary for MMS Cloud Support/Administration and Network Administration: Cloud Support/Administration:
- The Contractor shall provide account management of cloud environments.
- Create Contractor accounts for hosted application administrators
- Configure Multi-factor Authentication via smartphone app (e.g., Google or Microsoft) for account access.
- Remove accounts that are no longer required by app administration team.
- Manage and maintain Virtual Private Cloud (VPC) in support of application functionality (Applicable to all environment types VPC=AWS, VNet= DISA Stratus, etc.).
- Deploy hardware-based/virtual servers in support of system and application requirements.
- Configure account access.
- Enable Role Based Access Control (RBAC) model for LSB Domain attached systems.
- Configure console access for cloud-based systems requiring browser enabled access.
- Configure network access, employing assigned IP addresses, FW rulesets, and security groups.
- Employ configuration management best practices to include required documentation and disaster recovery processes.
- Assist application administrator with disaster recovery operations when restoration of the environment is called for.
- Network Administration
- Provide transport within Coral or from Coral to cloud-based enclaves as necessary.
- Communicate requirements to JSP F5 admins for DMZ traversal.
- Submit and track FW rulesets required for application functionality.
- Manage and maintain required IP space, subnets, route-tables, Internet gateways.
- Manage and maintain hardware-based or virtual router and/or FW instances supporting network access.
- Configure account access.
- Employ configuration management best practices to include required documentation and disaster recovery processes.
- Apply security focused STIGs and patches.
- Update network OS images as required.
- Assist application administrators in developing/employing security groups allowing only required ports and protocols from approved sources and destinations.

1.3.24 The Contractor shall develop and maintain a network Virtual Test Environment on the LSB to which operable spare devices will be connected to ensure sustainment of cyber security patches and testing of patches and updates on test devices to ensure functionality. The Government will

supply a space for the physical connection of spare devices. JSP will supply network connections to the identified space; this will be coordinated through CPD.

- Operational spare devices consistent with systems identified in Appendix A Systems and Devices Tab 17 CBRNE Systems shall be connected to the LSB Test Environment and the Contractor shall perform cyber security scanning, monitoring, patching, updates, and upgrades for the connected devices at weekly intervals to maintain a CCRI score below 2.50; valid exceptions (e.g., a score above 2.5 due to extended mitigation requirement in the case of a Microsoft driven "bad patch") shall be brought to the COR upon identification of issue.
- The Contractor shall scan, patch, and update non-operational spares once they are rendered operational and before they are connected to the LSB.
- The Government will provide, as requested and approved through the COR, any necessary hardware, such as laptops, desktops, tablets, cabling, and peripherals; the Contractor shall ensure items are properly configured, with approved operating systems, for network connection.

1.4 Cybersecurity: he Contactor shall perform Cybersecurity for all Agency managed systems, applications, and hardware identified in the Environment Document. Cybersecurity is comprised of Risk Management (RM), Defensive Security and Compliance. The Defensive Security Tools include but are not limited to ACAS, HBSS, Splunk, Microsoft Defender for Endpoint and future tools as identified by the Government. The Contractor's subject matter experts (SME's) shall be experienced and responsible for the following:

- Accrediting systems using eMASS (Enterprise Mission Assurance Support Services) and/or a specific software tool as directed by the Authorizing Official.
- Assured Compliance Assessment Solution (ACAS) scans and Department of Defense provided Security and Vulnerability tools.
- Front-end and back-end system administration and maintenance for Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), Splunk, and future tools as identified by the Government.
- Conducting host Security Content Automation Protocol (SCAP) and Security Technical Implementation Guide (STIG) scans to validate compliance or non-compliance.
- Mandatory support and attendance of Cybersecurity related meetings IAW requirements.
- Comply with:
    - NIST Cybersecurity and Risk Management Frameworks (RMF), including but not limited to, NIST SP 800-37, NIST SP 800-53, NIST SP 800-34, NIST SP 800-30.
    - Federal Information Processing Standards (FIPS) compliance including but not limited to FIPS 199 and FIPS 200.
    - Department of Defense Instruction (DoDI) 8500.01 and DoDI 5200.01
    - Department of Defense (DoD) 8140 Policies and Standards.
    - Computer Network Defense (CND)
    - DISA J6
    - DCDC DODIN inspections (i.e., CCORI, CSSP)

1.4.1 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): Adhere to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Governance, Identify, Protect, Detect, Respond, and Recover) to support the Agency Cybersecurity Mission to manage and reduce risk. In order to meet NIST requirements, Contractor shall develop and maintain standard operating procedures (SOPs) and work instructions (WI) for DISA J6 and PFPA mission assets identified in the LSB IT Environment Document to ensure information systems reliability, accessibility and prevent and defend against unauthorized access to systems.

1.4.2 Risk Management: Perform Department of War Risk Management Framework (RMF) in accordance with (IAW) DODI 8510.01 for all LSB Mission systems and applications identified in the LSB IT Environment Document. Provide content for RMF submissions as outlined in Section 2.2.2 under Mission Applications. Environment Document maintaining 100% system/application Authority to Operate (ATO) – DoDI 8510.01, NIST 800-53. The DOD RMF describes the DoW process for identifying, implementing, assessing, and managing Cybersecurity capabilities and services, expressed as security control, and authorizing the operation of information systems (IS). Align with J6, JPP, PFPA NIST, DODIN, and DISA Policies and Guidelines.

DELIVERABLE(S):

- RMF Summary: Weekly Agency System/Application Assessment and Authorization Report (Report provides status of all LSB Mission System and Applications and their authorization status to operate on the DoDIN.) Status of each systems authorization, ATO, and where it is in the RMF authorization chain. PFPA RMF Project Plan (Detailed spreadsheet for each system tracking all RMF deliverables required for packages submission or continuous monitoring.
- Maintain 100% ATO on all systems
- Leadership Reports on system status and current posture (as required)
- Plan of Action and Milestones (POAMs)

1.4.3 Defensive Security and Compliance: The Contractor shall perform Endpoint Security validations to ensure every device on the network meets all required security standards in accordance with (IAW) the DISA (Defense Information Systems Agency) Cybersecurity assessments, inspections, configuration guidance aligning with NIST, DOWIN and DISA Policies and Guidelines.

The Contractor shall:

- Provide complete Assured Compliance Assessment Solution (ACAS) management support to include maintaining the existing ACAS architecture and upgrading ACAS Security Center (SC) and scanner versions. All features, capabilities, and configuration changes shall be managed IAW DoD guidance.
- The Contractor shall monitor the health and performance of ACAS, HBSS, Splunk, and alert the Government of any disruptions within one (1) hour of disruption identification. The Contractor shall configure automated notifications to identify disruptions.
- The Contractor shall properly maintain compliance capability to achieve and maintain a 98% or greater credentialed scan rate and a 2.5 or lower CCRI (Commander's Critical Information Requirements) score.
- Maintain all current and future tools as identified by the Government software, configuration, system application, system administration, user access, and reporting for: ACAS, HBSS, Splunk, Tanium.
- Ensure all ACAS, HBSS, and Splunk PFPA data roll up to DISA repositories.
- Track and validate PFPA data on the DoD Continuous Monitoring and Risk Scoring (CMRS) dashboard
- Monitor, maintain and report compliance and/or noncompliance status to DISA J6, PFPA, and DCDC DODIN as required for all CTO, TASKORD, OPORD, SIGACT, and all other as required reports designated by or from DCDC DOWIN and/or DISA
- Lead all Cyber compliance reports, collaborate with OPS, Engineering, DISA, System Admins, to validate compliance status
- Maintains, monitors, obtains, reviews and verifies all Cybersecurity Compliance Reporting from Operations, Engineering, and DISA
- Develop system security contingency plans and disaster recovery procedures.
- Manage and maintain information security tools used in the performance of their duties.
- Develop and implement programs as required to ensure that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures.
- Ensure the rigorous application of information security/ information assurance policies, principles, and practices in the delivery of all IT services.
- Coordinate user and privileged account processing with PFPA's Personnel Security Division to process requests and work closely with the DISA J6 JPP team to ensure all necessary certification information is confirmed and documented.
- Support the Ports, Protocols, and Services Management (PPSM) Program IAW DoD Instruction 8551.1 through the assurance that all Enterprise Information System Ports, Protocols, and Services (PPS) are registered in the PPSM central registry, are categorized and updated on the PPSM Category Assurance List, are not deployed prior to approval from the Authorizing Official (AO), and assist the Government to develop, revise, implement, and enforce PPSM policies.
- Participating in network, systems, and application design reviews to ensure compliance IAW with all applicable government directives, approved frameworks, and industry standards, including, but not limited to, DOD Security Technical Implementation Guides (STIG), Instructions, Directives, Policies, Regulations, Publications, Guides, NSA Security Guides, and government approved frameworks, to ensure every DOD Information System & Computer Network provides the appropriate pillars of information assurance.
- Risk assessments shall be created prior to any changes to the LSB environment, e.g. hardware/software/configuration changes, etc. Details are outlined in NIST 800-30. These reports are ad hoc reports created by the Contractor, reviewed and approved by the government.
- Verify all products prior to use or installation are formally approved by DISA meet interoperability and Cybersecurity certification. Submit all new product requests to DISA using current or future documentation and ticketing/tracking system.
- Perform technical evaluations of software and hardware products to identify their capabilities and potential use within the organization's information technology program. Evaluations and assessments shall consider other Federal departments that have experience with similar products or capabilities and shall include lessons learned or best practices prepared by the organizations.
- Deliver and review for compliance, daily, weekly, monthly, annually and quarterly vulnerability assessments of security elements for all systems supported will follow DISA and DoD standards for compliance.
- Investigate and monitor all security incidents and violations. Provide reports on incidents and violations as required by the Government.

DELIVERABLE(S):

Daily:

- Security Logs – Reviewed daily for anomalous activity
- CTO Tracking and Reporting

Weekly:

- Dormant Accounts – Accounts not accessed in 30 calendar days
- Privileged Accounts – Completing list for tracking and verification
- Certificate Installation Files – Scan report for. p12 and .pfx files
- Account Configuration – Determine no changes have been to account configurations
- Firewall Rules/Configuration – Ensure firewall configuration for Star has not been altered
- Plan of Actions and Milestones – Track and maintain for Agency vulnerability remediation
- IAVM (Information Assurance Vulnerability Management) Reporting

Monthly:

- Secret Server Configuration – Review for changes and report - Monthly
- Active Directory Group Policy Review Group Policy to verify personnel are in correct groups for access – Monthly
- Ports, Protocols and Services Management – Verify systems adhere to ports and protocols listed with system in eMASS - Monthly
- Risk Assessment Review
- Incident Management Review

Annually:

- Exception Requests – Verify USB exception to policies are updated annually – Annually & Ad Hoc

Quarterly:

- Server and Workstation Image – Scan and validate up to date with current STIG release - As requested or Quarterly
- Local Systems Accounts – uarterly

As Required

- Reports as directed by the Department of War which may not be included in the directed deliverables

1.4.4 <u>Risk and Vulnerability Assessments</u>:

- Conduct monthly discovery scans of all PFPA's IP space and weekly risk and vulnerability assessments in accordance with TASKORD 20-2020. Vulnerability assessment scanning will be done using DOW provided and/or approved Security and Vulnerability tools (e.g. ACAS, DoD Security Content Automation Protocol (SCAP)).

DELIVERABLE(S):

- Weekly Audit Compliance Scan, and Vulnerability Assessments Reports
- Weekly TASKORD 20-2020 Compliance Report – Validate compliance with task order checklist
- Develop and Maintain Plan of Action and Milestones for all vulnerabilities identified which cannot be remediated within the allotted time based on criticality
- System reports as required/requested

1.4.5 <u>Trellix</u> / <u>Host Based Security Systems (HBSS)</u>:

- Perform Endpoint Security on the LSB IT environment. Deploy, manage, and maintain the Department of Defense endpoint security using Host Based Security Systems (HBSS) to maintain 100% OPORD 16-0080 Compliance for systems/applications identified in the LSB IT Environment Document. HBSS is a COTS suite of software applications used within the DOD to monitor, detect, and defend the computer networks and systems

DELIVERABLE(S):

- Weekly OPORD 16-0080 Compliance Report – Validate compliance with task order checklist
- System Reports (as requested e.g. Rouge Sensor Detection, McAfee Antivirus, Data Loss Prevention)
- System reports and required/requested

1.4.6 <u>DoD 8570.01-M and Application Certifications</u>:

- The Contractor shall ensure all Cybersecurity personnel shall maintain applicable certifications (e.g. CISSP, CEH, and Security+). The Contractor shall comply with DOD 8140 standards and policies to

meet Department of War requirements to perform Cybersecurity/Information Assurance (IA) duties on the LSB IT environment. The Contractor is responsible for all costs associated with obtaining and maintaining cybersecurity/information assurance certifications for personnel assigned to this contract. Certification requirements are based on role; additional application certifications may be required for future tools. Valid copies of certifications due at candidate start date.

DELIVERABLE(S) Certifications:

- DOD 8140 Standards
- eMASS, HBSS, ACAS, Splunk
- Windows and Linux Administration

1.4.7 Cybersecurity Inspections:

- The Contractor shall support cyber security-related audits, inspections and assessments. Support Site/Staff Assistance Visits (SAV), Command Cyber Operational Readiness Inspections (CCORI), and manual compliance assessments. Also ensuring compliance with Cyber Security Service Provider (CSSP) evaluations, Joint Staff Integrated Vulnerability Assessments (JSIVA), Balanced Survivability Assessment (BSA), Measures of Effectiveness (MOE), Red/Blue Team exercises and FISMA.

- The Contractor shall take appropriate remediation actions associated with findings from inspections and evaluations. Actions include the implementation of security tools, automated script development, reviewing system specific documentation and procedures, providing weekly status reports and metrics including vulnerability assessment results, patch management statistics, asset inventory, system configurations, waiver requests generation/validation and general information technology security guidance. Comply with OPORD 16-0080, TASKORD 17-0019, FRAGO to OGS/CTO 07-015, NIST Cybersecurity Framework, DoD Cybersecurity Services Evaluator Scoring Metrics.

DELIVERABLE(S):

- Weekly Audits, Inspections and Assessments Reports (e.g. Remediation status briefings/ reports)

1.4.8 Daily Cybersecurity Orders Processing:

- The Contractor will use SIPRNET to acknowledge and track Department of Defense Task Orders, Operations Orders, Warning Orders, and any other orders submitted by US Cyber Command (USCC) and/ or Defense Cyber Defense Command (DCDC) Department of Defense Information Network (DoDIN).
- The contractor will review each order Engineering released to determine if any actions are required by PFPA, collaboration with other Teams may be required to determine actions.
- The Contractor shall in coordination with the Government execute actions as required within the requirements of this PWS and provide status reporting to the Government. Additional requirements will be provided in a separate task order under the IDIQ and may be based on a TSI.
- The Contractor shall provide a daily report, which will consist of any orders released in the previous 24 hours as well as tracking any open orders with the status. The Contractor will maintain a comprehensive list of released orders for Agency Leadership reference. Orders Processing and Tracking, including but not limited to assisting the government in receiving, acknowledging, analyzing, interpreting, coordinating, assigning, communicating, implementing following up, verifying and reporting compliance with Cybersecurity task orders.

DELIVERABLE(S):

- Daily CTO and Task Order Status Tracking Report, Compliance Status and Reporting
- Attend daily classified OPSYNC meeting

1.4.9 Cybersecurity Standard Operating Procedures (SOP), Meetings, and Work Instructions (WIs):

- The Contractor shall create SOPs and WIs for new, revised, or missing requirements; ensure continuous review and maintenance of all Cybersecurity SOPs and WIs to ensure content remains current; and accurate. The SOPs and WI's shall be updated immediately when changes to a process

occurs. Every 6 months, all SOPs and WI's will also be reviewed to verify the process is accurately documented.

- Mandatory meeting support and attendance daily, weekly, monthly or as required IAW requirements

1.5 Configuration Management (CM): The Contractor shall provide Configuration Management (CM) support to all proposed and future, projects relevant to this task order. The DISA and Joint Service Provider (DISA J6) is the basis for change management policies. The Contractor's approach shall be IAW DISA J6 Enterprise Change Management (EChM) Process and best practices; and Information Technology Infrastructure Library (ITIL); to establish and control product attributes and the technical requirements across the total system life cycle. The Contractor shall support and comply with all established DISA J6/JPP governance processes, policies, and procedures supporting all areas of the FPTS contract.

- The current Configuration Management Database (CMDB) is maintained via Microsoft Excel. The Government recognizes that this isn't a long-term solution. In the Configuration Management Plan , the Contractor shall provide a recommendation for a CMDB. Until approved by the Government, the Contractor shall use the existing spreadsheet. During the length of the contract, the Contractor may upload existing CM data into a Government owned MMS. Contractor shall baseline, identify, track, document, audit, and control the functional and physical characteristics of the system design. The Contractor shall address a change and configuration control system and periodic audits by both Government and Contractor personnel, to include verification and validation of work. All configuration changes shall be implemented via the Change Management process and be validated at the Configuration Control Board (CCB).

- The Contractor abshall provide configuration management support by developing a process for establishing and maintaining consistency of a product's performance, functional and physical attributes, design and operational information throughout its life cycle.

- The Contractor shall provide DISA J6/JPP a drafted Configuration Management Plan (CMP) 30 calendar days after award and a final 60 calendar days after award, describing support for all hardware/software technology scheduled to be implemented into and maintained in the DISA J6 JPP production environment prior to (scheduled for) deployment, during (while in) production, and after its deployment (scheduled for decommissioning).

DELIVERABLE(S):

- Configuration Management Plan

- The Contractor shall assure the baseline configuration of all network assets (including hardware, software, point-to-point circuits and documentation). DISA J6 JPP network assets shall be accurately represented and reported in ELMS the Government system. The Contractor shall provide configuration management reports as requested by the government.

- The Contractor shall work with the government for the full list of maintenance contracts, equipment and/or systems. The Contractor shall provide maintenance and warranty reports as requested by the government.

DELIVERABLE(S):

- Maintenance and Warranty Reports

1.5.1 Software Media and Document Library:

- The library is to contain updated COTS/GOTS hardware and software user and technical manuals, network diagrams, and documents on and about the components, equipment, systems and subsystems that make up the PFPA FPTS systems. Note: Updated library components including, but not limited to hardware, software manuals, network diagrams and documents must be managed and maintained/updated upon a change or a minimum of once quarterly. This includes Internal Use Software (IUS).

- The Contractor shall establish, operate, maintain and sustain a structured and well-kept software media and documentation library (electronic and hard copy as appropriate) in a secure information technology repository, including SharePoint and Coral, in which authorized versions of software media

and related documentation (i.e. SOP's, processes, procedures, and tech. manuals…), are stored and protected.

DELIVERABLE(S):

- Maintain current or create Online Software Media and Document Libraries
- The Contractor shall ensure the library is available to JPP management, system administrators, and users at all times.
- The Contractor shall recommend to the Government additional items to be included in the Software Media Library and Documentation library.
- The Contractor shall ensure any hardware, software and firmware complies with federal, DoD, and DISA DISA J6 JPP regulations before deploying onto a JPP or Coral/ LSB/CORAL environment.
- The DISA J6 Supported Products List (SPL) is the single authoritative source for approved software and hardware products intended for use on the DISA J6 JPP production network. Acquisition and/or operation of products not listed on the SPL is not authorized unless a waiver is approved by DISA J6.

1.5.2 CM Standard Operating Procedures (SOP) and Work Instructions (WIs): The Contractor shall create SOPs and WIs for new, revised, or missing requirements; ensure continuous review and maintenance of all CM SOPs and WIs to ensure content remains current and accurate.

1.5.3 Change Management (ChM): The Contractor shall assess, recommend, develop, and implement the Change Management process to organize and efficiently facilitate change, based on a documented requirements baseline, and utilizing industry best practices in change management. This is intended to ensure that customer expectations are fully understood and realized in an efficient manner, including proper consideration of all potential impacts on customers and resources. Change Management is a necessary and critical process to ensure the LSB systems environment remains current, orderly, and a stable evolution of the LSB Architecture and Configuration Management.

- The Contractor shall develop a plan (draft due 30 calendar days after award (DAA); final due 60 DAA, responsible for controlling the lifecycle of all changes. The primary objective is to enable beneficial changes to be made, with minimal to no impact or disruption to the LSB environment, Mission System & applications, and the DISA J6 JPP Mission.
- The Contractor shall manage changes to the LSB infrastructure that may arise in response to problems, internally or externally imposed requirements (e.g. legislative changes) or proactively seek improved efficiency and effectiveness. These changes may also be implemented to enable or reflect business initiatives or from programs, projects or service improvement initiatives.
- The Contractor, IAW DISA J6 JPP processes, shall ensure standardized change management methods and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.
- The Contractor shall follow existing standards IAW DISA J6 JPP processes including engineering decommissioning policies and processes to ensure orderly termination on/disposal of network devices/ circuits and components. The Contractor shall follow decommissioning engineering standards where such connectivity is located. Where an engineering standard does not exist, the Contractor shall submit a recommended standard to DISA J6 JPP Engineering for review and approval. The Contractor shall update the status of the equipment in the CMDB and provide decommissioning reports as requested by the Government.
- The Contractor shall ensure that any modification to the Information Technology (IT) environment are tracked and controlled using DISA J6 JPP standardized methods for efficient and prompt handling of technical changes, to minimize the impact of change-related incidents to service, quality, and improve standardized day-to-day operations within DISA J6.

- The Change Management Process requires the Contractor to manage baseline configurations; hardware and software; organization policy and procedural documentation; SOPs, WIs, and coordination and collaboration with other activities and processes.

- All changes must be approved by the Government's governance process.

DELIVERABLE(S):
- Decommissioning Report
- Change Management Plan

1.5.4 ChM Standard Operating Procedures (SOP) and Work Instructions (WIs): The Contractor shall create SOPs and WIs for new, revised, or missing requirements; ensure continuous review and maintenance of all Change Management SOPs and WIs to ensure content remains current; and accurate.

1.5.5 Document Management: The Contractor shall provide a Document Management Plan, within the PM Plan. The Contractor shall use the DISA J6 JPP SharePoint site for project collaboration and document management of, but not limited to, deliverables, SOPs, WIs, AARs, POAMs, reports, briefings, meeting minutes, action items, training and certificates, etc. The Contractor shall establish, operate, maintain and sustain structured and well-kept document repositories (electronic and hard copy as appropriate). The Contractor shall provide a plan describing document management and control; creating documents and use of Government templates and markings; and managing the document repositories in SharePoint and the Coral. The plan shall include, as part of document management, a quality peer review process and how document management is communicated. The plan shall include an index or schematic showing location and naming convention that easily identifies PWS deliverables.

1.5.6 Data Repositories: The Contractor shall develop and execute a scheme for storing and managing all documentation developed and/or maintained under this contract and, as appropriate, disseminating or publishing material via mechanisms such as the Coral Network, the web, and Microsoft SharePoint. The tools and methods selected to perform this function must be approved by the COR/TM prior to implementation if different than the tools or processes currently in use.

DELIVERABLE(S):
- Data Management Plan (included in the Change Management Plan)

1.6 Continuity of Operations (COOP): The Contractor shall execute IAW DFARS 252.237-7603 Continuation of Essential Contractor Services and 252.237-7024 Notice of Continuation of Essential Contractor Services and develop a Mission Essential Contractor Services (MECS) Plan to include the Mission Essential Functions (MEF) and Essential Supporting Activities (ESA) of the Force Protection Technology division. This plan will be strategically aligned to the PFPA COOP plan and support all activities associated with the reconstitution of the PFPA at an alternate location.

- As directed by the Contracting Officer, the Contractor shall participate in training events, exercises, and drills associated with Government efforts to test the effectiveness of COOP procedures and practices. The Federal Continuity Exercise, referenced in the DISA J6 JPP COOP Plan, is an annual, integrated continuity exercise.

- The Contractor shall be capable of providing and maintaining essential Contractor services at local and regional COOP sites during exercise scenarios and during periods of actual crisis as directed by the Contracting Officer.

- The Contractor shall submit, for approval via the COR to the KO, its MECS Plan to provide and maintain essential Contractor services in conjunction with DoDI 1100.22, "Policy and Procedures for Determining Workforce Mix" Change 1, December 1, 2017. Once approved by the KO, the Contractor's plan is automatically incorporated in this contract (with no need to issue a modification).

DELIVERABLE(S):
- Mission Essential Contractor Services (MECS) Plan

The Contractor shall, IAW the DISA DISA J6 JPP deliver a MECS After Action Report (AAR) to the Government within seven (7) days following the end of a COOP exercise or actual crisis. The report shall include, but is not limited to, timeline of events; personnel assigned; success/failures; lessons learned; recommendations for improvement.

DELIVERABLE(S):

- COOP After Action Report

1.6.1 COOP Standard Operating Procedures (SOP) and Work Instructions (WIs): The Contractor shall create SOPs and WIs for new, revised, or missing requirements; ensure continuous review and maintenance of all COOP SOPs and WIs to ensure content remains current; and accurate.

1.6.2 Compliance: The Contractor shall comply with the following clauses in order to meet DISA/ JFHQ DODIN cybersecurity compliance requirements:

- Training and certification compliance IAW DFARS 239.7102-3 and DFARS 252.239-7001 Department of Defense (DoD) 8570.01-M, "Information Assurance Workforce Improvement Program".
- Compliance IAW DFARS Subpart 239.76 Cloud Computing for components that employ contracts with external entities.

1.7. Security Requirements:

1.7.1 Personnel Security Clearances: Unless otherwise specified herein, the minimum-security clearance for personnel performing services herein is Secret.

1.7.2 Facility Security Clearance:

- **Security Requirements:** The Contractor shall maintain a Top Secret facility clearance in accordance with the attached DD254.

1.8 Period of Performance: The period of performance shall for one (1) Base Year of 12 months and four (4) 12-month option years.

1.9 General Information:

1.9.1 Place(s) of Performance and Stakeholders:

1.9.1.1 Place of Performance: The Government-designated locations to be serviced include the Pentagon Reservation and Department of Defense (DoD) occupied facilities (not under the jurisdiction of a Military Department) within the National Capital Region (NCR) to include, but not limited to:

- Suffolk Building (Falls Church, VA)
- Pentagon Operations Center (POC)
- Mark Center Security Operations Center (SOC)
- Raven Rock Mountain Complex (RRMC)
- PFPA Police Cruisers/Vehicles
- Pentagon Police Mobile Command Vehicle (MCV)
- Federal Law Enforcement Training Center Cheltenham, MD
- Other leased facilities throughout the NCR

1.9.1.2 Stakeholders: Primary stakeholders include other Government Employees (OGE) and other Government Contractors (OGC). This is not an all-inclusive list:

- PFPA Headquarters
- Pentagon Operations Center (POC)
- Mark Center Security Operations Center (SOC)
- Enterprise Physical Security Division (EPSD)
- Technical Integration Defense Division (TIDD)
- Security Services Division (SSD)
- Pentagon Police Department (PPD)
- Office of Emergency Management (OEM)

1.9.2 Phase In/Phase Out Period: A smooth and orderly Phase In/Phase Out process between the incoming and outgoing vendors is necessary to ensure no disruption to vital services and Government activities. The Contractor shall ensure all existing and applicable services and support are successfully transitioned from the incumbent Contractors to the awarded contractor. At time of proposal, the Contractor shall provide a Phase In plan defining the strategy to expedite onboarding personnel and participate in the knowledge transfer process. In turn, the Contractor shall also provide their Phase Out plan defining the strategy to continue to meet contractual requirements and participate in the knowledge transfer process at the end of this contract. The Contractor shall ensure Continuity of Services, so that no disruptions to program services and support occurs during the transition period. Immediately following contract award, and throughout the execution of the transition plan, both Contractors are fully accountable and responsible for successful performance of all objectives and requirement on the contract. The Phase In/Phase Out Plan shall include, but not limited to:

- Day-by-day transition schedule with key milestones identified
- Review and evaluation of current support systems/services
- Transition of historic data and knowledge transfer to new contractor systems
- Acknowledgement that Knowledge transfer of historical data has occurred
- Recruitment, onboarding, training, and identification of key and non-key personnel
- Transition incumbent personnel, re-badging/ re-issue of credentials and access, user agreements, and conduct orientations

- Acknowledge and confirm the Transfer of hardware/software warranties, licenses, and service maintenance agreements has occurred
- Acknowledge and confirm the Transfer of all necessary business and/or technical documentation in the JPP's Knowledge base repositories, consists of SharePoint and Coral network information has occurred
- Acknowledge and confirm the Transfer of compiled and un-compiled source code, to include all version, maintenance updates, and patches, if applicable
- Acknowledge and confirm the coordination with Government to account for government keys, ID/access cards, and security codes
- All other issues associated with the appropriate transition of the FPTS requirement

MEETINGS:

- Program Award Kickoff Meeting
- Periodic Transition Updates

DELIVERABLES:

- Phase In/Phase Out Plan
- Kickoff Presentation
- Stakeholder Presentation

1.9.3 Key Personnel: Before replacing any individual designated as Key by the Government, the Contractor shall notify the KO **no less than 10 business days in advance**, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the Contracting Officer. **The Contractor shall not replace Key Personnel without written approval from the KO.** The following Contractor personnel are designated as Key for this requirement.

DELIVERABLE(S):

- Resume for Key Personnel

1.9.3.1 Program Manager:

The qualified individual for this position must have:

- Minimum fifteen (15) years of experience in the implementation and sustainment of complex security systems, in related technical fields to include I/T Management, Engineering, Project Management, Cybersecurity, and Computer Science, and a Baccalaureate Degree in I/T Management, Engineering, Cybersecurity, Computer Science, or other related technical fields.
- Project Management Professional (PMP) Certification.
- Active or current Top Secret (TS) security clearance adjudicated by DIA or DoD CAF at the time of proposal submission and maintain the TS continuously thereafter.

The Program Manager shall:

- Serve as the single focal point accountable for the quality of all FPTS services, projects, risks, personnel, activities and deliverables.
- Brief FPTS services, activities, and deliverables to a wide range of individuals to include United States Government personnel up to Executive Service level.
- Assure the right mix of management, technical, engineering, and maintenance personnel. Assure all personnel have the necessary qualifications, including training, security clearance, badging, and access privileges.
- Manage and de-conflict multiple ongoing baseline support and technical tasks.
- Lead the monthly PMR presentation to the Government.
- Manage, control and report FPTS program costs.
- Identify FPTS system dependencies or of non-FPTS systems dependent on FPTS systems. Document concerns and findings and present to the Government.
- Communicate to the Government emerging trends and technologies in the information technology industry.

1.9.3.2 Engineering Manager:

The qualified individual for this position must have:

- Minimum ten (10) years of demonstrated experience in the development of enterprise-wide or large-scale information systems
- Minimum ten (10) years of demonstrated experience in a senior leadership engineering position
- Minimum ten (10) years of demonstrated experience managing a team of IT engineers implementing IT projects involving networks, including network infrastructure, information assurance engineering, and software applications;
- Current DoD 8570.01-M IAM Level II certification;
- Active or Current Top Secret security clearance adjudicated by DIA or DoD CAF;

Preferred:

- Fifteen (15) years of demonstrated experience in the development of enterprise-wide or large-scale information systems

The Engineering Manager shall:

- Establish system information requirements using analysis of the information engineer(s) in the development of enterprise-wide or large-scale information systems.
- Determine and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture.
- Design architecture to include the software, hardware and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.
- Identify, assess, and present options for meeting the functional and technical requirements including hardware and software updates or upgrades.
- Be responsible for developing high-level system design diagrams.
- Ensure systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards e.g. Institute of Electrical and Electronic Engineers (IEEE) Open Systems Environment (OSE) reference model.
- Ensure a compliant common operating environment is.
- Evaluate analytically and systematically problems of workflows, and organization.
- Plan and develop appropriate corrective action.
- Provide daily supervision and direction to staff.

1.9.3.3 Operations Manager:

The qualified individual for this position must have:

- Minimum ten (10) years of demonstrated experience in IT Operations utilizing ITSM best practices in a Federal Government with a preference to experience in the DoD environment;
- Minimum ten (10) years of demonstrated experience in a senior IT management role in a Federal Government or DoD environment;
- Current DoD 8570.01-M IAM Level II certification;
- Meet requirements IAW DoDD 8140.01 -System Administrator Core Competencies defined within the DoD Cyber Workforce Framework;
- Active or Current Top Secret security clearance adjudicated by DIA or DoD CAF; and

The Operations Manager shall:

- Manage LSB Systems operations and maintenance (O&M).
- Ensure production schedules are met (e.g. deployments, imaging, patching schedules).
- Ensure LSB Systems resources are used effectively.
- Coordinate the resolution of production-related problems.

- Ensure proper relationships are established between customers, teaming partners and vendors to facilitate the delivery of information technology services.
- Provide users with computer output.
- Supervise O&M staff (i.e. Desktop Administration, Systems Administration, Network Administration, etc.)

1.9.3.4 Cybersecurity Manager:

The qualified individual for this position must have:

- Minimum ten (10) years of demonstrated experience in Information Security, with a good working knowledge of both DoD and Federal Government Cybersecurity/Information Assurance Security policies and procedures.
- Minimum five (5) years of demonstrated experience leading Cybersecurity Teams.
- Minimum ten (10) years demonstrated experience with Risk Management Framework (RMF). Includes experience performing DoD authorizations, Accreditations, and Assessments.
- Minimum five (5) years demonstrated experience accrediting systems using Enterprise Mission Assurance Support Service (eMASS), Host Based Security Systems (e.g. Trellix, MS Defender, etc.), and Assured Compliance Assessment Solution (ACAS).
- Valid current training Certificates for eMASS, HBSS, and ACAS.
- Current DoD 8570.01- M IAM Level III certification.
- Active Top Secret security clearance adjudicated by DIA or DoD CAF.

Preferred:

- Fifteen (15) years of demonstrated experience in Information Security, with a good working knowledge of both DoD and Federal Government Cybersecurity/Information Assurance Security policies and procedures.

The Cybersecurity Manager shall:

- Be the contract Subject Matter Expert (SME) all matters related to Cybersecurity and the Risk Management Framework (RMF), eMASS, ACAS, HBSS, Splunk and Microsoft Defender for Endpoint (MDE);
- Provide daily supervision and direction to Cyber staff
- Ensure Risk Assessments, Exemption/Exception requests and RMF Packages meet compliance
- Monitor, report and assess Cyber compliance for all Operations and Infrastructure
- Maintain, monitor, report and assess Cyber compliance on all security tools and technology
- Monitor, report and assess Cyber internal and external policy compliance
- Monitor, report and assess Cyber regulation compliance; and
- Work to mitigate risk across security system's infrastructure

1.9.3.5 Master Project Scheduler:

The qualified individual for this position must have:

- Active or Current Top Secret security clearance adjudicated by DIA or DoD CAF; and a bachelor's degree from an accredited college or university in Engineering, Information Systems, Information Technology or a technical discipline.
- 5 years in Project Management or Security Management
- PMP certification or related program or project management experience
- Expert level skills with MS Project, MS Project Server, or MS Project Professional Project.
- Ability to work collaboratively with all team members and be proactive in organizing PMO outreach to PMs to gather and report on schedule critical information

The Master Project Scheduler shall:

- Prepare comprehensive project schedules and assist with the management of project milestones and deliverables
- Develop and maintain integrated master schedules using MS Project
- Ensure issues are called out to the appropriate decision-making authority in a timely manner so that decisions can be made that minimize impact to critical path
- Partner with Project Managers to identify schedule dependencies and ensure those are clearly linked across projects or programs
- Identify and analyze schedule risks and mitigation strategies
- Update project schedules to conform to current schedules and submit the updated Project Schedules
- Utilizes Gantt, PERT, milestone charts, other project management techniques to gauge progress and identify performance variances
- Manage both baseline work and remaining work
- Identify and manage resource over-allocation

PART 2
Major Support Categories:

PART 2
DEFINITIONS AND ACRONYMS

2.0 DEFINITIONS AND ACRONYMS:

2.1 DEFINITIONS:

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2. ACRONYMS:

ACS	Access Control System
ACOR	Alternate Contracting Officer Representative
ASI	Authorized System Interruption

BVMS	Bosch Video Management System
CAC	Common Access Card
CO	Contracting Office
KO	Contracting Officer
COR	Contracting Officer Representative
CMR	Contractor Manpower Reporting
DHHQ	Defense Health Headquarters
DODCIO	Department of Defense Chief Information Officers
DoD	Department of Defense
ESS	Electronic Security System
FPTS	Force Protections Technology Support
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GUI	Graphical User Interface
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
IDIQ	Indefinite Delivery Indefinite Quantity
IA	Information Assurance
IMS	Integrated Master Schedule
ISMP	Integrated Security Master Plan
ISSC	Integrated Security Services Contract
ICD	Intelligence Community Directive
ISC	Interagency Security Committee
ISO	International Standards Organization
IP	Internet Protocol
IDS	Intrusion Detection System
JPP	Joint PFPA Provider
DISA J6	Joint Service Provider
LAN	Local Area Network
MMS	Meteorological Modeling System
MAC	Media Access Control
NCR	National Capital Region
NISPOM	National Industrial Security Program Operating Manual
O&M	Operations and Maintenance
OS	Operating System
OEM	Original Equipment Manufacturers
OGA	Other Government Agencies
OGC	Other Government Contractors
PFPA	Pentagon Force Protection Agency
PWS	Performance Work Statement
POP	Period of Performance
PIN	Personal Identification Number
PIV	Personal Identification Verification
PACS	Physical Access Control System

PSIM	Physical Security Information Management
PoE	Power Over Ethernet
PM	Preventative Maintenance
PMP	Privilege Management Program
PMR	Program Management Review
PM	Program Manager
PKI	Public Key Infrastructure
QA	Quality Assurance
QC	Quality Control
RRMC	Raven Rock Mountain Complex
SCI	Secure Compartmentalized Information
SMA	Service Maintenance Agreements
SDK	Software Development Kit
SOP	Standard Operating Procedure
SQL	Structured Query Language
STIG	Security Technical Implementation Guides
TM	Task Monitor
TDP	Technical Design Package
TS	Top Secret
UL	Underwriters Laboratories
UFC	Unified Facilities Criteria
UPS	Uninterruptible Power Supply
VMS	Video Management System
VRM	Video Recording Manager
VSP	Virginia State Police
VSS	Visual Surveillance System

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3.0 GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1 Services: The Government will provide project leads, for all installation projects. The Government will also provide available drawings for facilities and office spaces.

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

3.3 Materials: The Government will provide the Standard Operating Procedures for the Access Control Center.

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

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4.0 CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: NOT APPLICABLE

Part 5

Lifecycle/ Technical Refresh and Modernization

5.0 Requirements Overview:

The overarching objective of this requirement is to ensure the LSB platform, and its associated end-user environment evolve in a planned, proactive, and financially predictable manner. The contractor is expected to execute a continuous cycle of lifecycle replacement, technical refresh, and strategic modernization. This will prevent technological obsolescence, maintain a robust security posture, and align the environment with emerging Department of War (DoW) mandates and mission requirements, thereby minimizing the need for out-of-cycle, unfunded projects.

The contractor shall execute the planning, engineering, and implementation required to complete recurring lifecycle and technical refresh projects, as well as drive IT futures modernization. All labor associated with the planning, assessment, design, and implementation of the projects and activities defined in this section shall be included in the Firm-Fixed Price (FFP) of the contract.

5.1 Execute Scheduled Lifecycle Replacement Projects
The contractor shall successfully plan, engineer, and implement all identified lifecycle and modernization projects according to the Government-approved schedule. All known lifecycle replacement projects are completed continuously across the life of the contract Period of Performance.

- Virtual/Physical Trusted Platform Module (TPM) implementation
- Windows Server 2016 Migration to a supported version (2019/2022)
- Workstation LCR (remaining 40%): Complete by base year
- PAAS-3 Infrastructure Refresh
- Desktop/ Laptop/ Toughbook LCR

5.2 Technology Refresh Cycle:
The contractor shall manage, execute and maintain a continuous rolling technology refresh cycle to ensure the LSB environment remains current and supportable.

- **End-User Devices**: The contractor shall implement a continuous lifecycle replacement plan for all desktop, laptop, and Toughbook devices. The plan shall target a refresh rate of approximately 30% of the total device inventory on a three-to-four-year cycle to ensure no device remains in production beyond its effective operational lifespan.

- **PaaS Infrastructure**: The contractor shall implement a similar continuous lifecycle replacement plan for the complete PaaS physical environment e.g. servers, virtual hosts, and storage infrastructure etc. The plan shall target a refresh cycle of approximately 20-25% of the infrastructure on a four-to-five-year cycle.

- **Bill of Materials**: For each planned refresh cycle, the contractor shall deliver a complete Bill of Materials (BOM) and technical specification package to the Government no less than 180 days prior to the required procurement date. This package must be sufficiently detailed to ensure the Government can procure equipment that meets all technical and functional requirements of the environment.

- **Deliverables**:

    - Execute Lifecycle Replacement Projects per sect. 5.1
    - Deliver complete Bill of Materials for each lifecycle replacement project

5.3 Proactive Modernization and Strategic Planning:
The contractor shall serve as a strategic partner, actively identifying and planning for future improvements to the environment. Always functioning as the Government's forward-looking technology expert, responsible for ensuring the LSB platform does not become obsolete. The primary objective is to drive a continuous modernization strategy that keeps pace with the rapid evolution of technology, minimizes operational and security risks, and proactively identifies opportunities for innovation. The contractor is mandated to keep the Government constantly abreast of new and emerging technologies that could enhance the efficiency, resilience, and mission capability of the LSB environment, translating these opportunities into actionable plans.

- **Modernization Roadmap**: The contractor shall develop and maintain a five-year IT Modernization Roadmap, delivering updates annually. This roadmap must be a dynamic, strategic document that accurately reflects the lifecycle refresh schedules and integrates detailed proposals for new technology insertions that align with Government and DoW strategic goals.

- **DoW/ Federal Mandated Requirements**: For all externally mandated requirements (e.g., from DoW CIO, OMB), the contractor shall deliver a comprehensive Assessment & Design Package within the timeframe directed by the Government. This package must fully define the scope of work, to include cost required to meet the mandate.

- **Mandated Requirements Assessment and Design**: In addition to responding to external mandates, the contractor shall develop and deliver a comprehensive Assessment and Design Package for each of the following Government-identified strategic initiatives. This package, in the form of a Technical Solution Identification (TSI), must provide a complete analysis of the current state, a detailed technical design for the future state, a full scope of work, and a bill of materials required for implementation.

    - Readiness to convert the LSB Enterprise from IPv4 to IPv6 (TSI)
    - Post-Quantum Cryptography (PQC) Management and Integration (TSI)
    - Develop and Maintain an LSB Data Strategy (e.g., Data Lake, Fabric, and/or Mesh) (TSI)
    - Establish and Maintain an LSB Lab Environment (TSI)
    - Raven Rock Mountain Complex (RRMC) PaaS Integration/Modernization (TSI)
    - Advanced Endpoint Security Implementation (TSI)
    - Software Bill of Materials (SBOM) Management for all software within the LSB (TSI)
    - Laboratory Information Management System to LSB (TSI)
- Deliverables:
    - Modernization Roadmap
    - Technical Solution Identification (TSI)

5.4 Zero Trust Architecture Implementation:
The contractor shall provide continuous engineering engagement for the implementation and evolution of the Government's Zero Trust Architecture throughout the entire period of performance.

5.5 Configuration Management Database (CMDB):
The contractor shall implement and maintain a comprehensive Configuration Management Database (CMDB) throughout the entire period of performance.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS):

6.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures listed in Appendix B.

PART 7
TECHNICAL EXHIBIT LISTING

7. ATTACHMENT/TECHNICAL EXHIBIT LIST:

7.1 Technical Exhibit 1 – Performance Requirements Summary

7.2 Technical Exhibit 2 – Deliverable Schedule

7.3 Technical Exhibit 3 – Estimated Workload Data

TECHNICAL EXHIBIT 1
PERFORMANCE REQUIREMENTS SUMMARY

7.1 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.

Projects and Architectural Engineering

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Integrated Master Schedule	1.3.2	Contractor shall maintain a current and accurate Integrated Master Schedule	100%	100% Government review of Integrated Master Schedule
Project Schedules	1.6.5.5	The Contractor shall maintain Project Schedules for each project assigned	100%	100% Government review of Project Schedules
Weekly Baseline Reports	1.6.5.5	Contractor shall submit a current and accurate Weekly Baseline Report	100%	100% Government review of all Weekly Baseline Reports

Operations and Maintenance

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Operations & Maintenance	1.6.6.2	PFPA Mission Critical Applications/Systems Infrastructure-Availability: 99.99% uptime = allowed 52.56 minutes downtime per year	99.99%	100% Government review of system uptime
	1.6.6.2	PFPA Mission Essential Applications/Systems Infrastructure-Availability: 99.9% uptime = allowed 8.76 hours downtime per year	100%	100% Government review of system uptime
	1.6.6.2	PFPA Mission Support Applications/Systems Infrastructure-Availability: 99% uptime = allowed 3.65 days downtime per year	100%	100% Government review of system uptime

Operations and Maintenance Cont.

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Access Management	1.6.6.2.1	Permit only authorized users access to the LSB environment	100%	Periodic and Random Review & Sampling
	1.6.6.2.1	Maintain an accurate identity and rights registry (Active Directory) that undergoes periodic maintenance and review	100%	
	1.6.6.2.1	Auditable record of access attempts is maintained and available to authorized personnel	100%	
	1.6.6.2.1	Data necessary to demonstrate compliance relative to service and information access is available	100%	
	1.6.6.2.1	Security vulnerabilities and incidents are identified, monitored and reported	100%	
	1.6.6.2.1	Unauthorized access to information, applications and infrastructure is detected, reported, and resolved	100%	
	1.6.6.2.1	Access-related security incidents are defined and access controls are regularly tested	100%	
	1.6.6.2.1	Ensure account creation within 8 business hours	> 95%	
	1.6.6.2.1	Ensure account modification within 12 business hours	> 95%	
	1.6.6.2.1	Ensure account disable within 4 business hours	> 95%	
Event Management	1.6.6.2.2	Ensure all planned events are coordinated with government stakeholders, other government contractors, and other government agencies to ensure collaboration for planned events.	100%	100% Government review of Event success
Incident Management and Response	1.6.6.2.3	The Contractor shall support the PFPA infrastructure, applications, and systems to ensure the specifications of the three (3) mission criteria requirements are met.	100%	Periodic and Random Review & Sampling

Operations and Maintenance Cont.

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)

Incident Management and Response	1.6.6.2.3	Response to outage or degradation shall be in line with the Mission Critical, Mission Essential, or Mission support requirements defined within the IT Environment Document.	100%	100% Government review of time to complete actions
Incident Management and Response	1.6.6.2.3	The Contractor shall acknowledge all Incidents within 10 minutes of receiving ticket or notification of incident, and notify the Government immediately of any alerts or events impacting any LSB system or application	100%	100% Government review of time to complete actions
Security Patching and Vulnerability Management	1.6.6.4	Monitor security sources (e.g. DoD, Microsoft, etc.) for vulnerability announcements, patch and non-patch remediation's, and emerging threats that correspond to the software within the inventory	100%	100% Government review of cyber security posture
Security Patching and Vulnerability Management	1.6.6.4	Prioritize the order in which vulnerabilities and remediating should be addressed	95%	100% Government review of cyber security posture
Security Patching and Vulnerability Management	1.6.6.4	Conduct testing of patches and non-patch remediation's on IT components that use standardized configurations	100%	100% Government review of patching and vulnerability management success
Security Patching and Vulnerability Management	1.6.6.4	Oversee vulnerability remediation process	100%	100% Government review of cyber security posture
Security Patching and Vulnerability Management	1.6.6.4	Distribute vulnerability and remediation information to local administrators	100%	100% Government review of cyber security posture
Security Patching and Vulnerability Management	1.6.6.4	Perform automated deployment of patches to IT devices using enterprise patch management tools	100%	100% Government review of time to complete actions

Operations and Maintenance Cont.

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Security Patching and Vulnerability Management	1.6.6.4	Configure automatic update of applications whenever possible and appropriate	100%	100% Government review of time to complete actions
Security Patching and Vulnerability Management	1.6.6.4	Verify vulnerability remediation through network and host vulnerability scanning	100%	100% Government review of weekly scanning results
Security Patching and Vulnerability Management	1.6.6.4	Train administrators on vulnerability mitigation and procedures	100%	Periodic and Random Review of Contractor staff performance

Security Patching and Vulnerability Management	1.6.6.4	The Contractor shall ensure all infrastructure components are compliant in accordance with the DOD rules, regulations, best practices and federal laws as directed by DoDI 8500.01 and DODD 8140.01.	100%	100% Government review of cyber security posture
Security Patching and Vulnerability Management	1.6.6.4	Maintain the DOD mandated system credentialing rate at 98% or better	95%	100% Government review of weekly scanning results
Security Patching and Vulnerability Management	1.6.6.4	Maintain CCRI score below 2.5 for all systems TO2 is responsible for that are connected to the DODIN.	95%	100% Government review of weekly scanning results
System Monitoring	1.6.6.6	Log, review, acknowledge, and track Incidents and Problem tickets received	100%	Periodic inspection of Incident and Problem tickets status via metrics and customer feedback
	1.6.6.6	Use Government provided monitoring tools (i.e. SolarWinds) and procedures	100%	Periodic inspection of infrastructure health status
End User Service Requests	1.6.6.8	Receive, address, and track service requests for LSB and other Infrastructure support from DISA J6	100%	Periodic inspection of service requests status via metrics and customer feedback

Cybersecurity

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Weekly Audit Compliance Scan, and Vulnerability Assessments Reports	1.7.6.4	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
•Weekly TASKORD 17-0019 Compliance Report – Validate compliance with task order checklist	1.7.6.4	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Weekly OPORD 16-0080 Compliance Report – Validate compliance with task order checklist	1.7.6.5	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Ad-HOC System Reports as requested; (e.g. Rouge Sensor Detection, McAfee Antivirus, Data Loss Prevention)	1.7.6.5	Contractor shall submit a current and accurate Ad-hoc Reports as requested	100%	100% Government review of Ad-hoc reports
Agency System/Application Assessment and Authorization Report – Report provides status of all LSB Mission System and	1.6.7.2	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports

Applications and their Authorization status to operate on the DoDIN				
Provide copy of valid DoD 8570.01-M Certifications	1.6.7.6	Contractor shall submit a current copy of 8570.01M certification prior to start of employment and no later than 30 dates after expiration to show renewal	100%	100% Government review of certifications
Weekly or AD-HOC Audits, Inspections and Assessments Reports	1.6.7.7	Contractor shall submit a current and accurate weekly and/or Ad-hoc Reports as requested	100%	100% Government review of cyber security posture
Risk Assessment Report	1.6.7.3	Contractor shall submit Risk Assessment Reports as required	100%	100% Government review of Risk Assessment Reports
Dormant Accounts	1.6.7.3	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports

Cybersecurity Cont.

Service	PWS Reference	Standard	Acceptable Quality Level	Government Surveillance Method(s)
Privileged Accounts	1.6.7.3	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Certificate Installation Files	1.6.7.3	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Account Configuration Firewall Rules/Configuration	1.6.7.3	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Exception Requests	1.6.7.3	Contractor shall submit a current and accurate Annual and Ad-hoc Reports	100%	100% Government review of Annual and Ad-hoc reports
Plan of Action and Milestones	1.6.7.3	Contractor shall submit a current and accurate Weekly Reports	100%	100% Government review of weekly reports
Secret Server Configuration	1.6.7.3	Contractor shall submit a current and accurate Monthly Reports	100%	100% Government review of Monthly reports
Security Logs report	1.6.7.3	Contractor shall submit a current and accurate Daily Reports	100%	100% Government review of Daily reports
Active Directory GPO	1.6.7.3	Contractor shall submit a current and accurate Monthly Reports	100%	100% Government review of Monthly reports
Server and Workstation Image	1.6.7.3	Contractor shall submit a current and accurate Quarterly Reports	100%	100% Government review of Quarterly reports
Ports, Protocols, and Services Management	1.6.7.3	Contractor shall submit a current and accurate Monthly Reports	100%	100% Government review of Monthly reports

Local System Accounts	1.6.7.3	Contractor shall submit a current and accurate Quarterly Reports	100%	100% Government review of Quarterly reports
Daily Task Order Status Tracking Report	1.6.7.8	Contractor shall submit a current and accurate Daily Reports	100%	100% Government review of Daily reports

TECHNICAL EXHIBIT 2
DELIVERABLE SCHEDULE

7.2 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 Government 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. 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 X – DELIVERABLE SCHEDULE

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Program Management				
Transition-In	1.6.2 Phase In/Phase Out period	Contractor Determined	Draft: At time of proposal Final: 5 calendar days after contract award.	Standard Distribution*
Periodic Transition Updates	1.6.2 Phase In/Phase Out period	Contractor Determined	Daily after contractor award, during 30 calendar day transition	Standard Distribution*
Outgoing Transition Plan	1.6.2 Phase In/Phase Out period	Contractor Determined	Initial: 45 calendar days after award (DAA) Updates: 30 days after exercising of any option	Standard Distribution*
Kickoff Presentation	1.6.2 Phase In/Phase Out period	Contractor Determined	15 Business days of ward of the contract	Standard Distribution*
Stakeholder Presentation	1.6.2 Phase In/Phase Out period	Contractor Determined	30 Business days after award of contract	Standard Distribution*
Program Management Plan	1.6.3 Program Management Plan	Contractor Determined	Draft: Evaluated as part of proposal Initial: 45 DAA Final: 90 DAA Updates: 30 calendar days after exercising option	Standard Distribution*

Program Management – Continued

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Program Management Review Meeting	1.6.3 (Refer to FPTS PWS and Exhibit 2	Contractor Determined	To be held monthly	Standard Distribution*

	Deliverables Schedule)			
Programmatic Report / Presentation	1.6.3 (Refer to FPTS PWS Exhibit 2 Deliverables Schedule)	Contractor Determined	Monthly	Standard Distribution*
Resume for Key Personnel	1.6.4 Key Personnel	Contractor Determined	Prior to Employment and Upon GOV Review and Approval	Standard Distribution*
Technical Solution Identification	1.6.5.2 Architectural Engineering and Analysis	Contractor Determined	Two per Quarter	Standard Distribution*
Project & Architectural Engineering				
Project Assessment (TSI Deliverable)	1.6.5.3 Current and Ongoing Projects	Contractor Determined	10 Business days after Assessment Request for Sub-Task Order as required	Standard Distribution*
Technical Solution Identification	1.6.5.3 Current and Ongoing Projects	Contractor Determined	10 Business days after CCB Approval	Standard Distribution
Project Schedules	1.3.2 Integrated Master Schedule	MS Project	10 Business days after Charter Approval	Standard Distribution
Weekly Schedule Updates	1.3.2 Integrated Master Schedule	MS Project	Weekly or as Requested	Standard Distribution

Project & Architectural Engineering – Continued

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Integrated Master Schedule	1.3.2 Integrated Master Schedule	MS Project	Weekly or as Requested	Standard Distribution
Baseline Report	1.3.2 Integrated Master Schedule	MS Project	Weekly or as Requested	Standard Distribution
Milestone Report 2.1.3	1.3.2 Integrated Master Schedule	MS Project	Weekly or as Requested	Standard Distribution
SOPs and WIs	1.6.5.6 P&AE Standard Operating Procedures (SOP) and Work Instructions (WI)	Contractor Determined	As requested	Standard Distribution
Operations and Maintenance				
Training and certifications IAW DFARS 239.7102-3 and DFARS 252.239-7001. Provide valid copy of DODD 8570 IAT Level II Certification	1.6.6.1 Operations and Maintenance Contract Personnel	Contractor Determined	Prior to or start of contract support	Standard Distribution*
Access Management Create/ delete/modify accounts	1.6.6.2.1 Access Management	Contractor Determined / Form 2875	As requested	Standard Distribution*
Incident Management and Response Processes and SOP	1.6.6.2.3 Incident Management and Response	Contractor Determined	See Service Desk	Standard Distribution*

Mission Application Maintenance - After Action Report (AAR) for System Outages	1.6.6.3.7 Mission Application Maintenance	Contractor Determined	Within 24 hours of restoration services for system outages	Standard Distribution*

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Operations and Maintenance - Continued				
Mission Application Maintenance - State of the System Report	1.6.6.3.7 Mission Application Maintenance	Contractor Determined	Monthly 28th of every month	Standard Distribution*
Operations Patching Report	1.6.6.4.3 Patching Report	Contractor Determined	Weekly, Friday no later than 1200	Standard Distribution*
Quarterly Failover Report	1.6.6.5 Failover Testing	Contractor Determined	Due no later than the end of each calendar quarter (i.e. March, June, September, and December)	Standard Distribution*
Problem Resolution After-Action Reports	1.6.6.6 System Monitoring	Contractor Determined	Within seven (7) days following problem resolution	Standard Distribution*
System Backup Plan	1.6.6.7 System Backup and Restoration	Contractor Determined	No later than 30 calendar days following contract award date	Standard Distribution*
Daily Backup Report	1.6.6.7 System Backup and Restoration	Contractor Determined	Daily no later than 0900	Standard Distribution*
Quarterly Data Recovery Test Results	1.6.6.7 System Backup and Restoration	Contractor Determined	Due no later than the end of each calendar quarter (i.e. March, June, September, and December)	Standard Distribution*
Daily Status Report(s) and Briefing	1.6.6.9 Daily Infrastructure Operations Reporting	Government Approved	Daily no later than 0630 on business days; Briefing 0730	Standard Distribution*
Quarterly Large Scale Diagrams	1.6.6.10 Diagrams and Documentation	Contractor Determined	Due no later than the end of each calendar quarter (i.e. March, June, September, and December)	Standard Distribution*
O&M Work Instructions	1.6.6.11 O&M Standard Operating Procedures (SOP) and Work Instructions (WIs)	GOV Approved	As required	Standard Distribution*
O&M Standard Operating Procedures	1.6.6.11 O&M Standard Operating Procedures (SOP) and Work Instructions (WIs)	GOV Approved	As required	Standard Distribution*

Cybersecurity / Information Assurance

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Weekly Audit Compliance Scan, and Vulnerability Assessments Reports	1.7.6.4 Risk and vulnerability assessments	Government approved Contractor provided format	Weekly. Due every Monday and Thursday no later than 1000	Standard Distribution*
Weekly TASKORD 20-0020 Compliance Report – Validate compliance with task order checklist	1.7.6.4 Risk and vulnerability assessments	Government provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*

Weekly OPORD 16-0080 Compliance Report – Validate compliance with task order checklist	1.7.6.5 Host Based Security Systems (HBSS)	Government provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Ad-HOC System Reports as requested; (e.g. Rouge Sensor Detection, McAfee Antivirus, Data Loss Prevention)	1.7.6.5 Host Based Security Systems (HBSS)	Government approved Contractor provided format	Weekly as requested no later than 4 hours after request	Standard Distribution*
RMF Summary	1.6.7.2 Risk Management (RM)	Government approved Contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Agency System/Application Assessment and Authorization Report – Report provides status of all LSB Mission System and Applications and their Authorization status to operate on the DoDIN	1.6.7.2 Risk Management (RM)	Government provided PFPA RMF Project Plan / Contractor Updated and Maintained (Format modifications permitted with Government approval)	Weekly. Due every Tuesday no later than 1200	Cybersecurity Government

Cybersecurity / Information Assurance – Continued

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Develop and Maintain SOP for PFPA mission assets identified in the LSB IT Environment Document.	1.6.7.9 Cybersecurity Standard Operating procedures (SOP) and Work Instructions (WIs)	Stand DISA J6 Format	SOPS reviewed within 30 days of contract award. As Required and Annual Reviews completed thereafter	Standard Distribution
Training and certification IAW DFARS 239.7102-3 and DFARS 252.239-7001. Provide copy of valid DoD 8570.01- M Certifications	1.6.7.6 DOD 8570.01 and Application Certifications	Contractor Determined Format	Prior to start of employment and Monthly report of all required personnel thereafter. Last Friday of each month by 1200	Standard Distribution*
Weekly or AD-HOC Audits, Inspections and Assessments Reports (e.g. Remediation status briefings/ reports)	1.6.7.7 Cybersecurity Inspections	Government approved contractor provided format	Weekly or as requested no later than 4 hours after request	Standard Distribution*
Daily CTO and Task Order Status Tracking Report, Compliance Status and Reporting	1.6.7.8 Daily Cybersecurity Orders Processing	Government approved contractor provided format	Daily no later than 0800	Standard Distribution*
Risk Assessment Report	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Prior to the approval of any changes to the network configuration	Standard Distribution*

Dormant Accounts	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*

Cybersecurity / Information Assurance – Continued

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Privileged Accounts	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Certificate Installation Files	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Account Configuration	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Firewall Rules/Configuration	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Exception Requests	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	30 calendar days after award and every 12 months thereafter. Adhoc reports no later than 4 hours after request	Standard Distribution*
Plan of Action and Milestones	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Weekly. Due every Friday no later than 0900	Standard Distribution*
Secret Server Configuration	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Monthly no later than 1000 on the 28th of every month	Standard Distribution*
Security Logs report	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Daily no later than 1600	Standard Distribution*

Cybersecurity / Information Assurance – Continued

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Active Directory GPO	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Monthly no later than 1000 on the 28th of every month	Standard Distribution*
Server and Workstation Image	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Due no later than the end of each calendar quarter (i.e. March, June, September, and December)	Standard Distribution*
Ports, Protocols, and Services Management	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Monthly no later than 1000 on the 28th of every month	Standard Distribution*

Local System Accounts	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Due no later than the end of each calendar quarter (i.e. March, June, September, and December)	Standard Distribution*
Daily Task Order Status Tracking Report	1.6.7.3 Defensive Security (DS) and Compliance (CP)	Government approved contractor provided format	Daily no later than 1000	Standard Distribution*
Configuration Management (CM)				
Configuration Management Plan	1.6.8 Configuration Management (CM)	Government approved contractor provided format	No later than 30 calendar days following contract award date	Standard Distribution*
Maintenance and Warranty Reports	1.6.8 Configuration Management (CM)	Government approved contractor provided format	Ad hoc reports no later than 4 hours after request	Standard Distribution*
Online Software Media and Document Libraries	1.6.8.1 Software Media and Document Library	Government approved contractor provided format	No later than 30 calendar days following contract award date	Standard Distribution*

Change Management

Deliverable	PWS Section	Format	Due Date, Frequency, and Remarks	Distribution/ Copies
Decommissioning Report	1.6.9 Change Management	Government approved contractor provided format	Ad hoc reports no later than four (4) days after decommissioning approval	Standard Distribution*
Change Management Plan	1.6.9 Change Management	Government approved contractor provided format	No later than 30 calendar days following contract award date	Standard Distribution*
Data Management Plan	1.6.9.1 Data Repositories	Government approved contractor provided format	Draft: 30 calendar days after award Final: 90 calendar days after award Updates: 30 calendar days after exercising option	Standard Distribution*
Continuity Of Operations (COOP)				
Mission Essential Contractor Services (MECS) Plan	1.6.10.1 48 CFR § 237.7603 Solicitation provision and contract clause	Government approved contractor provided format	No later than 90 calendar days following contract award date	Standard Distribution*
COOP After Action Report	1.6.10.1 48 CFR § 237.7603 Solicitation provision and contract clause	Government approved contractor provided format	Within seven (7) days following COOP exercise or actual crisis	Standard Distribution*

TECHNICAL EXHIBIT 3
ESTIMATED WORKLOAD DATA

7.3 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.

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

Base Period

	FTE's	**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
Master Project Scheduler (Key)	1	1872	1872	1872	1872	1872
Operations Manager (Key)	1	1872	1872	1872	1872	1872
Engineering Manager (Key)	1	1872	1872	1872	1872	1872
Principle Systems Engineer	4	7,488	7,488	7,488	7,488	7,488
Senior System Administrator	2	3,744	3,744	3,744	3,744	3,744
System Administrator	8	14,976	14,976	14,976	14,976	14,976
Configuration Management Specialist (Lead)	1	1872	1872	1872	1872	1872
Configuration Management Specialist (Intermediate)	1	1872	1872	1872	1872	1872
Communication Specialist	7	13,104	13,104	13,104	13,104	13,104
Principal Information Engineer	1	1872	1872	1872	1872	1872
Senior Systems Architect	8	14,976	14,976	14,976	14,976	14,976
Cybersecurity Team Lead (Senior IA Analyst) (Key)	1	1872	1872	1872	1872	1872
Intermediate Information Assurance Analyst	7	13,104	13,104	13,104	13,104	13,104
Information Assurance/System Security Architect Level 2	5	9,360	9,360	9,360	9,360	9,360
Information Assurance/System Security Architect Level 3	3	5,616	5,616	5,616	5,616	5,616
Database Administrator	2	3,744	3,744	3,744	3,744	3,744
Labor Total	**54**	**101,088**	**101,088**	**101,088**	**101,088**	**101,088**

Option Period 1

	FTE's	Option Period 1: 12 Months	Option Period 2: 12 Months	Option Period 3: 12 Months	Option Period 4: 12 Months	Option 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
Master Project Scheduler (Key)	1	1872	1872	1872	1872	1872	936
Operations Manager (Key)	1	1872	1872	1872	1872	1872	936
Engineering Manager (Key)	1	1872	1872	1872	1872	1872	936
Principle Systems Engineer	4	7,488	7,488	7,488	7,488	7,488	3,744
Senior System Administrator	2	3,744	3,744	3,744	3,744	3,744	1872
System Administrator	8	14,976	14,976	14,976	14,976	14,976	7,488
Configuration Management Specialist (Lead)	1	1872	1872	1872	1872	1872	936
Configuration Management Specialist (Intermediate)	1	1872	1872	1872	1872	1872	936
Communication Specialist	7	13,104	13,104	13,104	13,104	13,104	6,552
Principal Information Engineer	1	1872	1872	1872	1872	1872	936
Senior Systems Architect	8	14,976	14,976	14,976	14,976	14,976	7,488
Cybersecurity Team Lead (Senior IA Analyst) (Key)	1	1872	1872	1872	1872	1872	936
Intermediate Information Assurance Analyst	7	13,104	13,104	13,104	13,104	13,104	6,552
Information Assurance/System Security Architect Level 2	5	9,360	9,360	9,360	9,360	9,360	4,680
Information Assurance/System Security Architect Level 3	3	5,616	5,616	5,616	5,616	5,616	2,808
Database Administrator	2	3,744	3,744	3,744	3,744	3,744	1872
Labor Total	**54**	**101,088**	**101,088**	**101,088**	**101,088**	**101,088**	**50,760**