APPENDIX A

Pentagon Force Protection Agency

Force Protection Technology Support

(FPTS)

Force Protection Technology Division

Life Safety Backbone (LSB)

Information Technology Environment

Purpose

The purpose of this document is to present an overview of the Force Protection Technology Support (FPTS) Life Safety Backbone (LSB) IT environment.

Scope

The scope of this document is limited to the PFPA Unclassified LSB IT environment and not meant to be a complete inventory or architecture description.

Pentagon Force Protection Agency Mission

Pentagon Force Protection Agency's (PFPA) mission is to provide force protection, security, and law enforcement, as required for the people, facilities, infrastructure and other resources at the Pentagon Reservation and for Department of Defense (DoD) activities and DoD-occupied facilities not under the jurisdiction of a Military Department within the National Capital Region (NCR)". This responsibility includes security of the buildings; Access Control; anti-terrorism and force protection; chemical, biological, radiological, nuclear and explosive (CBRNE) protection and detection; and other key functions. The Agency is divided into multiple directorates, each performing specific responsibilities to carry out the mission of the Agency.

LSB IT Environment

The PFPA Force Protection Technology Support (FPTS) systems are currently made up of unclassified networks (LANs) known as the Life Safety Backbone, Coral Network, and Metropolitan Area Networks (MANs) located at the "Pentagon Reservation" and within the "National Capital Region" as defined in 10 U.S.C. 2674. This includes but not limited to the Pentagon, Defense Health Headquarters (DHHQ), The Mark Center, Military Court of Appeals, and Raven Rock Mountain Complex (RRMC).

The current PFPA LSB architecture is centered on the Microsoft Windows operating systems platform (i.e. Windows 10/11, Server 2016, 2019, 2022, etc.). There are Linux, MSSQL, Oracle databases, COTS, GOTS and custom software-based applications/systems connected to the network. Currently there are approximately 500 LSB user accounts and over 500 Workstations, The virtual environment comprises 407 virtual machines distributed across five geographically separated sites. The workload mix spans the full application stack with SQL database servers, application servers, Active Directory domain controllers, and end-user workstation VMs. Each carrying distinct performance, availability, and security profiles and requirements. Operating across five sites adds meaningful complexity in data flow, replication, and service continuity. Domain controllers must sustain consistent indemnity and authentication services across all locations; the SQL and application tiers carry latency-sensitive dependencies; and VMs require reliable session delivery to a distributed user base. While the virtualization layer and systems

running on it are within scope, the underlying inter-site network connectivity is owned and managed by DISA. This division of responsibility demands close, effective, working coordination with the network authority; allowing the ability to maintain reliable performance of the virtual environment without owning the transport layer.

In support of our mission, PFPA relies on the Defense Information Systems Agency (DISA) J6 for Desktop/ Common IT functions and support. This support does NOT include support for the LSB infrastructure and desktop environment. The LSB infrastructure and the desktop environment support will be covered under this FPTS requirement.

PFPA has a layered network defense architecture, including firewalls, routers, intrusion detection systems, anti-virus software and an established Demilitarized Zone (DMZ) providing protection from intrusion via external systems and networks. The PFPA Innovation Office (PIMO)/JPP is responsible for complete oversight of the LSB IT environment and requires support for the PFPA LSB Systems Infrastructure specific to PFPA mission needs. This includes but is not limited to the following:

- Hardware, Software, and Network Components Maintenance Services.
- Hardware repair maintenance for PFPA infrastructure components (see Appendix A Systems and Device Counts).
- COTS and GOTS software (see Appendix A Systems and Device Counts).
- Meeting incident response per Mission Criteria and application or system (see table 3).
- Software maintenance support services for Microsoft products, Oracle Database, LINUX, antivirus, network and infrastructure monitoring and management tools (see table 4).
- Continuous tracking of all PFPA LSB assets electronically within the Enterprise Logistics Management System (ELMS).
- Support for current and future projects (see table 5)

The PFPA LSB Environment also includes operations and maintenance support for law enforcement cruisers with approximately 50 Toughbooks; and 1 Tactical Command Vehicle (TCV). The TCV IT assets consist of an additional 2 servers, 7 Toughbooks, 2 laptops, 1 network consisting of Cisco 2811 Router and one Catalyst 3560-G, and satellite communications equipment supported by a 3rd party vendor, Knight Sky.

PIMO/JPP utilizes a MS SharePoint site as the primary repository for storage and access of SOPs, Work Instructions, Forms, etc. The site is broken down by several sub-sites (i.e. Engineering and Architecture, Information Assurance, Operations, Taskers, FPTD Change Management, Policy and Governance, Transition Library, and Program Management). This will be the central knowledge base used for a successful transition.

INCIDENTS/ MAINTENANCE (PLANNED/ UNPLANNED)

During the past year (12 months) the PFPA PIMO/JPP supported the following number of incident/service requests:

- Serviced (640) LSB incident requests over the last consecutive 12 months (approximately 54 averaged per month)
- Serviced (2782) LSB service requests over the last consecutive 12 months (approximately 231 averaged per month)

- Approximately (42) Planned maintenance outages for LSB IT systems over the last consecutive 12 months, averaging (3) per month. (this includes, patch management & scanning)
- Approximately (90) Planned building maintenance power

DISA/JSP IT Hosted Environment

DISA/JSP's IT environment (USER domain) is an unclassified network consisting of common IT services (e.g., e-mail, file, print, storage, telephones and mobile device operations). DISA J6 has full operations and maintenance responsibility over this environment.

PFPA has mission specific applications (e.g. Computer Aided Dispatch and Reporting Management System (CAD/RMS), Workforce Telestaff, WebEOC, and Visitor Management System (VMS) that reside on the DISA J6's IT hosted environment. These applications are considered LSB applications and may require support (application only) as part of the FPTS requirement (see table 5).

IT Cloud Environment

DoD Cloud Environment:

PFPA has approximately 4 cloud environment projects ongoing:

- Salesforce – PFPA Recruit Management Tool
- Metrological Modeling System (MMS) – CBRNE Weather Modeling
- PFPA Intranet Extranet Website (PIEWS) – PFPA internal website
- Counter Small Unmanned Aircraft Systems (C-sUAS)

The cloud projects listed above will have shared responsibility for management, security, and administration. The vendor is responsible for at a minimum, support for RMF work to achieve ATO.

Historical Environment / IT Environment Staffing Estimate

(For Information Purpose Only)

Based on the FPTD's current operations tempo and increasing workload, PIMO/JPP subject matter experts have estimated the following number of full time equivalents (FTEs) would meet the FPTS requirements. This information is based on 2080 hours per FTE:

- Program Management (1)
- Operations (19)
- Engineering (11)
- Cybersecurity (12)
- Asset Management and Inventory (4)
- Change Management (1)
- Configuration Management (1)

Example of position descriptions

Labor Category	Description
Task Order Project Manager	FPTS Program Manager
Project Control Specialist	Project Manager. Responsible for ensuring project management plans (as defined by PMI) are developed and available for GOV and stakeholder access
Information Engineer - Intermediate	Assigned to assist with project management
Operations Manager	Lead - Managing Daily Operations, Service Desk, Systems Administration, and Network Operations
Senior Hardware/Software Installation Technician	Deployment/Delivery Lead
Documentation Specialist	1 assigned to work with Project Manager and 1 assigned to Configuration/Change Management
Principal Systems Engineer	Lead
Senior Systems Administrator	Lead – SysAdmin specific
System Administrator	Support is required to focus on O&M, patching, engineering support, monitoring, conducting surveys, backup and recovery, imaging management, and implementing efficiencies. Skillsets should include proficient knowledge with automation and monitoring tools (e.g. Solarwinds SAM, MS System Center Configuration Manager (SCCM), VEEAM (backup and recovery), VMWare, etc.) in addition to the platforms identified within the PWS.
Configuration Management Specialist (Lead)	1 position responsible for configuration management and 1 for change management
Enterprise Communications/Network Manager	Lead – NetOps specific
Communications Specialist	NetOps support personnel required to provide sufficient support to the PFPA (i.e. monitoring, troubleshooting, conducting surveys, submitting requirements to DISA J6, and O&M of networking devices within the NCR)
Principal Systems Architect	Establishes system information requirements using analysis of the information engineer(s) in the development of enterprise-wide or large-scale information systems
Senior Systems Architect	Designs 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
Senior Application Engineer	Analyzes and studies complex system requirements. Designs software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manages software development and support using formal specifications, data flow diagrams, other accepted design techniques and Computer-Aided Software Engineering (CASE) tools
Logistics Analyst (Lead)	Lead Asset Manager

Example of position descriptions

Labor Category	Description
Logistics Analyst (Intermediate)	Asset Management support. Annual 100% inventory requirement, and asset control.
Senior Information Assurance (IA) Analyst	Team Lead – 1 (IAM Level III Certified)
Intermediate Information Assurance (IA) Analyst	Support focused on ACAS(All areas of scanning and remediation tracking), RMF (20+ systems/applications AA and AO's), HBSS (management of the EPO and all associated tasks)
Information Assurance/System Security Architect Level 2	Provide input and expertise guidance on acquisition, design, implementation, and environment changes.
Information Assurance/System Security Architect Level 3	Focused on Team support for all areas
Database Management Specialist	Lead – Database specific
Database Administrator	Assigned to implement, monitor, code, test, troubleshoot, ensure backup and recovery, etc.)

Table 1: PFPA Infrastructure System Components

This is an approximate listing of systems residing on the PFPA Infrastructure. The contractor shall be responsible for continuous monitoring and oversight of the LSB Systems to include the cybersecurity and operations requirements described in the PWS. Additional systems are located in the Systems and Device Counts Appendix.

LSB IT Environment	Short Description
IT Management Tools	ACAS, Active Directory, DameWare, HBSS, OCSP, SolarWinds, Splunk, SCCM, VMWare,
Meterological Modeling System	Chemical Biological Radiological (CBR) System Division (CSD) Exterior Modeling System
Sentry	Chemical Biological Radiological (CBR) System Division (CSD)Environmental Monitoring
LIDAR	Chemical Biological Radiological (CBR) System Division (CSD) Exterior Modeling System
Laboratory Information Management System (LIMS)	Chemical Biological Radiological (CBR) System Division (CSD) Labratory Information Management System (LIMS)
Privileged Management Program (PMP) (Access Management Portal, VMS)	EPSD -Identity Control and Access Management System
AMAG	Access Control and Intrusion Detection System (ACIDS). A component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC).
CCURE 9000	Access Control and Intrusion Detection System (ACIDS). A component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC).
Bosch Video Management System (BVMS)	CCTV System supporting the Video Surveillance Program
Activu	Pentagon and Mark Center video Wall Display system
Under Vehicle Inspection System (UVIS)	A threat deterrent component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC).
Mobile License Plate Recognition (LPR)	Parking Enforcement component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC)
Physical Security Information Management (PSIM) System	Multi-system (i.e. AMAG, CCURE, BVMS, SENTRY) common operating picture (COP).
Future Fibre Technologies (FFT) Aura	A threat deterrent component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC)

Table 2: PFPA Infrastructure System Components Cont:

LSB IT Environment	Short Description
Virginia Criminal Investigative Network (VCIN)	Virginia State Police statewide data communications network
Mark Center Active Vehicle Barrier System	Physical Security Barrier Control System
Active Client	Smart Card middleware, allows easily use of smart cards for desktop and productivity applications
Static Vehicle Screening System (SVSS)	A threat deterrent component of the Electronic Security System located at Mark Center, Defense Health Headquarters, and Raven Rock Mountain Complex (RRMC).

PFPA Mission Systems Incident Response Posture

PFPA uses multiple missions' systems and technologies to perform it force protection mission. PFPA has defined these Mission systems and applications which are significant to the efficient response of any type of Security, Law Enforcement and Life Safety situation. In the event these systems are inoperable or degraded the contractor shall triage these incidents in accordance with the following Incident Response Posture.

PFPA Mission Critical Applications /Systems

A system whose operational effectiveness and suitability are critical to successful completion of the force protection mission. If this system fails, the mission likely will not be completed. These applications are required to be highly available and resilient. They must have a disaster recovery and a continuity of operations plan. Lives are at stake.

Mission Critical Support Response Posture: Subject Matter Expert (SME) support for all aspects of JPP-provided infrastructure available 24/7/365. Tickets generated for Mission Critical Applications should be URGENT - CRITICAL IMPACT (Priority One) tickets and acknowledged within ten minutes of notification. Critical tickets shall be resolved within 2 hours.

- **Mission Critical Systems/Applications**
  - Access Control and Intrusion Detection Systems - Electronic Security Systems
  - Meteorological Modeling System - MMS
  - E911
  - Bosch Video Management System (BVMS) - Bosch CCTV system

PFPA Mission Essential Applications /Systems

A system whose operational effectiveness and suitability are essential to successful completion of the force protection mission. If this system fails, the mission will be impacted but does not signify mission failure. These applications are not considered basic and required to be available for mission accomplishment. They must have a disaster recovery and a continuity of operations plan.

Mission Essential Applications: Support Response Posture: SME available 24/7/365. Tickets for Mission Essential Applications should be HIGH - SIGNIFICANT IMPACT (Priority Two) and acknowledged within 10 minutes of notification. High Impact tickets shall be resolved within 8 hours.

- **Mission Essential Systems/Applications**
  - ACTIVU - CAC Authentication (OCSP)
  - Physical Security Information Management (PSIM)
  - Privilege Management Program (PMP)
  - SENTRY/ Pentagon Shield - CBRNE Environmental Monitoring
  - Computer Aided Dispatch (CAD)
  - PIMI (MS Access - SQL Server)
  - Records Management System (RMS)
  - Visitor Management System (VMS)

Mission Support Applications

A system whose operational effectiveness and suitability support the successful completion of the force protection mission. If this system fails, the mission will be impacted but does not signify mission failure.

Mission Support Applications: Support response posture: SME during business hours. Tickets for Mission Support Applications should be NORMAL - MINOR IMPACT (Priority Three) and acknowledged within 10 minutes of notification. Normal impact tickets should be resolved within 24 hours

- **Mission Support Systems/Applications (This list is not all inclusive)**
    - VCIN
    - LIDAR
    - VMware - vCenter Software
    - WEBEOC
    - Static Vehicle Screening System (SVSS)

Table 3: Special Knowledge and Experience

This is an approximate listing of knowledge and experience needed to perform the requirements listed in the Performance Work Statement. This list includes monitoring, management, and administrative tool critical to the operations and maintenance to the LSB Systems architecture.

Microsoft desktop/server operating systems;
Server Administration
Business and Disaster Recovery Planning
Remote Access Technologies
Satellite Communications
Storage Area Networking
Virtual Storage Platform
Enterprise Patching Solutions
Microsoft Endpoint Configuration Manager
Active Directory
Network Node Manager
VCenter/vCloud
Network Monitoring Tools (e.g. Solarwinds)
Cisco and Juniper network device administration
Various brands of server hardware (e.g. HPE, Dell, etc.)
Redhat Linux
Configuration Management and Change Control;
Microsoft Server
Microsoft SharePoint
Microsoft Azure Government
Amazon Web Services
Microsoft SQL Administration
Veeam Availability Suite
Splunk
Host Based Security System (HBSS)
Assured Compliance Assessment Solution (ACAS)

Table 4: LSB Engineering Projects

The following table is a list of projects that has been assigned to Projects and Architectural Engineering. The Priority 1 Projects are actively being worked and the expectation is that these are the projects that will continue to be worked upon Task Order award. The Priority 2 projects are supporting type where JPP is coordinating with other government agencies to provide the transport for our stakeholder's project. The Priority 3 project is completing an analysis and making a recommendation to LCR the LSB network.

Project Title	Project Description	Current Status	Expectation
PaaS LCR	The Contractor shall be responsible for the turn-key lifecycle replacement of the existing PAAS1 with new PAAS2 hardware, virtual machine and storage migration, and upgrade of the virtualization platform to vmWare vSphere v8.	Working on installation of equipment, configuration, and closeout.	Coordinate with DISA on network requirements, optimize storage, and complete installation.
Agency-wide Workstation Life Cycle Refresh	LCR of all LSB workstations	An assessment of the Agency-wide was conducted, Bill of Materials was developed, and a procurement is being developed.	A deployment plan is required to include, but not limited to, inventory, transport, imaging, communication plan, deployment schedules, testing.
Integration of LIMS to LSB	Integrate the CBRNE lab system into the LSB network	Planning and developing	Assessment and full integration
LSB Lab	Assess plans and location for an LSB lab environment	Assessment and planning	An on-site lab for LSB testing
Server Migration	Migration from 2016 to 2019/2022	Assessment being developed	Complete assessment, plan, and execute
LSB Modernization	LSB Modernization Roadmap	Assessment required	Develop a plan and way ahead of the future of LSB

Table 5: DISA/JSP IT Hosted Environment

The Following is an approximate list of applications/systems hosted on the DISA/JSP network

DISA/JSP IT Hosted Environment	Short Description
Visitor Management System	Web-based Visitor Registration System
WebEOC	Collaborative Emergency Management System
Computer Aided Design (CAD)	Law Enforcement Event/Incident Recording and Reporting System
Records Management System (RMS)	Law Enforcement Event/Incident Recording and Reporting System
KRONOS Telestaff	Public Safety Automated Scheduling Solution