Exhibit 2.3.1

Solution – Mainframe Services

VA-240322-PSLI - Mainframe Services

COMMONWEALTH OF VIRGINIA

VIRGINIA IT AGENCY (VITA)

SUPPLIER STRATEGY AND PERFORMANCE DIVISION

7325 BEAUFONT SPRINGS DR

RICHMOND, VA 23225

TABLE OF CONTENTS

2.0   Common Services

Using our Mainframe Services Team, a CMMI for Service Level 3 assessed and certified delivery organization, we monitor, maintain, and manage VITA's Mainframe environment (Mainframe, storage and network hardware and communication circuits) and system software configurations through 24x7x365 service that aligns with the requirements provided in the Agreement documentation.

Peraton proactively monitors VITA's Mainframe infrastructure with the available tools currently in use, supplemented by automation to support availability and performance objectives. Daily activities within our support services include Mainframe initial program loads (IPL), batch monitoring and remediation, performance and capacity monitoring, and ticket management. The monitoring team escalates and assists on triage conference calls during outages that affect VITA, including participating and collaborating with the VITA Joint Operations Center and other Service Tower Suppliers.

We provide 24x7x365 operations and technical support in sustainment of VITA, DMV, and DSS mission objectives. This includes running daily operations, maintaining / upgrading the hardware and software used in the Mainframe environment, monitoring security, capacity, performance, and cross-functional integration across Multi-Sourcing Service Integrator (MSI), and the Service Towers. Using the Mainframe Services Team currently delivering Mainframe services to VITA, our technical support personnel are responsible for the following actions:

- Monitoring the VITA Mainframe environment, to include hardware, software, networks, and security.
- Managing Mainframe infrastructure, including compute and storage for availability, capacity, and performance.
- Providing database and database administration support.
- Performing system backups and restores.
- Planning, staging, executing, and testing scheduled changes.
- Providing Level 2 and Level 3 incident and problem management.
- Conducting software installation, maintenance, and updates.
- Performing preventive maintenance
- Providing audit support
- Planning and supporting business and service continuity (DR).

To deliver these services, our team, as illustrated in **Figure 1,** is organized to promote reliable and efficient Mainframe operations that address all aspects of the required services.
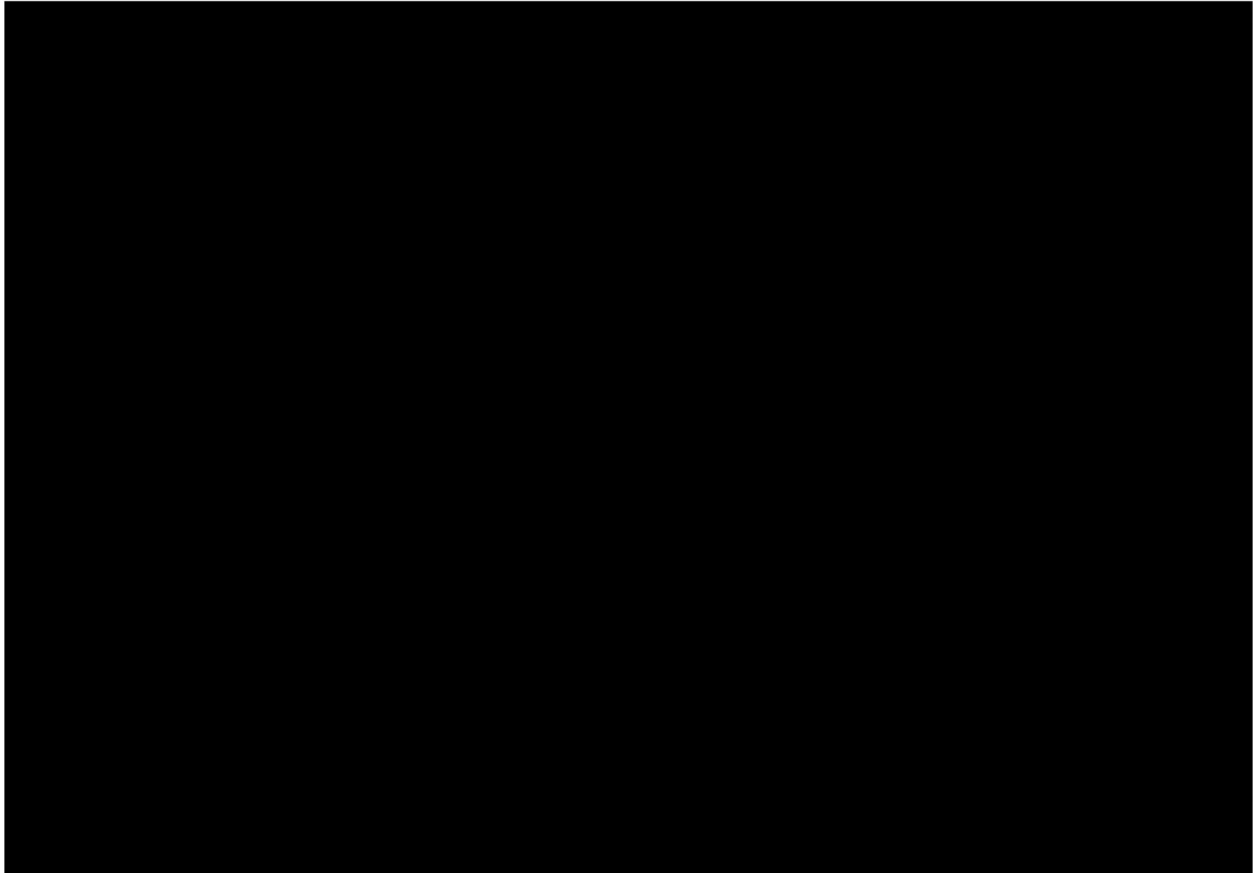
We have a process to collect resource items (e.g., storage, user accounts) owned by the migrating Customer and collaboratively review each item to confirm an appropriate disposition. Once reaching consensus on each item the Customer uses that information to submit a series of requests which the Mainframe Services Team fulfills. The result is a documented, orderly exit from the Mainframe reducing stranded resources and unintended loss of resources such as accounts which may be required for other business purposes. Our team provides consistency, reliability, responsiveness, secure operations, and continuous improvements and innovation in support of each VITA agency. This includes:

- Focusing our business efforts on anticipating and responding to VITA's needs.
- Complying with quality models, frameworks, VITA Rules, and Commonwealth of Virginia and international standards for security, privacy, and service management, as defined in our contracts.
- Identifying and implementing process improvements and task automation to maximize efficiency, as well as customer and VITA satisfaction.
- Refining process improvements through newer tools and techniques and training Peraton staff to continually excel.

> **VITA Outcomes:**
> - Continued reliable, predictable, secure, and efficient IT Mainframe services
> - Seamless, non-disruptive transition to new contract and services
> - High executive branch/agency level service delivery visibility
> - Transparency into IT costs at the agency level
> - Faster business processes and IT service deployments
> - Ongoing IT innovation and continual improvements

We apply the latest technical and operational improvements, along with best practice support aligned with ITIL and industry standards, and resilient security measures for our overall Mainframe solution. We

collaborate with VITA to adopt a holistic, end-to-end approach, with a solution that transcends compartmentalized service component architecture. **Figure 2** illustrates our robust approach to VITA Mainframe operations and services.
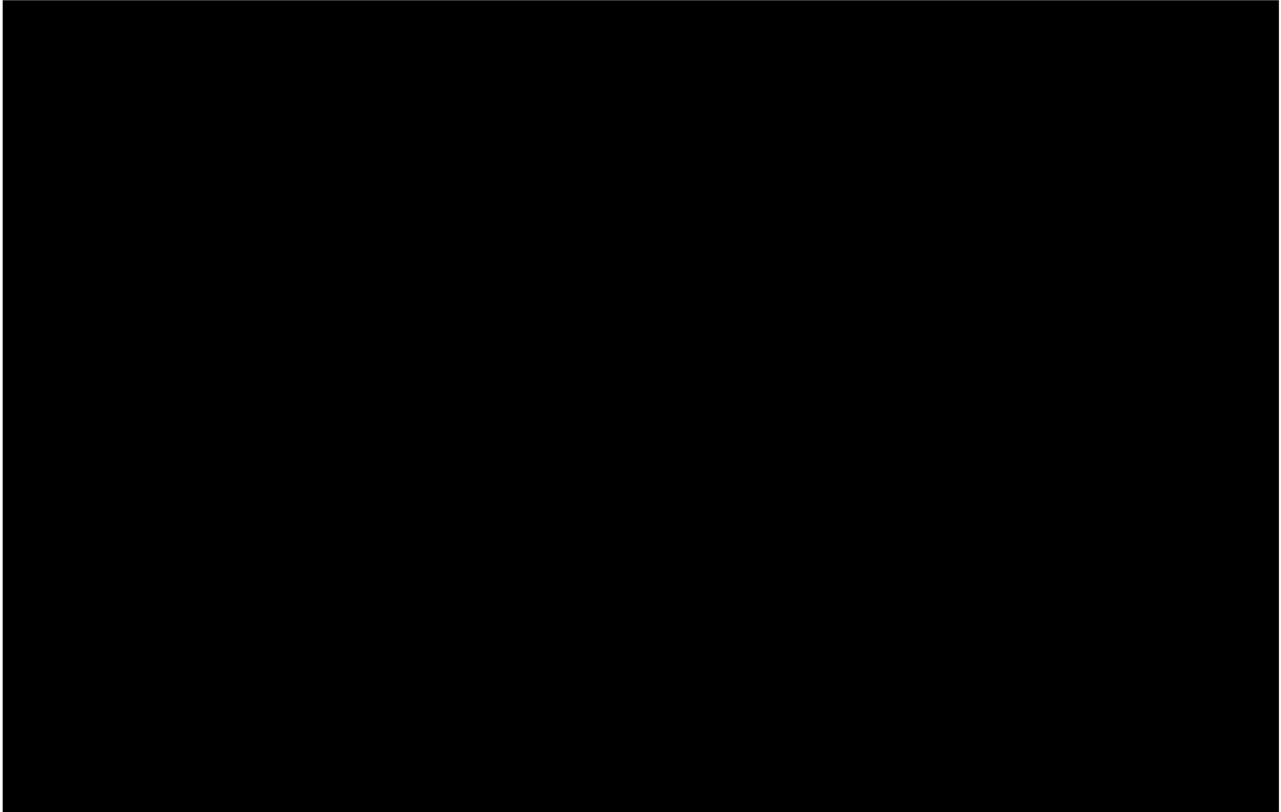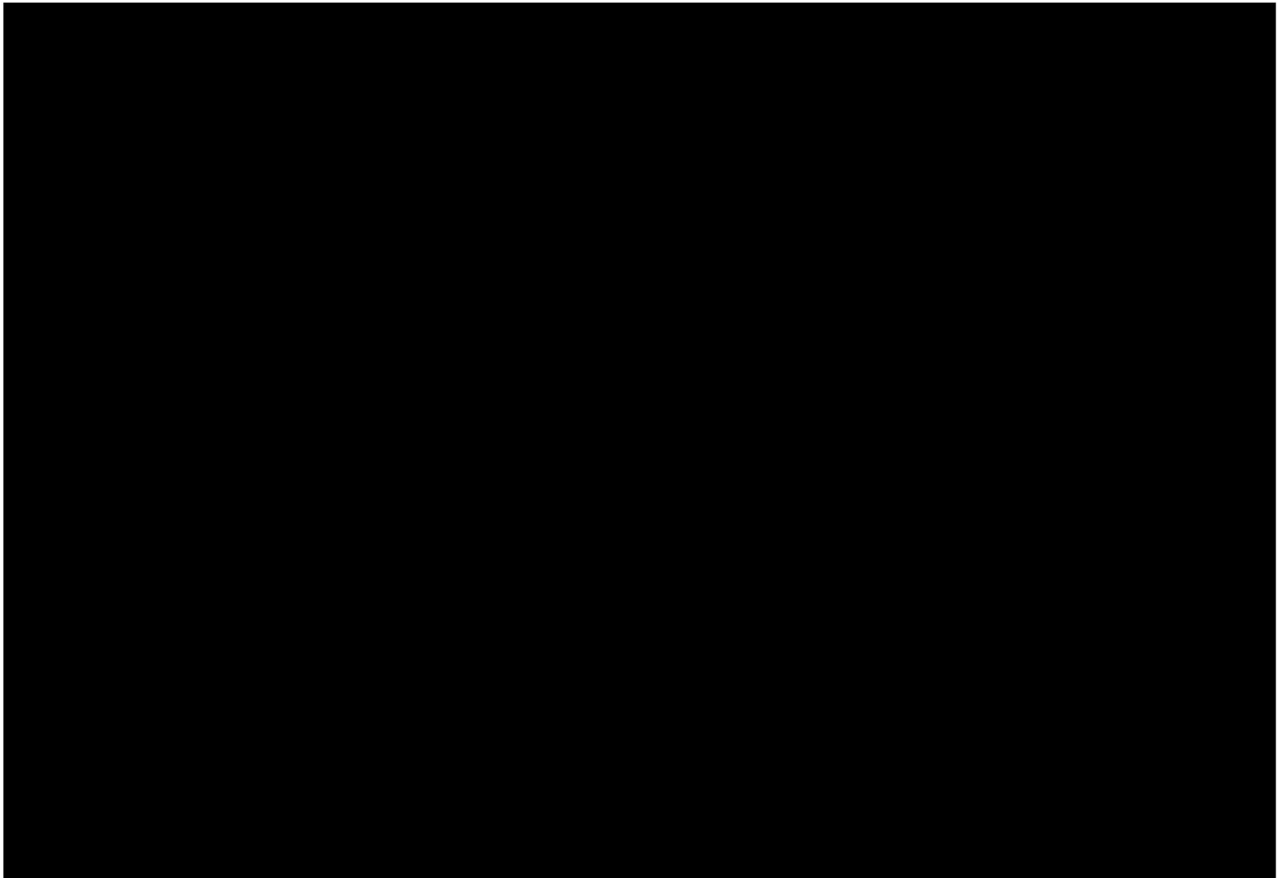
The Peraton Mainframe architecture above, depicted at a high level, includes multiple features that address availability and security. Key features include:

- Redundant, geographically diverse MPLS circuits between the VITA Sandston, VA, datacenter, and the VITA Dedicated MPLS Network managed by Peraton, eliminating single point of failure that would impact VITA users and customers.
- Redundant, geographically diverse MPLS circuits between the Peraton MDC data center and the VITA Dedicated MPLS Network managed by Peraton.
- Federal Information Processing Standards (FIPS) encryption across network pathways to protect VITA data in transit.
- Firewalls between sites, and compartments segregate processing from other critical functions providing layers of security further strengthening VITA's security posture.
- Geographic diversity between the Peraton MDC (primary site) and the Colorado Springs DR facility to negate any impact of natural and man-made disasters to DMV and DSS.
- The Table 1 below reflects our current hardware sizing and configuration. If one of the two Agencies currently on the Mainframe migrate off of the Mainframe, Peraton may change (right-size) the hardware configuration, including a smaller Mainframe.
- Storage sizing notes the amount targeted for allocation as well as the total size available within the solution to accommodate any fluctuations in usage requirements. Our pricing is based on the targeted allocations leveraging Dell's Flex on Demand solution where we are charged for actual usage but have additional capacity if needed.

Peraton works closely with VITA in contributing to agency wide IT plans. We develop and maintain currency of the long-range, comprehensive Technology Plan for VITA's Mainframe systems, processes, technical architecture, and standards. Continuing into the next contract, we plan to update the VITA infrastructure through a Mainframe and storage refresh activities that will provide VITA with access to the latest technology throughout the contract term.

2.1 General

Our approach to the required services is consistent with the delivery model that we have used successful to deliver Managed Mainframe to VITA since 2017. This approach includes consistency of processes, procedures, tools, and staff along with demonstrated collaboration with VITA, the MSI, and Service Towers Suppliers (STS). As a technical interface to the VITA, VITA Customers, the MSI and Service Towers, our approach to collaboration provides the keystone for successful Mainframe operations, security, and support.

Approach to Maintain Security Practices

Our security management approach is compliant with VITA requirements, policies, and procedures and we understand our responsibility to protect the environment. We have implemented the latest processes and

technologies to mitigate risk and potential business disruption. Our approach and experience managing risk to VITA Mainframe environment enables us to quickly identify threats to the environment, including the networks, applications, system components and subcomponents and to subsequently neutralize them. Our security management approach is described in detail in Section 4.0 Security Requirements. Maintaining the Confidentiality, Integrity, and Availability of Mainframe customer data is Peraton's focus which we accomplish through multiple defensive layers including the following:

- **Qualified personnel** – Our staff are trained and have the experience to apply appropriate controls and configurations on data, applications, Mainframe hardware and backup/disaster recovery infrastructure, networks, security perimeter equipment such as Firewalls, IDS/IPS, and telecommunication circuits.

- **Multifactor Authentication (MFA)**

  Current MFA capability: There is no current MFA capability within the solution beyond the existing licensing of CA Advanced Authentication for Mainframe (software installed but not activated by vendor license code).

  Services and supports included in base offering: Peraton's solution includes utilizing and configuring the existing software toolset per VITA requirements to integrate with VITA's chosen MFA solution, Okta, collaborating with VITA and Customers to understand the impact of implementing MFA, and supporting VITA in defining and analyzing the requirements for implementing MFA on the Mainframe. Since these activities are in-scope there is no additional charge.

  Services under a Request for Solution: After working collaboratively with VITA to develop the MFA scope and requirements, Peraton will propose a solution via the Request For Solution (RFS) process to support implementation of MFA and adding required capabilities beyond those which are part of the existing Mainframe solution. Peraton's RFS solution will include 40 hours of labor performed by Mainframe project support resources to perform MFA implementation tasks at no charge. These 40 hours will be utilized for software installation and configuration, mainframe security system and operating system configuration, and network configuration and these 40 hours will begin to be tracked upon approval of the MFA RFS by VITA. These first 40 hours will not be charged for meetings, discussions, or collaboration sessions. We use the RFS process to track labor hour expenditure during execution and monitor for progress towards the 40-hour trigger point. Additional labor hours beyond the 40-hour trigger point will be charged to VITA as incurred to complete the project. RFS solution components which are outside existing capabilities, such as a software product that is necessary but not currently licensed to VITA or Peraton, hardware components such as tokens or appliances, or additional support server instances, may trigger additional costs.

  To solidify the path to MFA, we will need to have significant discussion and collaboration with VITA to develop the requirements, schedule, dependencies, etc. This work with VITA will likely involve deploying and integrating CA Advanced Authentication for Mainframe 2.0 with existing ACF2 instances, and Okta capabilities. This project will allow Peraton to plan, design, and test the MFA solution to avoid disrupting VITA users and business while increasing access security to the VITA Mainframe environment. The VITA Mainframe is currently not configured to use MFA, which is considered an advanced authentication for the Mainframe. For successful advanced authentication Mainframe sign on, the application performing the sign on validation must support password phrases and provide user data entry field for changing credentials by entering an old password and replacing it with a new password.

  The current in-flight project of changing from 8-charater passwords to 14-character passphrases will require accommodation within any activities to implement MFA capabilities at the mainframe. We are working closely with DMV and DSS to conduct testing prior to implementing password changes in production. As MFA capabilities are deployed across the VITA enterprise and for non-COV users, including laptops, desktops, and other devices, Peraton will introduce appropriate compatible solutions to integrate the Mainframe with VITA's MFA infrastructure as required by VITA.

- **Logging** – We support system logging and retention of logs representing all user, access, application, system, and network changes/actions, including customer provisioning and administrative activities. The logs are the means of continuous monitoring and used for analysis, detective, and preventive actions against active and potential threats. Appropriately formatted logs can be integrated with the Managed Security Service (MSS) SIEM for enterprise level correlation and monitoring. Logs will be retained and integrated for required retention periods.
- **Data Protection** – We prevent accidental or deliberate exposure to data through compliance with confidentiality standards. We enable system entry validation, resource control, auditability, accountability, and administrative control, including secure user access management through ACF2 managing user authorization and access, including securely issuing administrative credentials to users with administrative rights. We support security event management of user activity by collecting, retaining, forwarding, and responding to events identified through user access and system logs originating from ACF2 and other Mainframe tools and log generators.
- **Data Encryption** – We will maintain data security and integrity by encrypting data at rest and in transit at all times within our solution. We use hardware and software-based data encryption features on the storage, as well as transmission circuits in compliance with FIPS 140-3 encryption standards. Additional details relating to our data encryption strategy, technologies and processes are documented in Sections 4.1 General Security Requirements and 4.1.6 Full Disk Encryption.

Approach to Collaboration

Effective collaboration and relationship management is critical to ensuring the services provided by different suppliers collectively deliver high-quality, integrated IT services that align with VITA and VITA Customer strategic goals. Peraton serves as the primary technical interface for the Mainframe Service in the VITA ecosystem. We build and maintain relationships with the other Service Tower Suppliers (STS) by participating on Governance Forums, such as the Platform Service Delivery Forum, collaboration during Incident Resolution efforts, joint planning sessions for implementations, negotiating and maintaining Operating Level Agreements (OLA), and through informal one-to-one interactions to share knowledge and perspectives. The Peraton Account Executive and Account Manager are available as points of contact who can respond to requests or issues or make connections into the Peraton organization to collaborate and resolve issues.

Our team maintains cross-functional awareness of MSI and Service Tower operations, the interdependent systems and process, and organizational priorities to promote collaborative interactions, removal of barriers, and resolution of conflicts vertically and horizontally through the organization. Beyond other formal and informal means of collaboration, the MSI's Service Management System (SMS) is a key mode of communication that promotes collaboration. Timely updates and reassignments to Incident tickets, detailed change requests, and service requests within Keystone Edge (KSE) foster an environment of teamwork and mutual support in the mission of IT service delivery to VITA Customers. In instances where two or more STSs do not agree on a topic or lines of responsibility are not clear, Governance Cases are used to achieve clarity and resolution and document decisions and outcomes.

2.2   Operations, Maintenance, and Monitoring

Peraton performs all Mainframe service operations, maintenance, and monitoring functions following VITA's standards and requirements, augmented by our CMMI for Services assessed and certified Mainframe Delivery Framework (MDF). Our MDF is a suite of processes, tools, and methodologies aligned with VITA requirements and based on industry best practices from PMI, ITIL and ISO.

Automation and Preventative Maintenance: Peraton operates and monitors all Mainframe computer platforms and infrastructure using current VITA Mainframe tools, processes, and installed software. With these tools we monitor for system alerts that read the Mainframe System Management Facility (SMF)/RMF data, syslog, Customer Information Control System (CICS), and database logs and other performance data to

control all aspects of the Mainframe environment. We monitor, detect, and report system problems and use automation to proactively identify warning signs of potential issues and to resolve identified issues. Peraton's operation, maintenance and monitoring process includes a focus on preventative maintenance across all the above components (HW, SW, security) to identify and prevent issues from occurring. This includes performing all maintenance according to the manufacturer's specifications and providing documentation verifying that preventive maintenance has been completed including change records, OS and firmware versions and current support levels.

Maintenance activities are performed both as normal scheduled activities, and when required, performing emergency Systems Maintenance as critical incidents occur, to maintain system and application availability. As an example, we have implemented automation that monitors Direct Access Storage Device (DASD) storage replication to the disaster recovery site, alerting the operations team for immediate action to diagnose the loss of replication and restoration of the service. Implementation of this automation reduces the risk of "out of sync" data storage status and provides the integrity of the DR solution. Key performance indicators we use include CPU utilization trending (MIPS) and storage utilization monitoring by storage group/pools (Database, CICS, GDGs, PDS, SMS Managed).

Hardware Maintenance Approach: Hardware Maintenance Services provides the requisite activities to maintain the VITA Mainframe environment according to the manufacturer's specifications and allows Peraton to resolve problems. We engage with Mainframe hardware environment vendors, including IBM and Dell/EMC to regularly assess hardware maintenance issues. Within this activity, we schedule and perform emergency and preventive maintenance, including microcode updates, firmware updates, and other hardware maintenance tasks to maintain system availability and performance. Managed in conjunction with the established change management process, we maintain tracking and visibility through change management reporting of the maintenance activities.

Software Maintenance Approach: Software Maintenance Services provide the activities to manage deployed software in the VITA Mainframe environment. We maintain relationships with deployed software vendors, to include IBM, CA/Broadcom, BMC, and other product vendors to effectively manage deployed software. Specific activities include:

- Software Life-Cycle Management for each software products, including maintaining visibility of operational and End-of-life/End-of-Service (EOL/EOS) status, and any changes and enhancements in between. By maintaining software currency, we plan for upcoming software changes that minimize vulnerabilities and disruption to VITA and its customers.
- Software Patch Management as described in Section 2.3 Patch Management. We plan, implement, and track patches required to maintain currency, system integrity, availability, and performance of all software through its life cycle. Our services include assisting users with application support issues based on root cause analysis from incidents, and analysis of utilization and performance data captured.

We perform hardware and software maintenance services according to manufacturer's specifications, and we maintain documentation of all changes, including routine and preventive maintenance.

Security Support Services: The complete scope and scale of our security services for the Mainframe environment and the managed networks including daily operations and the monitoring of the Mainframe environment and networks, can be seen in Section 4.0 Security Requirements. We select, implement, and configure security controls including access, authorizations, and passwords based on data criticality, the potential risks, and emerging threats to the Mainframe environment. As seen in Section 4.3 Risk Management, we manage the lifecycle of security controls using NIST RMF methodical approach including internal and external assessments and audits to ensure their continued efficacy in tune with the current standards and emerging threats. We provide audit and compliance support through SMEs with environment, VITA, and industry security knowledge. We monitor operational status of the Mainframe environment through log collection and correlation, with enabled capability to forward the logs to VITA MSS supplier and SIEM.

Service Management and SLAs: A key component of Peraton's operation, maintenance and monitoring process is service measurement and the management of Service Level Agreements (SLAs). Peraton aligns to VITA's Service Measurement process and approach as described in **SMM 4.1.6.3 Service Measurement**, designing measures that reflect the overall objectives of VITA and how they are incorporated into the delivery of Mainframe Services and the applicable SLA's. Key components of our Service Measurement process include the following:

- Focus on the needs of VITA to improve quality, performance, value, and process compliance, both qualitatively and quantitatively.
- Capture the availability and performance of mainframe services with a focus on end state service results.
- Reduce risks and provide cost control and optimization.
- Integrate and use Information Technology Infrastructure Library (ITIL), PMI, ISO, and other industry standards.
- Provide the tools for measurements of service performance within the entire services life cycle.
- Collect Metrics and KPIs to support all services.
- Identify service improvement opportunities.
- Design Services to allow for the monitoring and measurement of Service Levels and other metrics and the addition/modification of objects being measured and monitored.

SLA's communicate to the service delivery team what is important to the business consuming the service and guide our focus. Our approach to SLA management focuses on proactive service management. As an example, we produce a daily report of all tickets related to the Mainframe Service from Keystone Edge (KSE) from the previous 24 hours documenting their current status, open and resolution time, and performance to SLA's. This daily report is emailed to the operations team and leadership. The intent is to raise visibility of these tickets early so that we can institute a plan to resolve within SLA's and minimize Customer business impact or fulfill Customer requests. By receiving the report daily and providing visibility to leadership we align our collective delivery focus to the current priorities and are able to proactively address issues before they turn into SLA violations and significant Customer impact.

Within this approach, Peraton uses the following process steps for creating an effective Mainframe Service Measurement and Management approach:

- **Strategic Measurement Identification:** Focus on the identification of key measures for the objectives of Compliance, Value, Performance and Quality. Measures are selected from all four objectives to ensure that the set of measures are balanced and complete. We establish target values and thresholds for all measures.
- **Monitor and Maintain all Measures:** Measurement data is gathered and processed using the defined process. Overall measures and assessments for each objective is established by aggregating measurements across the platform and objectives.
- **Evaluate and Manage:** Perform analysis of all measures and identify trends and opportunities for continuous improvement. Manage SLA attainment through operational reporting and leadership visibility to avoid SLA violations.

Through the execution of our effective service management process Peraton provides VITA measurable and significant benefits including a focus on continual service improvement opportunities, performance data, Service Level Agreements (SLAs) and metrics as well as trend analysis for further improvements.

2.3 Patch Management

Peraton will continue our 5-step Vulnerability and Patch Management process that we currently perform. This process includes phases for Detection and Discovery, Assess and Prioritize, Remediate, Verify, and Report. This 5-step approach provides the structure necessary to patch the Mainframe environment with minimal risk of disruption to VITA and VITA Customer business. Our timely patching activities help maintain technical currency and system stability. The patch management process addresses patching across three distinct service areas: hardware, software, and security.

Detection and Discovery: Correlating data from configuration records and patch release notifications from hardware and software vendors, we identify applicable patches to the VITA Mainframe environment. We conduct monthly meetings with hardware vendors to review MCL/firmware update availability and its applicability to the hardware deployed. For software patches and updates, we subscribe to vendor notices specific to installed software products. For security patching, we perform vulnerability scanning weekly using NESSUS. We submit the security patching report to the Account Information Security Manager (ISM) for review and determine what actions are required. Throughout the patch management process, the Security team reviews vulnerability scans and requests patching, as appropriate.

The Peraton ISM is the primary point of contact for receiving information regarding vulnerabilities from NESSUS, and the ISMISO participates in the weekly Security Tower meeting where information on known or new vulnerabilities are shared across towers. Our ISM will participate in Security Tower meetings conducted by the MSAI and attended by all STSs.

A comprehensive list is continually maintained to track potential activities that support the Assess and Prioritize step.

Assess and Prioritize: The second step of the patching process involves analyzing identified patches for criticality and overall impact to the environment. Assessments include severity of Security Integrity Alerts, Security Notices, or Red Alerts incorporating vendor-provided impact and exposure assessments. Each patch is then prioritized, considering the criticality and impact. We promptly schedule critical and high-impacting patches with emergency and urgent changes following the VITA change management process. All other patches are remediated during normal routine change windows following the change management process. For example, critical security patches to address vulnerabilities identified by NESSUS may require emergency patching activities to remediate vulnerabilities. During the step, we open and assign the appropriate change ticket to the responsible team for resolution. We present all changes to the VITA Change Management Board (CAB) for review and approval, as well as approval by agency personnel. Prior to change tickets being submitted to CAB, Peraton coordinates with agencies informing them of what the change is, where it will be applied, and what time the agencies can have testers on the bridge.

Remediate: Remediation includes implementation planning activities, technical package development, and deployment and testing of patches. The Peraton Account team oversees all changes within the Mainframe environment whether it is a patch to a Mainframe product, a patch/upgrade to the network hardware, or any scheduled maintenance to be performed within the MDC itself. The technical package contains all patch implementation instructions, rollback steps, and testing and verification procedures. As each patch or update is unique, we create the technical package and instructions for the specific patch, firmware update, or other maintenance activity. Once created, we review the technical package for correctness and completeness and include it within the change record created in the change management process. Upon approval of the change record, we implement the patch through a process that involves testing in the Peraton 'sandbox" (where possible), and into production within required timeframe and in accordance with security policies.

Verify: The verification step completes patch implementation into the Mainframe environment, where we check successful deployment against the desired outcomes and test system status. This verification step validates that the patch is successful without adverse impacts. We execute each test and verification procedure with tests that are unique to the patch and tests that are common to the environment component that validate the system operates as desired. Should a patch disrupt the production environment, we execute rollback steps with a problem ticket created to perform root cause analysis and reinitiate the patching process.

Reporting: The patching process is complete after successful patch implementation, with the change record being closed and patch status reports completed monthly. We are also able to export patch data and provide to VITA if required.

2.4   Technical Support

For general technical support, as outlined in Section 7.0 Technical Support, Peraton uses the established and approved process controls currently in place to monitor, operate, maintain, and manage the Mainframe infrastructure and software, including performing Equipment Repairs.

Technical Support As described in detail in Section 2.1 General, under heading Approach to Collaboration, we provide technical advice and support to VITA users, VITA Customers, application development and maintenance suppliers (VITA application owners), and database administration (DBA) staff, as needed. Through forums and strategic planning activities, such as the Change Advisory Board (CAB), Peraton leadership and technical teams contribute to and participate with VITA to plan, implement, and manage technology direction, engineering and routine changes to the Mainframe and other VITA technical infrastructure. Through such collaboration, Peraton proactively, and without disruption, develops and changes the Mainframe and other VITA environments.

Equipment Repairs To perform equipment troubleshooting, repairs and maintenance, we engage with Mainframe hardware environment vendors, including IBM and Dell/EMC to both respond to hardware issues and regularly assess hardware maintenance issues. Peraton has configured the VITA mainframe hardware to utilize proactive monitoring features built within the IBM mainframe and EMC storage devices. These features perform constant equipment health checks including daily dashboard reports that are sent to the OEMs. Additionally, any detection of equipment failure is immediately sent to the vendor support teams and Peraton works with the local vendor Field Engineers to provide the necessary spare parts and perform the repairs to meet service levels. Additional health checks are performed after the repairs are complete to ensure the hardware is back to operating at full capacity and performance levels. All changes are performed following the VITA change management process with the appropriate approvals.

2.5   USER SUPPORT

Peraton provides user support in accordance with VITA agreed upon procedures, including analyzing root causes within and beyond the Mainframe environment to eliminate systemic user complaints, routine advice, and assistance, and troubleshooting Mainframe matters, including application and access issues. We triage and manage user support requests using available tools, technical SMEs, and VITA KSE system to record and track requests. We close out request for assistance only upon confirmation of successful resolution by the requesting users. We support programmers and users by implementing authorized requests in accordance with established ITIL processes for change, incident, and problem procedures, and in compliance with SMM and VITA Governance processes. In collaboration with VITA agency application owners, programmers, and their third-party application developers, we support infrastructure implementations and changes required to complete end-to-end development, test, and validation of agency applications.

We work closely with applications teams to support application rollouts. As applications proceed through development and testing phases, we perform system configuration changes, manage user privileges, change firewall rules, and help agency application owners install and configure any required development and testing tools. We analyze Mainframe usage including production control and scheduling, system performance and capacity management, and configuration management through existing tools to optimize the use of production resources routinely and during change cycles. To continually assess, prevent, and respond to operational issues, we use automated tools, including BMC Control-O, that promotes system performance and availability via automation systems and policies that detect messages, commands, events and responds through automated commands, batch jobs and other automated scripted replies. Peraton has currently deployed over 4,600 automation rules and automated responses across over 20+ service groupings such as started task management, CICS automation, Content automation, security, MVS, log management, file transfer, dataset management, message suppression, DMV and DSS custom automation that maximizes performance and minimizes issues and allows for Peraton to meet and exceed SLAs. We collect, analyze, act upon, and

provide performance data, including CPU and RAM utilization, disk and I/O utilization, and network performance to VITA agency application owners and maintenance personnel.

2.6 Personnel/Clearance Management

Peraton will staff the program with qualified resources that possess the requisite experience and clearances appropriate for their assigned roles. Peraton continues to present key personnel candidates for VITA's review and approval prior to placing them on the project. At VITA's request, we provide documentation of qualifications for any staff supporting VITA or VITA's Customers for review. Peraton uses an effective process for onboarding staff, which includes successful completion of the VITA-mandated security background check prior to gaining access to VITA systems.

We have developed a VITA-specific security training program tailored to VITA and VITA Customer-specific requirements, including IRS Federal Tax Information (FTI) and Social Security Administration (SSA) data safeguards. Following successful completion of the VITA background check process, all personnel including subcontractors supporting VITA are required to complete the VITA-specific security training. We track and manage completion of background checks and training relevant to ensuring eligibility of all resources to support the VITA program. We maintain role-based access controls which are reviewed routinely and as changes including background checks affect personnel eligibility to support VITA. The access controls are configured and adjusted as required to ensure that advanced security operations functions and escalation tasks are performed by senior authorized staff cleared to conduct those functions and roles.

3.0 Enterprise Architecture

3.1 General Architecture Requirements

Peraton's approach to general architecture requirements is to continue following VITA requirements and road map, and fully integrate with the COV Technology Architecture Requirements and Roadmaps, and industry best practices.

Our architecture management approach at VITA enables us to manage the technology life cycle providing the appropriate combinations of hardware and software technologies and processes to manage the day-to-day operations. To support operational efficiency and best value, we support software at N, N-1, in accordance with VITA and its customers' specific requirements or with an approved deviation/waiver. We follow our 5-phase process of Planning, Acquiring, Deploying/Integrating, Maintaining/Upgrading, and Retiring activities for asset currency.

The **Planning** phase verifies that hardware and software meet the requirements and implementations are coordinated and communicated with VITA and all stakeholders. We begin the **Acquiring** phase after completing the Planning phase. As required, we work with our procurement team and vendor partners to find the best value for required hardware and software and get multiple quotes to select the most optimal technical and cost-balanced solution. After acquiring hardware and software, we work with VITA and the stakeholders for **Deploying and Integrating** all acquired components within the environment following the appropriate change control process and ITIL best practices. Once deployed and integrated, we support steady-state operations, including monitoring, maintaining, and upgrading the hardware and software throughout its life cycle. At the EOL/EOS, we work with VITA on a Retirement and Replacement plan that fits into the future roadmap. We phase out older systems with appropriate and compatible replacements gracefully and in a nondisruptive manner.

Our approach and methodology for VITA enterprise architecture management provides the foundation for implementing an efficient operations model allowing VITA and its customers to only pay for what it is needed without compromising performance, availability, and security.

We have strong relationships with industry hardware and software vendors, many with formal enterprise licensing agreements (ELA). We get routine notifications of patches, fixes, and version updates for all hardware firmware and software. We have formal internal monthly reviews to make sure all deployed architecture components are current, supported, and patched to the appropriate level. This process verifies that we meet VITA's requirements, maintain currency and supportability of the architecture.

3.1.1   DESIGN / ARCHITECTURE REQUIREMENTS

Our collaboration and coordination efforts for all architecture and service design, strategy, and planning activities is the foundation of VITA MSI platform success. We work closely with the MSI, VITA, and VITA Customers to ensure consistent deployment and use of enterprise tools where applicable and to achieve VITA and VITA Customer objectives, including effective and efficient Mainframe services. We enable and measure effectiveness and efficiency of Mainframe services through the metrics of performance, availability, and security. We provide measurable results by implementing VITA Mainframe technologies and processes and supporting it using operations services and our qualified resources. As part of the review process, we develop and document VITA-approved templates and artifacts for MSI Holistic Architecture Review Process (HARP), which include Architecture Overview Document (AOD), high-level, detail-level, and as-built designs, and relevant architectural perspectives.

Architecture reviews help avoid duplicating functionality, which keeps overall costs down. Led by our VITA Account Manager and Chief Architect, Peraton will continue to engage with the MSI and VITA Architecture teams to follow the MSI HARP for new solutions and significant updates and changes to existing solutions within the VITA environment. The artifacts produced provide a valuable reference resource and compliance tool for the respective architectures.

All solution designs consider security; performance and scalability; availability and resilience; accessibility; resource budgets; technology evolution, usability; applicable regulations, including those identified in the VITA Rules; and the ability of the solution to evolve over time. Designs consider desired business outcomes and are built to satisfy continuity and high-availability requirements that business outcomes dictate. Peraton documents new solutions submitted for review and approval using the VITA-approved AOD.

The AOD provides context to the solution by describing the interactions among the people, systems, and external entities with which it interacts. It provides a functional description of the system's key elements, the part they play in the solution, and the interfaces available for interaction. Information storage, manipulation, management, and distribution is described in the AOD, as well as component execution concurrency and software development support as applicable to the solution being documented. The AOD includes a description of the environment that the solution will be deployed into, how it depends on the elements within that environment, and how the system will be operated and administered once deployed into the production environment.

Prior to solution implementation, the high-level section (HLS) documents the components and high-level details of the proposed solution, including new solutions and technologies in the high-level service diagram and existing technologies and service components. After receiving approval of the HLS section, we initiate an implementation project and develop the Detailed Design (DD) section of the AOD to document the information required to build or rebuild the solution's systems and integrate with other STS solutions within the VITA environment. We use the information in the DD section to deploy the solution and update it during the project to reflect any changes or knowledge gained during implementation. Prior to new solutions going live, we update and submit the DD section for review and approval through the next phase of the HARP. We close out the project by updating the AOD's As Build Section (ABS) to document any required variances from the approved DD section to complete implementation and provide a complete, detailed overview of the architecture and implementation of the new solution.

Upon deployment of the new solution and approval of the initial AOD, we review the environment and revise supporting documentation, as required, at least annually during the life of the service. Peraton reviews VITA

and VITA Customer business priorities and desired outcomes as technology updates and evolution opportunities align and propose updates for consideration through applicable ITISP Governance processes.

3.1.2   TECHNOLOGY REQUIREMENTS

Peraton's approach to managing technology requirements is to verify that all hardware, firmware, and software are kept up to date with the latest versions, patches, and upgrades; is fully supported by the vendor across all required geographic locations; and is an approved technology consistent with VITA's Rules and architecture requirements. We use our Architecture and HW/SW Management process defined in Section 3.1 General Architecture Requirements, to manage these requirements. Our process includes five phases: Planning, Acquiring, Deploying/Integrating, Maintaining/Upgrading, and Retiring. During the **Planning** phase, we make sure all technology requirements meet VITA's requirements for Architecture compatibility and currency (N, N-1) or document and receive an approved waiver. In **Planning**, we verify all requirements can be fully supported by the vendor in all required locations, including hardware firmware support and break/fix patches. During the **Acquiring** phase we procure approved technologies as required from reputable vendors while ensuring compliance with approved designs. We use ITIL and best practices honed from our vast experience, NIST Special Publications, and VITA policies and procedures for integrating technologies during **Deploying/Integrating** phase. During the **Maintaining and Upgrading** Phase, we promptly apply all firmware, patches, and upgrades, maintaining version currency and providing proper vendor support. During the **Retiring** phase, we gracefully and verifiably remove all components for secure disposal.

3.1.3   INTEGRATION / INTEROPERABILITY REQUIREMENTS

Integration and interoperability of services and data in a multiplatform multivendor environment is critical to the success of the VITA program and mission. Our success, demonstrated in our current delivery of services, is based on our documented process and procedures for deploying and changing services for successful interoperability and integration. Our process is tailored for VITA and starts with a change procedure that includes integration and interoperability steps and checkpoints built in. Peraton's change process follows VITA SMM 4.1.4.1 guidelines and includes steps for Change Requirement Reviews, Evaluate Change, Approve Change, Implement-Test Change through Environment Stack (Alpha, Beta, System Test, User Test, Production), Verify Change, and Close change with lessons learned and success stories.

During the **Change Requirement Review and Evaluate** phase, we review all changes (hardware, firmware, software, and services) for impacts to other VITA systems and architecture requirements, including specific integration points for Mainframe service integration with event logging (Splunk, NOC) to ensure consistency with requirements. We also consider data integration and file transfer impacts with other systems and components during the requirements and evaluation phases to make sure all data types are consistent with VITA data requirements. During the **Implementation and Testing** phase, Peraton deploys changes up the environment stack, including our own Mainframe System Test Repository where we test changes for consistency and integration with major Mainframe software services, including the current VITA OS and other Mainframe middleware SW components from IBM, CA, BMC, before installing at a VITA LPAR.

Peraton then installs the change in the VITA LPARs from lowest to highest to verify integration and interoperability before installing into production. This process makes sure that Mainframe environment and services and changes to those components seamlessly interact regardless of where and how they are hosted, is thoroughly tested for integration and interoperability, and meets VITA requirements.

Integrating Mainframe logging with VITA and COV System and Event Logging: Once VITA has developed and implemented a solution for housing event logging across all supplier infrastructure and agency applications, Peraton works with VITA, MSI, Service Towers, and the MSS to implement a feed from the Mainframe and other technologies to the central event logging system. As part of this implementation, we provide people and develop processes to support subsequent actions stemming from an event.

Integrating and Interacting across other VITA Systems: Peraton currently interacts with suppliers across Service Delivery Management by participating in Governance meetings and monthly Architecture Discussions. Peraton provides an on-call roster to the MSI Joint Operations Center (JOC) for support after normal working hours if issues arise.

3.1.4   AVAILABILITY/PERFORMANCE REQUIREMENTS

Peraton's approach to Availability and Performance Management continues with our current approach, which first defines all availability and service requirements and configuration item requirements, including hours of availability, change windows and service levels with key performance indicators, and performance benchmarks. These processes are closely aligned and integrated with our overarching Operations, Maintenance, and Monitoring services outlined in Section 2.2 above. For each capacity item (CI) included, we develop and document the required availability and define the KPI and benchmarks. Examples for CPU CIs are the 4-hour rolling MIPS utilization, Peak CPU utilization, and formal service levels for availability, such as 99.9% availability during scheduled uptime. Other CIs, such as storage, have their own KPIs and SLAs, such as response time, and IO service time as appropriate.

Once we documented all Mainframe availability and performance requirements, Peraton developed and deployed the appropriate monitoring and automation mechanisms to track and capture system performance, utilization, and efficiency in accordance with document requirements.

In addition to monitoring, Peraton implements a continuous tuning and performance process where we address necessary upgrades and changes to any Mainframe infrastructure not meeting the defined requirements and enhance them to meet the requirements. Our tuning efforts are driven by our continuous collection of data and analysis to identify areas of improvements. Once identified, we look for root causes that may stem one of more issues, including network congestion and latency, system configurations, EOL/EOS, or lack of hardware and software resources to support application and database processing. We systematically eliminate issues to restore acceptable levels of performance, availability, and security through refresh, updates, and allocating additional bandwidth. These tuning efforts can be driven from increases in capacity and new workloads or from increases in existing application volumes. We conduct six activities for performance tuning:

- **Define Capacity Items** – Identify specific infrastructure components to monitor and manage from a performance tuning viewpoint.
- **Define KPIs and Requirements** – Identify, measure, and track the KPI and associated metrics and requirements. We use KPIs to describe and measure system performance.
- **Metrics Capture** – Gather metrics for analysis within the performance tuning process.
- **Monitor and Report Performance** – We monitor and report performance against established KPI thresholds. We identify and implement tuning steps through threshold analysis and reporting forms.
- **Investigate** – As thresholds are exceeded or performance issues are identified, we correlate gathered data and metrics and analyze them for potential tuning actions.
- **Correct** – From the performance analysis, we develop tuning plans to improve performance. The plan details the tuning effort to be performed, expected results, and monitoring plan.

Understanding that performance tuning is an iterative process, all or a portion of these steps may be performed multiple times to achieve the desired outcome.

Throughout the Availability and Performance processes, Peraton provides real-time data through the current VITA tools set and full reporting on all availability requirements and service levels. Reporting includes analysis of historical performance data through trending graphs obtained by monitoring all phases of performance.

The result of these processes provide VITA with availability and performance that meets and exceeds the defined requirements and SLAs, supporting VITA's and VITA's customers business processes.

3.1.5 CAPACITY AND PERFORMANCE REQUIREMENTS

SMM 4.1.3.6 Capacity Management

Peraton aligns to VITA's approach for capacity and performance management as described in **SMM 4.1.3.6 Capacity Management**. We support the three main processes of Business Capacity Management (Strategy), Service Capacity Management (Tactical), and Component Capacity Management (Operational).

Business Capacity Management – Peraton supports VITA and the MSI Capacity Manager as they translate business needs and plans into requirements for service, service level agreements (SLAs), and IT infrastructure initiatives which communicate what is important to be incorporated into design and implementation. Peraton's solution to Mainframe Services is designed in response to the SLA's and strategic requirements. We make sure services and components can deliver the capacity and performance required.

Service Capacity Management – Peraton performs tactical reviews of current capacity and performance focusing on the management, control and prediction of the end-to-end performance and capacity of operational IT services, workloads, and usage. Peraton reviews capacity and performance related to all services including CPU and storage utilization and trending for peaks and any metrics above thresholds.

Component Capacity Management – Peraton executes operational procedures focused on the management, control and prediction of the performance, utilization, and capacity of individual IT technology components. This includes current resource utilization, trends, forecasts, and exceptions as well as analysis of any planned component deployments. Findings, results, and recommendations are shared with VITA concentrating on the identification of trends and potential capacity issues and risks via monthly reporting per **Exhibit 3.4 (Report Matrix)**.

Perform Infrastructure or Platform Upgrades

Peraton will perform infrastructure and platform upgrades as required to provide effective capacity to maintain and improve performance while continuing to meet architectural requirements. All upgrades will be coordinated with VITA, third party vendors and other suppliers as appropriate to maintain infrastructure capacity. All changes will be documented and follow the VITA change management process and receive appropriate approvals.

Transitioning into the new contract, our solution includes a refresh of the existing Mainframe and storage hardware. To determine this next generation of hardware, and the accompanying sizing, we have analyzed the historical utilization and trends and used the following factors in sizing the new HW solution.

- Factors and Approach:
  - Evaluation and analysis of the previous 12 months of usage, capacity, performance data (SMF Data) and storage GBs utilized.
  - Evaluation and analysis of growth trends (2/6/12 month intervals) – Stable over the last 12 months
  - Collaboration with Vicom, IBM and Dell to determine the best solution to meet performance and capacity objectives.
  - IBM CPU sizing provides capacity over the forecasted requirement (941 MIPS vs. 865 MIPS).

- Analysis Tools Used:
  - System Management Facility (SMF) Data
  - Vicom Performance Analysis Tool (VPAT) – Allows multiple CPU modeling/simulations between hardware sizes and configurations.
  - Storage Capacity Reports – Peraton Batch Jobs evaluating the cataloging of data across disk pools, collected monthly.
  - Tape DLM Configuration and CA1 Catalog (Compressed and Un-compressed)

As a result, we provide refreshed Mainframe CPU and storage hardware to support VITA over the contract term that is appropriately sized to provide required capacity and performance and accounts for future capacity

based on current usage assumptions. This solution eliminates issues with vendor hardware end of support life timing and provides VITA with current technology to meet capacity and performance requirements.

SMM 4.1.6.3 Service Measurement

Peraton identifies key measurements and data points on process and Service performance in order to perform analysis and identify opportunities to optimize performance and reduce costs. Examples of cost saving opportunities include:

- System performance optimization to take full advantage of existing resource capacities.
- Retire unused resources to reduce overhead costs.
- Provision additional capacity only when required.
- More accurately forecast future consumption and plan and budget procurement.
- Identify service improvement opportunities.
- Proactively address rising costs driven by excessive consumption.

Application Bandwidth Usage

Peraton will track usage over a period of 12 months and using that data will develop an estimated bandwidth usage per interactive user login TN3270 session to the Mainframe system and document in the Mainframe platform's Application entry in Archer. The following estimates will be documented:

- Average number of concurrent users,
- Amount of bandwidth required for each concurrent user,
- Total users configured for the Mainframe (active user accounts),
- Track over time and document peak usage periods,
- Estimate total network throughput for interactive uses the system can process at once.

3.1.6   CONTINUITY REQUIREMENTS

To support VITA's Business Continuity (BC) and Disaster Recovery (DR) requirements, Peraton will continue to deliver a holistic mainframe services solution, including data replication, mainframe failover, network failover, DR procedures and test plan, and expert recovery personnel in accordance with **SMM 4.1.3.5 IT Service Continuity Management**. Our DR facility will remain at the current location in the Colorado Springs CXC data center, which creates a geographical diversity between the Peraton MDC (primary site) and negates any impact of natural or man-made disasters.

Our BC and DR solution capitalizes on dedicated replication to expedite data recovery and meet VITA's mainframe reliability, service availability, data availability, and service restoral requirements. This service offering will meet the required not to exceed 24 hours Recovery Time Objectives (RTO), and not to exceed 6 hours Recovery Point Objectives (RPO) for VITA Tier 2 services. While data replication is the primary enabler for protecting Commonwealth data, as described in more detail in Section 9.0 Online Storage and Backup Management, we supplement data replication with a comprehensive backup and restore capability providing customers the ability to perform backups and restores of their Commonwealth Data to meet their specific business requirements.

Another risk to business continuity is data corruption which can result from a number of causes including human error, malicious third-party actions, or software and hardware failure and can be very difficult to prevent and detect. In such a scenario the corruption can quickly be replicated to secondary storage. Peraton recommends Customers employ a data backup strategy which provides for sufficient time-based retention windows to allow for restoration of data to a known-good state prior to corruption rather than rely solely on active replication of data to support availability requirements. The backup and recovery tools available within the Mainframe Service support establishment of these types of backup and retention strategies. Peraton monitors data storage systems for hardware and system issues within the storage arrays and Mainframe system events indicating data corruption within system configuration and operational data. Peraton will notify Customers of any detected indications of corruption which affects Customer data as quickly as possible and support recovery efforts as circumstances dictate.

Peraton coordinates with VITA and MSI Disaster Recovery SMEs to participate in VITA's Annual Disaster Recovery Exercise (DRE), which enables Peraton to test our Disaster Recovery Plan (DRP) and our Technical Recovery Plan (TRP) used by the Mainframe Services Team in bringing up the disaster recovery site. Annual DREs allow for training and continuous improvement opportunities, as well as to identify any deficiencies within the DRP or TRP or communications. Peraton has successfully performed annual disaster recovery activities within the 24-hour Recovery Time Objectives (RTO) and 6-hour Recovery Point Objectives (RPO) requirements and has received praise from the VITA and VITA Customers.

Key features and accompanying benefits of our BC and DR solution is shown in **Table 3**.

<p align="center">**Table 3: Continuity Features and Benefits to VITA**</p>

FEATURE	BENEFIT
Properly maintained DR Mainframe and storage infrastructure that exceeds the capacity of the Primary Production environment	Provides system and application performance in the DR environment on par with the production environment to eliminate business disruption while running in the DR environment
Established and tested DRP and TRP, based on Disaster Recovery Institute International (DRII), ITIL, Government directives, VITA policies and Peraton's industry and VITA experience	Proven DR approach, protecting VITA and VITA Customer business operations from Day One of the Contract
Regular review and testing of the DRP and TRP	Plans are current to the state of operation ensuring that the plan is valid and executable in the event of disaster
Proactive posture and planned resilience within the Mainframe environment	Offers service and infrastructure availability reducing the impact of disaster events and meeting or exceeding agreed upon RTO and RPO objectives
Common understanding of disaster initiators and processes	Supports rapid invocation of the DRP and TRP to minimize business disruption

Peraton will continue to provide a Mainframe Services Team that has first-hand knowledge of IT Service Continuity Management (ITSCM) requirements and issues that the user base regularly experiences. We implement mature, ITIL-aligned processes tailored for VITA's TRP solution, including ITSCM methodologies for DR-related activities to facilitate standardized, repeatable, tested DR solutions. Our knowledge includes experience in troubleshooting issues beyond Mainframe services, such as knowledge of the underlying networks and applications to rapidly address the unique demands of providing IT service continuity support to different VITA services consumers.

We participate in VITA's Service Design process, to help generate practical, effective ITSCM planning solutions, coupled with advice based on our experience in delivering services to a wide range of clients with critical missions. Our goal is to provide end user access to Mainframe systems and service continuity through improvements in disaster tolerance capabilities. We advise on risks and disaster protection measures based on our experience in implementing and delivering ITIL-based services.

4.0   Security Requirements

4.1   General Security Requirements

Peraton's Mainframe Services Team currently works closely with VITA, the MSI, Service Towers, and ATOS the MSS provider to support Mainframe operations in addition to providing policy, procedures, technical, and threat advisory services to strengthen the VITA enterprise. Our security management approach implements VITA requirements, policies, and procedures, appropriately balanced with the risk and the evolving threats based on our experience managing the VITA Mainframe service architecture. We implement VITA-mandated MSI security policies and standards across Mainframe systems and networks through day-to-day security operation activities that include aligning configurations and controls natively from the Mainframe environment and inheriting those implemented within the managed VITA environment;

implementing security policy enforcement mechanisms, including access controls, such as CA Access Control Facility (ACF-2) and perimeter controls using firewalls and IDS/IPS; management, monitoring, and routine audits of control points.. Since the inception of our current contract, Peraton has and will continue to maintain compliance with any applicable Commonwealth, MSI, and federal policies and standards including but not limited to VITA's SEC530, NIST Special Publications (800-53, 800-37), FIPS, IRS PUB1075, FISMA, ISO27001, FTI (IRS PUB-1075), SSA, FedRAMP, CJIS, FISMA, PCI, ISO27001, FERPA, and HIPAA-HITECH. As new or updated standards emerge, Peraton will work with VITA to incorporate these requirements and make updates to appropriate documentation, including templates provided by the MSI to standardize information.

Peraton's Mainframe Services Team currently supporting VITA are CONUS-based, subject to routine background checks, and are US citizens and others legally authorized to work in the United States. They have long-standing experience working within the VITA MSI model, collaborating with all MSI partners, and implementing the shared, interdependent, and integrated security management model. We collaborate with MSI Service Towers through the established framework of processes and agreements. For instance, we have an Operational Level Agreement with ATOS, the MSS, to jointly work on security events and security incident responses that align with overarching MSI Security Management SMM 4.1.5.7, Annual Security Incident Tabletop exercises as part of the annual review of integrated processes with other towers. We attend routine meetings, including weekly security tower meetings to share information across towers regarding new vulnerabilities and cybersecurity monthly and quarterly baseline meetings to addresses interdependencies, tools, and workflows required. Our security controls leverage our deep understanding of the networks, VITA SMMs and customer guidelines for hardening, available controls for inheritance, and tools and workflows, including 24x7x365 monitoring to optimize Mainframe security architecture and operations:

We implement and maintain security mechanisms in compliance with COV data security standards, state, and federal laws to protect and safeguard all data against unauthorized access, destruction, loss, alteration, and commingling. Data security mechanisms relate to applying principles of data isolation, which include physical and logical separation of data based on policy, encryption during transmission, and at hardware levels during processing, along with verifiable up-to-date backups for recovery. Foremost, the VITA production Mainframe located at MDC in Clarksville, VA, has a full DR site located at DXC Data Center in Colorado Springs, CO. Data sovereignty to ensure that all Commonwealth Data remains in the United States is enforced by using non-internet–connected dedicated circuits and restricted access via geofences. **Table 4** provides the features and benefits of our data security activities.

Table 4: Security Requirements Features and Benefits

FEATURES	BENEFITS
Data classification assessments for identification of sensitivity, protected status, and impact to VITA and its customers.	Implements appropriate data protection controls aligned with criticality of data in accordance with VITA and its customers' requirements.
Dedicated direct attached storage (DASD) hardware that hosts all agency data configured to disallow any agency to connect to or see any other agency's DASD, and hardware encryption for all storage at rest.	Strong separation of data through physical and logical mechanisms including access controls and encryption. Enforces Confidentiality, Integrity, and Availability.
DASD is replicated to DR site continuously 24 hours a day over dedicated circuits and using FIPS 140-3 compliant encryption.	Protects data during disasters. Prevents data spillage during storage and transmission. Speeds operations and data DR.
ACF2 is replicated to the disaster recovery site ensuing all security attributes are identical between production and disaster recovery site.	Prevents compromise through continued inheritance and enforcement of access controls.

As part of our field-tested systems decommissioning and data migration processes, we manage data migration end to end by overseeing and guiding agencies through the process and subsequently validating successful completion of the process as per VITA rules. VITA provides a Certificate to the agency certifying the

removal of agency data and all agency user IDs. This verifiably ensures that zero residual data is left on the originating platform.

Peraton subscribes to third-party vendor websites for the most current information and status of vulnerabilities, patches, or software upgrades. We download and process patch files and analyze the content for applicable updates for the VITA Mainframe. Once we identify applicable updates, we test and validate appropriate actions for implementation in Peraton's test system to avoid potential issues prior to introduction to the production systems. On approval by Mainframe services, we apply updates/patches to customer agency test systems where they are tested against the agency applications to identify issues prior to being implemented into production. On test completion by the customer agency, Peraton follows the change management process and implements updates during standard maintenance windows.

Data Protection and Encryption: Peraton implements stringent encryption mechanisms for data at rest and in transit based on VITA requirements, including FIPS 140-3 standards to encrypt Mainframe file systems hardware disk storage array and mirroring to the recovery site storage array, both of which are hardware encrypted. We design and engineer controls and processes based on data sensitivity, protected status, classification, and impact categorization as part of the NIST RMF process seen in Section 4.3 Risk Management. This ensures compliance with all VITA and Customer Rules for the processing, storage, and transmission of information. We possess exclusive control and ownership of all encryption keys supplied by Unisys and by centrally managing host certificates securely stored in the "key ring", which is a collection of certificates that identify policy and networking trust relationships. Commonwealth retains exclusive control and ownership of all Key rings and usage is restricted based on credentials and authorizations thereby protecting resources from unauthorized users, services, and entities. Our implementation of FIPS 140-3 encryption tracks host and user access/encryption certificates and annually renews or revokes upon request from customer agencies. Our implementation of the encryption controls allows for time-based and user-based revocation of access/encryption keys based on the schedule defined by VITA and VITA Customers. We collect all regular and administrative personnel access and activity logs for analysis and alerting. Data transmission to and from the Mainframe is restricted to FTPS which is encrypted, and telnet 3270 connections are forced over TLS 1.2 or higher encryption. In transit data between our services and systems are encrypted to the extent possible based on available integration and systems compatibility. We block all sources of unencrypted transmissions at the firewalls to prevent unauthorized access from misconfigured client software. However, one authorized exception relating to a locality within the Commonwealth has been granted VITA exception to the data in transit encryption requirement until they implement a solution to support required encryption standards.

Security Operations: We implement security operations process and procedures for the Mainframe environment in compliance with VITA SMMs and customer policies and procedures, as follows:

1. Through our NIST RMF process as seen in Section 4.3 Risk Management, we manage the security life cycle of Mainframe assets including creation, implementation, and continuous monitoring of the security baseline configurations and standards in compliance with VITA and Customer Rules and requirements including hardening guides, and the SMM.
2. Audit user accounts quarterly and automatically disable any account not used for 30 days.
3. Protect endpoints using malware prevention through VITA-approved endpoint protection software on employee workstations, as well as the windows jump servers used to access the Mainframe. We update endpoint protection on employee workstations and jump servers daily.
4. Handle code prevention with code injection signatures on the IDS/IPS
5. In addition to endpoint protection software, Peraton has network IDS/IPS on systems in areas facing the internal Peraton network and on the dedicated link to the VITA network. The network IDS/IPS systems provide DDOS protection to the Mainframe environment, along with DDOS protection through its extranet connection to VITA's datacenter DDOS protection measures. Signature updates for the IDS/IPS are performed automatically every 48 hours and new signatures are enabled by default.

6. Peraton VITA personnel receive annual phishing and spamming training through the corporate security awareness program and the VITA account-specific annual training programs.
7. We use available tools to perform vulnerability scanning on the Mainframe environment network and jump server endpoints weekly to identify missing patches. In compliance with VITA Hosted Environment Information Security Standard (SEC530) requirements and policy, we proactively announce vulnerabilities and install missing updates and patches in accordance with change management and process coordination procedures including tickets in KSE. The patches/updates include prioritized critical ones as announced by third parties, vendors, or industry experts. Typically, critical patches are applied during standard maintenance windows on Sundays from 3:00 am to 8:30 am EST.

SIEM Related Options
- **_Option 1_** - *Converting SMF logs so they can ben ingested by VITA Managed Security Service Provider SIEM*
- **_Option 2_** - *Log Management and Supplier SOC (managing & monitoring events) to be handled within Mainframe Supplier (not through VITA Managed Security Service Provider) and the associated communication with VITA details (frequency, what type of communications, etc.).*

VITA has chosen and Peraton will implement Option 1, "Converting SMF logs so they can be ingested by VITA Managed Security Service Provider SIEM", as described below, as part of the base scope of the contract.

SIEM Related Options

Option 1 – Converting SMF logs so they can be ingested by VITA Managed Security Service Provider SIEM **Security Logging:** Peraton logs all Mainframe system, network, and user-level activities, which are automatically forwarded to Peraton SIEM for analysis and archive. The System Management Facilities (SMF) logging component of z/OS from IBM logs all activities, including regular and administrator user activities, remote access, and authentication actions. We maintain availability of the logging service and its security by monitoring all sources and the health of the SMF system.

We log all access to sources with installed SMF logger and immediately analyze and respond to any disruption of the logging service. This allows for prevention and quick response to alteration and deletion of logs, and unplanned or unauthorized stoppage of the logging service.

To implement and support log forwarding and ingestion into the MSS SIEM, we follow a project management approach that includes planning and definition, engineering and operation of the log forwarding solution. As we implement the log forwarding solution, we engage with VITA and the MSS supplier to determine and coordinate:

▪ The security data and events to extracted from SMF logs.
▪ The format of the event data records.
▪ The timing and frequency of log forwarding, striving for near real time forwarding.

Within our solution, the sources of data within the forwarding solution include security events from SMF. Our log forwarding solution performs the extraction and forwarding of logs by utilizing the Vanguard Active Alerts offering that includes the following features:

▪ Converts and delivers mainframe data to all conventional SIEM products.
▪ Connects with standard z/OS security products.
▪ Monitors z/OS and UNIX System Services (USS).
▪ Gathers intelligence from z/OS SMF and the system operator interface.
▪ Uses both signature and anomaly-based attack detection.
▪ Provides real-time alerts that can be managed, filtered, routed, and searched via SIEM software.

During the course of extraction, the identified data is initially converted to a format to be ingested into the MSS AIsaac SIEM utilizing the AIsaac SIEM provided interfaces. This approach provides an automated extraction and transmission on an ongoing basis to the VITA MSS managed SIEM.

In addition, as part of the user access and authorization review, we capture real-time user activity logs for all Mainframe interactions and transactions. We securely collect and forward logs to the MSS SIEM, in addition to storing and maintaining them within archives for at least 7 years based on VITA and its customer retention policies. An automated process sends SMF logs to a storage location within COV via VITA's Data Power gateway for additional retention. The request system for user authorization is VITA's KSE, which preserves tickets and actions for logging and management. In addition, ACF2 creates SMF records logging changes to accounts and account creation.

Finally, once implemented we monitor the data extraction and transmission processes as a component of steady state operations.

Option 2 – Log Management and Supplier SOC (managing & monitoring events) to be handled within Mainframe Supplier (not through VITA Managed Security Service Provider) and the associated communication with VITA details (frequency, what type of communications, etc.).

Security Logging: Peraton's security solution logs all Mainframe system, network, and user-level activities, which are automatically forwarded to Peraton DEVO SIEM for analysis and manually reviews daily reports of login attempts and failed dataset access each business day. The System Management Facilities (SMF) logging component of z/OS from IBM logs all activities, including regular and administrator user activities, remote access, and authentication actions. Network devices and non-Mainframe systems such as the MS Windows based Jump Servers, including the IDS/IPS firewall modules, log directly to the Peraton SIEM. We maintain availability of the logging service and its security by monitoring all sources and the installed SMF logger facility on the Mainframe and supporting storage resources. We maintain and protect logs for historical reference using virtual tape backups, off system archive, and active reference using SIEM storage. We monitor tape backup systems and SIEM repositories and restrict access to authorized personnel. We log all access to sources and the health of the SMF system and immediately analyze and respond to any disruption of the logging service. This allows for prevention and quick response to alteration and deletion of logs, and unauthorized stoppage of the logging service or interruption due to system malfunction or resource issues.

During execution of SIEM/SOC operations, the Peraton SOC and VITA Mainframe account team provide proactive alerts to VITA or Customers as appropriate. The Peraton SOC sends email alerts to the account ISO and account manager when an abnormal event is identified. Peraton reports to the MSS SOC via email or phone call after performing the initial triage of suspected security incidents. Following the Incident Response Process, MSS SOC opens an incident in Archer and if necessary, a corresponding incident ticket in KSE and manages the incident process with our support. Our security operations activities are all structured to act on system log events by:

- Retaining Peraton staff to monitor the Mainframe logs (SMF, Syslog), ACF2 logs, and IDS/IPS Systems
- Monitoring security events, forwarding to resolver groups for resolution.
- Providing notification to the MSS Supplier of Mainframe security events and support VITA Security Incident response processes in collaboration with the MSS Supplier
- Providing notification to VITA and Customers of Mainframe security events.
- Participating in the Incident Response processes as described in Section 4.1.1 Incident Response Security Requirements.
- Providing a monthly report to VITA summarizing event collection and response metrics for the previous month, delivered by the 15th business day.

4.1.1   INCIDENT RESPONSE SECURITY REQUIREMENTS

Peraton will maintain a qualified team of security engineers that implement our incident response approach, including all processes mandated by VITA SMM 4.1.5.7. In addition, our team deploys applicable creative

methods, automation, and unique techniques based on evolving threats, industry best practices, and our R&D and experience supporting numerous large federal and state agencies. We routinely review, update, and share Peraton's Security Incident Response plan for Mainframe systems and networks with VITA, MSI, and Service Tower stakeholders and get annual approval from VITA Commonwealth Security and Risk Management (CSRM).

Through routine collaboration and in support of the Integrated Incident Response Plan, our approach cohesively integrates with incident and risk management process workflows across VITA enterprise, the MSI, Service Towers, security, and SOC operations. We collaborate via security incident response tabletop exercises, platform service delivery forums, biweekly SIIF Forums, and other routine interactive activities, which include sharing lessons learned, threat intelligence, root causes, and changing objectives to help refine and adjust Mainframe incident response processes with MSI, Service Towers, and VITA. Our team remains vigilant over Mainframe operations to detect anomalies, zero day, benign, and active adversarial actions including malware, unauthorized content, hacking, phishing, and denial of service. Upon detection of significant events and incidents we invoke incident containment and response steps to arrest the spread and progressive damage, including immediate notification to VITA and the affected Customers. Our operations staff routinely baselines acceptable normal operations by monitoring system and network performance and resource degradations that may indicate events or incidents relating to adversarial actions.

Peraton's collects Mainframe system logs for 24x7x365 monitoring of all systems and networks for data analytics in accordance with VITA rules and VITA's analysis requirements. Upon receiving an incident ticket in KSE, Peraton performs the appropriate action to stop and analyze the event and put in mitigation steps. Alerts include threats encountered by our team during vulnerability and penetration testing assessments and may relate to current code and other threats owing to changing operations, standards, and industry practices that may be specific to VITA's environment, the Mainframe, or anything as observed by industry vendors and security researchers.

Peraton's Mainframe services team is highly qualified in Mainframe, IT, and security operations, and we are accessible to VITA, MSI, and Service Towers during normal hours and after hours to support incident management response actions and required changes to address emerging security requirements under direction from Customers. We are routinely engaged by the MSS, the MSI team, and Service Towers through KSE ticketing and resolution process. For incidents that may or may not directly relate to Mainframe systems and networks, our security engineers and program leaders maintain visibility of performance and availability degradation through active monitoring of the systems using available tools. We actively engage with MSI, the MSS, and other Service Towers to share containment and recovery insights, and risk calibration of incident response actions to ensure VITA enterprise and Mainframe operations maintain operational resilience.

As events and incidents are detected, multiple teams are mobilized, including key designated members, such as on-call personnel, Peraton ISO, Peraton account manager, and Peraton account executive. Our team helps handle the incident through remediation and recovery as required by SMM 4.1.5.7. Our team joins the incident bridge conference call, and as a first step, we gain a full understanding of the severity, scope, and scale of the data, systems, networks, and environments affected. We use the KSE system to manage and report incident ticket progress to VITA every 24 hours or more frequently based on the severity, scope, and scale of the incident. KSE enables the ticket to be owned by a specific tower based on analysis, participation, and contribution toward the resolution from all other towers. If the ticket is related to a security incident, the MSS SOC updates the Archer system.

Peraton's leveraged security team and VITA MSS SOC are included in the investigation to (a) provide historical data on the entry point and the modes used by the attackers to gain access within the environment; (b) provide continuous enrichment data, such as identifying the sources of the attack, the Tactics, Techniques, and Procedures (TTPs), attack path radius, and current threat intelligence on how the attack most likely morphs further; and (c) take specific actions to help contain the attack. Subsequently, we initiate or participate in containing the incident alongside MSI and Service Tower teams for all VITA enterprise systems to stop the

spread across the VITA enterprise systems. Based on the nature of the attack, containment actions include blocking sources of the attack at all managed rules and policy enforcement points, such as firewalls; IDS/IPS; and Lumen the current MPLS circuits provider. Additional steps become necessary, such as micro segmenting systems within the path of the attack to stop further spread of malware and malicious activity; quarantining affected systems to eradicate malware and unauthorized code; and diverting user traffic to backup circuits, systems, networks, and backup data centers at QTS Ashburn, VA, and DXC Colorado Springs Data Center. VITA enterprise SOC, Peraton's security operations teams maintain the environment as normal operations is restored. The remediation and recovery phase includes various steps to bring systems, data, and software to its last-known operational state, including (a) collecting malware, unauthorized codes, and other electronic artifacts from all quarantined systems for analysis and maintaining chain of custody for legal actions; (b) wiping all system random and fixed storage and reloading and hardening the operating systems as per policy before reintroducing them into the VITA environments; (c) reconstituting and testing corrupt data with available data from backup repositories; and (d) diverting traffic from disaster recovery circuits and data centers to regular circuits and systems. We lead and participate in post-incident After-Action Reports (AAR) and RCA activities, including identifying lessons learned, analyzing root causes, updating incident response plans and playbooks, concluding the incident, providing reports to all VITA stakeholders, and initiating improvements and enhancement as necessary for future avoidance of similar issues.

4.1.2   SECURITY INTEGRATION

Mainframe security integration activities follow VITA established risk and change management, and security controls implementation rules. We document, update, and periodically deliver a System Security Plan (SSP) to VITA that includes Mainframe security integrations as part of the system security and risk management process. The SSP is currently delivered annually or more frequently based on significant changes to the environment. As the living artifact of the Mainframe environment security posture, the SSP details the environment's architecture and processes as change occurs. As part of threat hunting and as newer threats emerge, Peraton engineers analyze and report Mainframe environment's susceptibility to the threat to VITA and its customers. These threats are included as part of our routine risk analysis in context of change approval and management process and needs for improved security and integrated compliance across VITA Service Towers. We focus on susceptible components of the environment to continually monitor the Mainframe environment through Peraton SOC and communicate all intrusions to the MSS tower and VITA stakeholders. We initiate corrective recommendations and actions in accordance with estimated potential risk, including improvements to Mainframe, VITA enterprise architecture, MSI processes, and integrated compliance and service management requirements. For systems outside of Peraton's purview, we respond to findings and corrective action plans/POAMs created by VITA through the Archer system. For Peraton-controlled systems, we create and manage findings, corrective action plans, and POAMs. These findings usually emerge from SOC 1 and 2 audits, penetration testing, vulnerability scans, and review of policies. Cross-functional activities via the MSI and between the MSS and Mainframe function involve managing firewalls and IDS/IPS rules as part of toolset integrations in addition to configuration and installation support as required. We help install and configure IDS, IPS, Firewalls, and ACF2 security authorization module on the Mainframe Z/OS operating system, vulnerability scanner, and log monitoring within the MSS SIEM. The MSS SIEM monitors user, Mainframe, IDS/IPS, and firewall activity and collects logs to correlate and identify intrusions for escalation and response. We make log and activity data available to the MSS SIEM and other tools for further analysis. Through collaboration and cross-functional reporting across the all teams, we create and maintain awareness of events, incidents, threats, and vulnerabilities, and support opportunities for data and logs sharing and integration of cross-platform toolsets as necessary between all the functions including the MSS.

4.1.3   AUDIT AND COMPLIANCE

As required by VITA, via the MSI, we provide ad hoc and recurring audit and compliance support as necessary in response to requests from VITA, VITA Customers, and Integrated Suppliers. Through our third-party subcontractor, we conduct independent SOC 1 and SOC 2 audits of the Mainframe environment and

facilities, delivering non-redacted reports to VITA annually or more frequently as may be necessary. Our Mainframe Services Team addresses identified remediation steps with quarterly status reports. We continue to support required audits for FTI and SSA by making system documentation, operations report, and supporting staff readily available. In compliance with SMM 4.1.3.7, Security Management Process Section 12, Peraton's account ISO initiates a new audit review annually, which includes physical security, logical security, and processing integrity. The ISO participates in full cooperation with MSS, MSI, and VITA for security assessments and audits. The Peraton account ISO coordinates with MDC and DXC onsite staff for onsite visits by auditors, such as the tri annual DSS IRS FTI audit and schedules interview sessions with facilities staff. If auditors provide findings from the audit, we log those findings into Archer, initiate a Corrective Action Plan (CAP), and coordinate and implement corrective actions to resolve findings. Peraton provides evidence as requested by VITA or the auditors to demonstrate resolution and closes the entry in Archer.

4.1.4   USER AUTHENTICATION

Peraton provides secure sign on functionality to staff members supporting the VITA accounts through corporate laptops that enforce MFA. During normal operations, Peraton staff logs onto the Mainframe using jump servers located in MDC; during DR exercises or DR events, they use the jump server located in DXC Data Center. Jump servers provide a secure intermediary supervised service to tunnel all access traffic through firewalls. Peraton hardens and monitors jump servers and make logs and reports available to VITA stakeholders to validate that only authorized users access the jump server and Mainframe.

Access logging is enabled using ACF2 functionality, which captures logs of user activity within the Mainframe. Logging is enabled for various products, such as DB2 or CICS on the Mainframe as required and specified by an agency. Access restrictions can be enforced through login rules mandated by the agencies to control and manage access based on role, need to know, access, and other parameters based on user roles and job functions. Peraton currently runs a daily violation report to collect access attempts and help determine if users trying to access Mainframe resources and applications have specific privileges or if the users are having password issues. The account operations and security teams review the report, perform follow up actions internally, and alert DMV or DSS with user details and the nature of abnormal activity observed for follow up and resolution.

All Peraton staff supporting VITA are subjected to an approved onboarding process to the VITA account, including fingerprinting and background checks by a local law enforcement agency. The results of the

background check are sent directly to VITA, who in turn, notify Peraton. Upon receiving a positive result, and prior to being allowed access to MSI resources, the staff member must complete the SANS Security Training modules customized to VITA requirements. Access to the Mainframe or network devices is only granted when both, background check is accepted, and SANS training is completed by the user. Upon completion, we submit a request via KSE to create appropriate accounts and access. For Mainframe ID, which enables user access to the Mainframe, Peraton works with the VITA Mainframe Service Owner for request approvals. Peraton monitors and maintains all security clearances for staff supporting the VITA account and reinitiate background checks shortly before they expire every 7 years. If a member of the Peraton technical team retires or transfers to a new position, Peraton submits an off-boarding ticket via KSE, which notifies MSI and VITA, and access to the Mainframe environment is removed.

We align and adhere to **SMM 4.1.5.6 Access Management** for managing all user accounts including privileged accounts. Only Peraton technical staff have privileged accounts, which gives them access to various products/resources on the Mainframe, storage arrays, and network devices. Users are granted access to only those applications and resources that were requested for them by their Authorized Access Coordinator (AAC). No regular user is given elevated privileges to the Mainframe. As part of the security footprint for the Mainframe, Peraton encompasses the strategy and enforcement of "Least Privilege", which is defined as the restriction of access rights and permissions for user's accounts, applications, systems, devices, and computing processes to the absolute minimum necessary to perform routine authorized activities. Additionally, as part of our account management and routine user access review processes, we revoke privileged user access within 30 days of non-use of the account, as requested, or when personnel depart or cease to require access to the Mainframe Services.

4.1.5   USER AUTHORIZATION

Peraton implements and manages user authorization and authentication through ACF2 in accordance with VITA policies and **SMM 4.1.5.6 Access Management**, applying access authorization controls following centralized policy driven settings, including requests for accounts, permission changes, and other changes as required from originating agency or locality Mainframe AAC. Users are authorized based on role and responsibilities assigned, which translates to rights authorizing and restricting them from performing tasks, including document storage. The ACF2 based implementation of authorization policy is applied to all users, and system and services including customer agency users, VITA Enterprise users, and across all our Mainframe systems, services, and network components. Peraton technical staff are granted access only after completing an onboarding process that includes a VITA-required background check, VITA-mandated security awareness training, and Peraton corporate requirements. As part of our ongoing improvement to the user authorization process, we hold quarterly user access reviews to look at the number of unused, suspended, or disabled account and review progress on user account cleanup efforts.

4.1.6   FULL DISK ENCRYPTION

Robust data security through encryption enables Peraton to maintain confidentiality and integrity of VITA data. Peraton enables encryption in transit by implementing FIPS-140-2 configurations on FIPS certified network and processing endpoints as required by VITA directives, including SEC530. On Peraton user endpoints accessing the Mainframe environment and VITA enterprise resources, BitLocker is installed for full disk encryption. On the Mainframe, we encrypt Dell/EMC Mainframe storage at the hardware level providing encryption at rest, which is transparent to the OS and any other system accessing it. Dells' Data at Rest Encryption (D@RE) provides hardware based, on-array, back-end encryption to the storage array, protecting VITA data from unauthorized access. D@RE provides encryption without performance degradation or disruption to the VITA environment. Incorporating the Dell EMC Key Trust Platform (KTP) provides for onboard, integrated key management. Our encryption and key management methods are fine tuned to support decryption of assets for forensics collection, secure storage, and analysis capabilities across all Mainframe storage and networked systems. Since the Mainframe storage array uses hardware encryption, we perform

decryption or forensic analysis of another system by configuring the array manager for that system to access the volume for direct access or the export of an image of any examined volume.

4.2   Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)

Peraton's Response

Peraton manages IDS/IPS at the following Mainframe infrastructure and interconnectivity points:

- **CXC** – located in Colorado Springs
- **MDC** – located in Clarksville, VA

We monitor performance, capacity, and network devices and connectivity that provide IDS/IPS functionality using available tools and processes. As part of our central logging and forwarding, all network and security devices, including firewalls and the IDS/IPS are configured to collect, encrypt, and securely transmit user access, system modification and data transfer activity and logs to MSS SIEM for analysis, event and incident containment, escalation, and response coordination with MSS. We follow **SMM 4.1.5.3 Monitoring and Event Management** and other applicable service management manuals for managing IDS/IPS devices and functionality. We coordinate activities with VITA, MSI, and MSS during incidents and collaborate with them for guidance, planning, and management of VITA enterprise event management tools and processes and Security Incident Response Plan and process. Peraton Mainframe security operations work with the MSS SOC to manage all security incidents, including troubleshooting, investigation, response, recovery, and providing evidence as prescribed by **SMM 4.1.5.7 Security Incident Management Process**, and as seen in Section 4.1.1 Incident Response Security Requirements. As part of the response and routine operations, Peraton security engineers update IDS/IPS signatures and IDS/IPS products as directed by VITA, its customers, MSS, and IDS/IPS systems manufacturer within 4 hours or less. Peraton security engineers work side-by-side with the other towers to identify, stop, and mitigate any security incident where events and incidents from other operational environments can potentially affect the Mainframe environment, and vice versa. Peraton has incident response playbooks containing well-rehearsed response actions based on the attack situation, including the nature of the attack, sophistication of the adversaries and their TTPs, the attack vectors being used, the environments directly or indirectly affected, and the impact potential. The MSS SOC coordinates P1, and P2 security incidents response with the MSI JOC using the KSE ticketing system, telephone and/or email. The JOC then reaches out to the Peraton on-call team member as necessary. The MSS SOC enters incident information into the VITA CSRM Archer system. To manage a coordinated effort between Peraton and the JOC, we provide JOC with a quarterly on-call roster that includes names, escalation chain, and contact information of all on-call personnel.

4.3   Risk Management

Peraton designs an optimized risk management program for VITA's Mainframe environment through our collaborative approach working with MSI and Service Towers to implement a well architected and integrated security environment, including responsive security operations and continuous monitoring and improvements to detect, prevent, and control all threats and environment failures. Our approach leverages NIST 800-37 RMF processes to organize our activities and collaboration across services to comprehensively manage risk for the VITA Mainframe environment. Within the RMF, we implement the rigor of risk management activities across all phases of the Mainframe environment's life cycle and operations. This includes identifying emerging threat trends, potential control failures, continuous risk assessments, and attribution and escalation of threats and risks across services. The Mainframe environment includes all architecture and network components managed under the contract, and those that Peraton has operational influence over alongside MSI and Service Towers. **Figure 3** illustrates the RMF process and our alignment of risk management activities.

Even though the RMF process may seem sequential, Peraton's implementation is continuous, in that our engineers are continually reacting and adjusting to the dynamic nature of threats to identify susceptibility of Mainframe environment components and data.

Peraton's risk management activity implements VITA's MSI model and vision mandating that all vendor and stakeholder functions operate in unison, including security risk management of the Mainframe environment. Through consistent and routine collaboration, participation on change control, incident responses and root cause analysis, in addition to reporting, and making available ingestible logs, we provide VITA and Customers access to information including common risks and controls, reports, risk logs, action plans, key controls and risk indicator data.

As **Step 0, Prepare** of NIST RMF process, Peraton implements a collaborative approach between MSI, Service Towers, and VITA stakeholders to create, implement, and communicate the risk management baseline and sustainment strategy. VITA environments are dynamic and subject to risk drift in lockstep with changes occurring due to routine operations and evolving threats. Peraton conducts frequent risk assessments as part of the change management process (SMM 4.1.3.8, and 4.1.4.1) and as newer threats and TTPs, vulnerabilities, and vendor product EOL/EOS are identified.
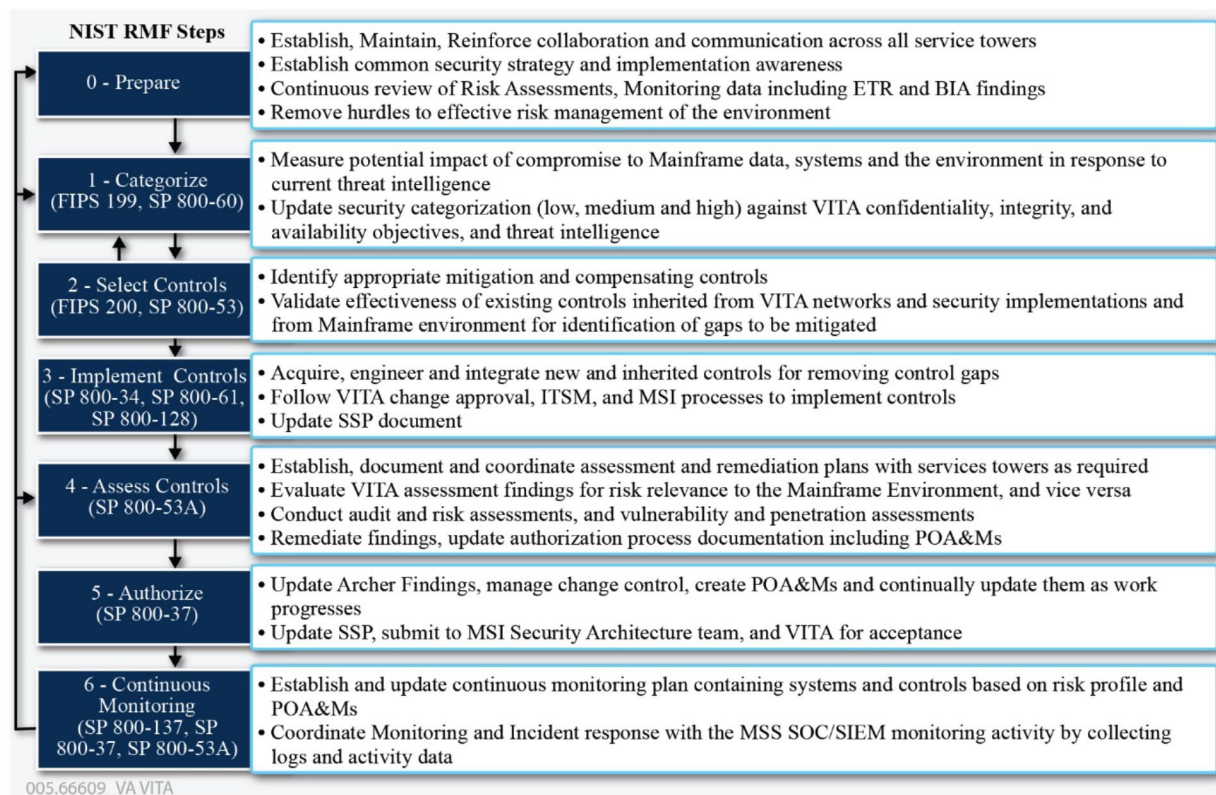
Figure 3: Peraton Risk Management Process – *Peraton's RMF process is a six-step iterative approach to manage risk and reduce the impact of emerging threats.*

Peraton program and security function leadership participate in and maintain visibility of this step, including working with VITA leadership to facilitate continuous improvements. We maintain visibility to VITA, MSI, and Service Tower team stakeholders through routine reporting and dashboarding using VITA CSRM Archer system, including sharing common risk and controls information, reports, risk logs, action plans, key controls, and risk indicator data.

For **Step 1, Categorize**, Peraton engineers use FIPS 199/200 guidance for initial and recategorization of VITA Mainframe assets and data in tune with evolving threats acquired from threat intelligence and risks identified during risk assessments. Risk-adjusted categorizations lead to identifying and implementing newer security and privacy controls and enhancements to existing controls, and compensating controls in compliance with the requirements of RMF process Steps 2 and 3. By using data, system, and component-level categorizations and risk profiles, and their susceptibility to attacks based on threat intelligence, Peraton engineers accurately quantify risk metrics, including risk indicators that drive operations and monitoring activities to effectively manage and mitigate risks. As we discover shared risks, Peraton engineers and leadership provide sharing and escalation of those risks through Archer and KSE systems to MSI, Service Towers, and VITA stakeholders.

During Step 2, Select Security Controls, Peraton engineers identify, document, and implement/augment interoperability controls in compliance with VITA policies and NIST directives across all infrastructure components that integrate disparate applications, systems, and networks. These controls include common controls, inherited from VITA infrastructure or available within the Mainframe environment, along with supplemental controls required for additional countermeasures addressing known control weaknesses. Controls included cover all functional areas, such as MFA, systems and platforms, applications and databases, network configurations and segmentations, points of external and internal integrations, cryptography and keys for encrypted platforms, data, communications, and connecting endpoints.

During Step 3, Implement, we implement/augment the selected inherited and Mainframe enclave controls using sound engineering practices in accordance with NIST 800-70, National Checklist Program for IT Products; NIST SP 800-207, Zero Trust Architecture; and NIST SP 800-160, Developing Cyber-Resilient Systems. We harden systems and applications by configuring and implementing applicable controls based on a wide variety of standards, including Center for Internet Security (CIS), Security Technical Implementation Guides (STIG), and associated control correlation identifiers (CCI). We verify compliance of appropriate security configuration settings with selected security standards for the Mainframe and VITA infrastructure endpoints within the VITA environment to establish a baseline of security controls enabled for continuous monitoring of the environment.

During Step 4, Assess, we review and assess security controls and configurations collaboratively with MSI and the Service Towers—via vulnerability, configuration, and penetration assessments to establish and document changes to baselines and subsequently apply control adjustments and newer countermeasure implementations to address known control weakness and maintain security compliance of the environment. Technical assessments are routinely required to identify susceptibility of VITA hardware, software, and network to emerging and existing vulnerabilities. Using available tools and processes, we assess Mainframe enclave security control and configuration effectiveness using risk assessment methodologies, such as vulnerability assessments, code analysis, and penetration testing. We make sure that risk assessment methodologies and tools are consistent with NIST SP 800-53a, Assessing Security and Privacy Controls and NIST 800-30, Guide for Conducting Risk Assessments. Our leveraged SIEM augments technical assessments in real time by providing alerts to susceptibility of Mainframe enclave components to emerging threats. It shares and maintains currency of newer threats and TTPs derived from multisource threat intelligence feeds to identify individual Mainframe enclave hardware and software components vulnerable to threats and attack vectors. We defend vulnerable hardware, software, and firmware, including those with EOL and EOS status through patching, updates, replacements, compensating controls, and continuous monitoring.

Peraton engineers work with VITA, MSI and Service Tower stakeholders to formalize and obtain approval to operate the environment. This process identifies the risk to environment; if the risk is acceptable, and VITA stakeholders approve operation of the environment. As part of the process for **Step 5, Authorize**, Peraton engineers finalize the POA&Ms that document and track remediations for the Mainframe environment, update/document the SSP and authorization package, and submit the package to the VITA stakeholders for review, acceptance, and as required authorization to operate the VITA Mainframe environment. **During Step 6, Monitor**, Through the MSS SOC/SIEM, we coordinate monitoring to verify that the Mainframe

environment is constantly monitored for adversarial activity and provides policy violation alerts for remediation through the KSE system.

5.0   Operations

Peraton's Managed Mainframe Services Team provides 24x7x365 system console operations, batch scheduling and monitoring, data transmission support, system updates and maintenance and system improvement services to VITA. With existing tools, automation, and standardized processes, Peraton provides real-time monitoring and management by collecting and monitoring system status and metrics to proactively identify issues and trends. Through comprehensive analysis, we evaluate all operational impacts in the delivery of VITA Mainframe Services, responding rapidly to identify and resolve issues before they impact VITA and VITA customers. We include all collected incident data in the VITA KSE tool for customer service awareness and historical work log workflow purposes. All Mainframes, storage equipment, and peripherals associated with the VITA Mainframe Services is located in either the Mid-Atlantic Data Center (MDC) or DXC Colorado Springs (CXC) data center and is under Peraton's oversights for management and monitoring.

While performing the monitoring and management functions described in the requirements, our Mainframe Services Team performs the following activities:

- With automated tools and processes, remove manual interventions for ongoing monitoring and operation activities across all platforms and LPARs.
- Monitor system resources, CPU and storage usage, and I/O activity against established thresholds and targets.
- Monitor processing across all applications, transactions, batch processing and mainframe utilities.
- Monitor workload allocation changes to resolve performance issues.
- Monitor data replication and hardware and SW alerts and take appropriate actions.
- Monitor the performance of online interactive traffic and take appropriate action to resolve online system-related incidents and problems to avoid business disruption.
- Monitor all processing and the environment, alarm systems and environmental controls, and transmission and reception of polling information from outside the organization.
- Perform problem determination and isolation for automated operational processes.
- Create, maintain, and execute system startup/shutdown scripts.
- Perform annual audit of automated alerts and thresholds.
- Issue network and operator commands to control all in-scope computer platforms throughout the organization, including print functions.
- Monitor and manage the impact of application or related scheduled changes affecting system performance.
- Provide incident resolution/escalation of event, warning, alert, and alarm messages.

Console Operations: Peraton will manage, maintain, monitor, and assume control responsibility for all master and subordinate console functions within the VITA mainframe environment. This will include issuing commands to control mainframe platform and LPARs as well as maintaining and updating the documentation for all operational procedures and services, including maintaining accurate information for all Configuration Items (CIs) in the Configuration Management Database (CMDB) deployed within the VITA Mainframe. Our console operations include detailed and extensive system availability management as outlined below.

Managing System Availability: Our approach to managing system availability is built upon an availability management process that is designed to anticipate and prevent business disruption through proactive and reactive activities. Peraton provides feedback to VITA and other Customers regarding the impact of potential architecture and design changes through existing VITA processes such as the Request for Solution (RFS) process. Table 5 describes the Peraton process for managing Mainframe environment availability.

Table 5: System Availability

PROCESS	DESCRIPTION
Availability Management	This process documents how VITA and Peraton create, review, and update/change Availability Management activities for Business Availability, Service Availability, and Component Availability. Activities considered within the scope of this process include the following: ■ Perform availability trend analysis for components identified as in-scope for Availability Management at the time-of-service commencement and for those that are subsequently added through change management. ■ Report results of the analysis ■ Provide VITA with access to availability reports, and SLA reporting
Availability Monitoring and Reporting Process	STS AVLM defines and develops measurement methods; monitors, measures, and reports availability measurements and information for supported services and components; and addresses availability outages, analyzing and improving availability to meet contractual and agreed availability targets. The STS AVLM Manager actively participates in MSI AVLM procedures for any reactive activities, proactive activities, and reporting for supported services or component approved Availability Plan. Monthly, the Availability Manager reports on availability and monitoring for the following: ■ Peraton-managed devices in scope for Availability Management at the time-of-service commencement ■ Any devices subsequently added through CM or Contract Change Orders
Availability Improvement Process	The availability improvement process documents: ■ How Peraton modifies availability or recommends modifications to availability management processes ■ How Peraton reviews availability achievement and recommends changes to improve component availability if required thresholds are not being met The Availability Improvement Process scope includes the following: ■ Analyze reports and data captured from systems management tools to identify root cause for missed availability targets. ■ Recommend changes that will result in increasing the ability to meet availability targets. ■ Review recommended changes with VITA and initiate CM process to implement any approved changes
Business Availability Management (BAM)	The BAM process makes sure we address VITA's business requirements when we plan and implement IT services. We use information detailing how VITA and VITA Customers currently use IT services, along with component-specific information, to align current and future IT services to meet mission-critical business requirements
Service Availability Management (SAM)	We use the SAM process to manage the availability of currently supplied IT services to meet VITA's needs. We monitor SLAs for these services and take appropriate actions make sure they meet the Service Level Objectives (SLO)
Component Availability Management (CAM)	We use the CAM process to monitor, analyze, and improve the IT infrastructure for each service. The CAM process makes sure that we provide IT services at the levels specified in SLAs

We report and analyze availability metrics, assess the impact of changes within the Mainframe environment, recommend improvements, and collaborate with VITA and affected agencies to meet and exceed objectives. A key output from Availability Management is the identification of issues requiring problem management before they disrupt VITA business operations.

Our solution incorporates methodologies, practices, and tools to help VITA maintain specific agency operational levels across the infrastructure. Peraton's Mainframe Services Team incorporates the analysis and plans necessary to help minimize the probability and impact of service interruptions.

Implementing the System Availability Management process reduces the risk of not meeting agency needs during peak processing hours due to lack of IT support or resources. With significantly fewer availability issues, Peraton can meet and exceed the defined the defined Service Level Agreements (SLA) and Mean Time To Repair (MTTR) for service.

Online and Batch Processing: Peraton will manage, maintain, monitor, and control the VITA online and batch processing across all agency's applications and interactive started tasks. Peraton will manage and

maintain all batch and CICS schedules to ensure processing occurs within the defined and agreed to windows to maintain maximum performance while also meeting batch completion times. This includes automated scheduling of batch jobs, CICS regions, Database instances and asynchronous tasks including backups. Peraton will maintain batch scheduling and CICS tables, as well as batch calendars to include holidays with no batch and other special processing dates. Peraton will maintain scheduling parameters and definitions within the batch and CICS tools used to automate manual procedures and improve the quality of the operations We further monitor online transaction execution and batch processing and backups to ensure all are executed in the correct sequence. We use automation to monitor and control the availability of the online regions, alerting the technical team of issues for immediate response. We monitor and control transactions using system tooling across batch and online. Batch Monitoring teams will repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual (SMM) and escalate abnormally terminated jobs to the appropriate agency application or support team as needed to repair application related abends. Emergency contact information and procedures required to perform escalations is collected from Customers and documented with applicable job documentation per Customer guidance. Peraton will help the application support teams to perform problem identification and resolution consisting of production batch restarts and reruns. All repair actions will be performed in accordance with the Incident Management and Service Level requirements. Peraton will monitor, control, and manage job outputs, print queues, job priorities, and take printers in and out of service and start/stop the spool and drain printers as needed and applicable.

Data Transmission Support

Peraton will continue to manage, maintain, monitor, and control data transmissions using existing VITA file transmission software and services, monitor the system log for transmission failure and issues, and re-transmit files as appropriate. Peraton has deployed SMF and syslog controls to detect failures and notify the appropriate parties for correction based on the transmission node error (sender and receiver). All data transmission operational support will be consistent with commercial and VITA standards.

System Updates and Maintenance

Peraton will continue to provide system updates and maintenance for all Mainframe hardware, software, and services following our detailed processes outlined in Sections 2.3 Patch Management and 3.1.2 Technology Requirements. This will include performing system hardware and software upgrades with VITA and other Customers. Performing periodic and emergency systems maintenance and IPLs in accordance with VITA procedures as documented in the SMM to minimize the impact to VITA and other Customers' businesses. Peraton will perform computer shutdowns and restarts and execute customary utility functions and terminate utilities or run-away processing that impact users or other processing. All shutdowns and restarts will be performed with VITA approval following the defined operation procedures. Peraton will work closely with VITA Application Development & Maintenance (ADM) groups from the initial design of any system update or maintenance change all the way through deployment and including production processing cycles and following the appropriate change management procedures.

System Improvement

Peraton will continue to provide ongoing enhancement and improvement capabilities and efficiencies through system tuning and other run-time improvements. These will include performing regular monitoring of utilization needs and efficiencies, and report regularly on tuning initiatives. Peraton will produce trend reports to highlight production issues and establish predetermined actions and escalation procedures when batch or online issues are encountered. Peraton will make appropriate adjustments to support timely batch and online application execution. Peraton will proactively monitor and report to VITA on resource shortages, and report utilization statistics and trends on a monthly basis and identify opportunities for VITA to reduce costs and improve system performance.

6.0   Production Control and Scheduling

Peraton assumes responsibility for all batch scheduling and production control services through a 24x7x365 staffing model. This involves following VITA or customer requirements in performing the activities associated with defining and maintaining an application's batch processing within the automated scheduling system, executing predefined application cycles in the proper sequence, and managing the movement of source/object code and developed programs/applications from test, through model office, to the production environment. VITA currently has 9,278 batch jobs defined in the scheduling system that are mission critical to both DMV and DSS, which Peraton is extremely familiar with and has been very successful in performing. Some key items included in these services include:

- Provide appropriate system resources (CPU, disk, and tape storage), tools, and procedures to help process user-initiated batch jobs.
- Maintain the necessary operational resources to support VITA-submitted or batch-scheduled jobs and additional requests for backups and restored batch processing.
- Communicate our batch processing definitions.
- Maintain, manage, and monitor BMC master scheduler and help perform batch scheduling and batch monitoring activities.
- Schedule, monitor, and manage on-request and ad hoc batch processing and provide approved batch schedules, including job flow, dependencies, and exception conditions.
- Add and maintain a master schedule with dependencies into the automated scheduling system based on VITA or Customer batch requirements.
- Work with VITA or Customers as needed manual restarts / re-runs, special requests, schedule approvals, and priority jobs based on deadlines.
- Support the set up zSeries file system datasets and Job Control Language (JCL) for the data files.
- Work with third parties as needed to troubleshoot L2 / L3 support issues.
- Analyze abnormally ended jobs caused by conditions external to production programs and escalate abnormally terminated jobs to the appropriate agency application team in accordance with batch escalation and reporting procedures and follow incident management processes.

Peraton's Production Control team is responsible for Production Control functions, including maintaining and making changes to job dependencies identified within the scheduling database system. The Production Control team modifies schedules based on special requests, and coordinate resolution of scheduling conflicts to maintain VITA schedule priorities. Peraton adds and maintains the defined batch schedules in the scheduling systems and maintains the scheduling database system.

Peraton maintains the list of the application owner of each scheduled job and monitor the execution of the scheduled batch cycles. We identify and investigate overdue or abended jobs. Batch incidents will be reported and escalated to the appropriate agency application support team. Peraton batch teams assist in performing problem identification and resolution and perform batch restarts and reruns as directed by the agency application team.

7.0   Technical Support

Peraton's approach to providing operations technical support encompasses the necessary tasks and activities to meet VITA's using the processes and procedures currently in place for successful delivery, enhancing to meet any additional requirements of the Agreement and Service Levels.

Storage Management Approach

As described in detail in Section 9.0 Online Storage and Backup Management, we manage the VITA integrated storage infrastructure of Dell storage appliance for VITA's online storage and virtual tape needs. This storage and backup architecture is sized based upon our analysis of historical storage utilization and performance data and trends. To deliver and manage the storage infrastructure, we provide the comprehensive

services of installation, facility management, project management, operations monitoring, storage system maintenance, and ongoing operational support of online and tape storage. The operational support of online and tape storage components includes performance management, DASD-related product support, catalog management, and media maintenance. Media management services comprise device-naming standards, usage guidelines, and the storage and archiving of files and data, including offsite DR storage. Additionally, we provide support for file-naming standards, enforcing standards, and maintaining the online storage and virtual tape services.

System Programming and Management

Our system software programming and management approach provides for the ongoing installation, configuration, maintenance, and support for system software products. We implement our established processes and procedures to meet capacity, performance, availability, and integration objectives and support the applications and business workloads of the Mainframe environment. Using automation as available, performing the tasks and activities for system-level components provides a stable, high performing and available Mainframe environment. We manage system software to provide interfaces to VITA systems and applications while maintaining system-level components through the following activities:

- Resolving system software and cross-product interface problems
- Analyzing and tuning system files and overall system performance
- Performing backup and recovery of system files
- Providing configuration information for initial setup and ongoing support
- Configuring, installing, testing, supporting, and maintaining DB2, ADABASE, and CICS system-level software
- Providing system integration support
- Providing information on planned changes in product functions that may impact VITA applications before scheduling software maintenance.
- Testing the applied software preventive maintenance before it is released for production processing.
- Scheduling all software maintenance changes using the approved CM process
- Scheduling downtime as appropriate to perform required software preventive maintenance, installation, and testing.

Capacity Management and Planning

As described in Section 3.1.5 Capacity and Performance Requirements, we perform Capacity Management activities to support VITA's and VITA Customer's Mainframe capacity needs. We apply the same approach currently in place to monitor, manage and address capacity needs. Using a practice that observes trends and plans for business changes, we maintain optimal computer resource capacity by evaluating usage patterns and configuring and managing system resources to meet the processing and storage demands.

Performance Management and Tuning

As described in Section 3.1.5 Capacity and Performance Requirements, our performance management activities focus on providing the agencies with the necessary system performance to achieve their business mission and program objectives. We monitor the Mainframe environment, including processor activity, memory usage, data storage devices, and network devices. Through data obtained from the infrastructure components, we analyze performance metrics, thresholds, and trends to proactively tune and implement performance changes. Monthly, we provide performance reports that summarize system performance and identify potential system improvements that contribute to system performance and efficiency.

Hardware Infrastructure Management

Our approach to managing infrastructure hardware follows processes and procedures to monitor, manage, and maintain the hardware components, as follows:

- **Monitor** – We actively monitor hardware components for alerts, errors, and events that indicate hardware issues that impact availability.

- **Manage** – In conjunction with the change management process, we configure and update hardware configurations to support online and batch processing, storage, and network infrastructure.
- **Maintain** – We engage with Mainframe hardware environment vendors, including IBM and Dell/EMC to regularly assess hardware maintenance issues. Within this activity, we schedule and perform preventive maintenance, including microcode updates, firmware updates, and other hardware maintenance tasks to maintain system availability and performance.

Account Management and Provisioning

As described in Sections 4.1.4 User Authentication and 4.1.5, User Authorization, we manage and provide user accounts in accordance with VITA policies and SMM 4.1.5.6 Access Management. We apply access controls, managing and reviewing accounts. As part of our ongoing improvement to the user authorization process, we hold quarterly user access reviews to look at the number of unused, suspended, or disabled account and review progress on user account cleanup efforts.

Interface and Data Transfer Management

Inclusive of our approach to system software management, we monitor and manage the system interfaces, which includes monitoring for interface alerts, error, and events, following established incident management processes to resolve interface issues, escalating where necessary to interface partners to minimize business disruption. Utilizing existing file transmission software and services, we monitor the system log for transmission failures, issues, and re-transmitting of files. This includes the deployment of SMF and syslog monitors to detect failures and notification of the appropriate parties for correction on the transmission code.

Billing and Chargeback

Peraton has fully integrated with the VITA billing, chargeback, and utilization tracking system under the legacy contract. We will leverage this current process and adjust as needed to meet the new requirements in the Agreement. Each month, Peraton collects Mainframe system processing data, formats it in compliance with SMM 5.3, Mainframe RU Listing, and delivers to the MSI ITFM team for ingestion into the ITFM system. The data is processed within the system and used to generate a supplier invoice to VITA for services provided and chargeback customer invoices to support cost recovery. We support investigation and resolution of any chargeback disputes raised by customers regarding billing data provided from the Mainframe. Peraton works with the MSI and VITA as necessary to update billing data collection and delivery to support new billing triggers required by the new contract and ensure a seamless transition to the new billing model.

Technical Consulting and Advice

Our team of experienced professionals have decades of industry experience, understands the intricacies of Mainframe systems, from hardware to software, and is dedicated to empowering customer Application development and maintenance staff with the knowledge and tools necessary to get the most out of the Mainframe technology available. We work closely with customer teams to assess current systems, identify areas for improvement, and support implementing best practices in Mainframe development to maximize the efficiency, security, and scalability of the Mainframe platform.

7.1 General Technical Support

Peraton continues to provide Technical Support to VITA with the same resources and following the same proven procedures we use today that are part of our Mainframe Delivery Framework outlined in Section 2.0 Common Services.

Our established and approved process controls plan and manage changes to the IT infrastructure by authorizing and reviewing test, implementation, and release plans. We respond to incidents and problems and provide continued support through resolution, as required and in accordance with established service levels and severity definitions, to meet online system and batch availability schedules. In addition, we provide technical advice and support to the Customer application development and maintenance teams, and DBA staff, as needed.

Incident Management

Peraton works closely with the MSI to quickly identify and resolve incidents through the Incident Management process documented in SMM 4.1.5.2, Incident Management Process. We work in conjunction with the MSI and other suppliers to identify and improve the incident management process to shorten time to resolution.

When incidents are received, we troubleshoot and resolve issues and provide end-to-end ownership of an incident by continuing to monitor tickets escalated to other resolver groups, whether to our team or others. To support response service levels, we make sure tickets are picked up or escalated within predefined time frames, depending on the severity/priority.

Our processes include incident identification, incident logging, initial investigation and diagnosis, assignment or escalation, resolution, closure, and delivery of the customer satisfaction survey, with metrics submitted for trend analysis. To prevent rework or repeat calls, we make sure that the resolution was successful by confirming with the end user, and making sure the knowledgebase is updated with any improvements to the process.

Incident Escalation and Management: When an incident cannot be resolved by the initial assignment, the issue is escalated for advanced troubleshooting. Incidents are initiated by automated detection systems, such as BMC's Control-O SW. if not resolved by self-healing automation, our systems automatically escalate to Tier 2 through our MDC automated paging systems a part of our ITSM tool stack and with Service Desk monitoring to be sure our teams rapidly address them. For Severity 2 and other less critical incidents, the Tier 2 Analyst accepts the ticket and works it through to resolution. If the Tier 2 Analyst cannot resolve the issue, they escalate to or conference in the Tier 3 support group or vendor, as applicable, following defined escalation procedures, and using warm transfers.

All resolution steps are documented within the ticket, with notification of the appropriate stakeholders according to incident severity. Throughout the incident management process, we frequently update customers on status and progress, using clear and concise communications as defined in the Communications Plan. If an incident is low severity but of wide interest, we post status updates to the service portal, if approved. We close the ticket after resolution is fully validated.

For major incidents, we engage the Major Incident Management process and assign a situation manager to coordinate and facilitate activities leading to service resolution. Quick response during a major incident is essential to rapid service restoration. After an incident is classified as a major incident, activities follow VITA's Major Incident Management process timeline. Post-event, the situation manager provides an AAR describing actions taken, initial assessment of root cause, and any lessons learned. Major incidents, as with all reoccurring and high-severity incidents, are escalated to the problem management process.

Problem Management

We work closely with VITA to reduce the likelihood and impact of incidents by identifying actual and potential causes, creating corrective action plans, and managing workarounds and errors. We coordinate with VITA to expand and codify a robust problem management process.

Peraton leads and facilitates the problem management process illustrated in **Figure 4** by gathering specialists and stakeholders who handle the problem, discuss, and analyze the data, and prioritize and determine the most appropriate problem owner. Using data from automated tools and structured problem-solving methods and techniques, such as predictive modeling and traditional root cause

Problem Identification	Problem Control	Error Control
• Identify/log problems in ServiceNow • Incident trend analysis • Recurring issues • Integration with Major incident response • USAID engagement • Information/data from USAID, internal teams, suppliers	• Write problem statement • Root cause analysis using structured tools/methods • Document workarounds • Create know error • Prioritize (create backlog and manage problems using risk management techniques)	• Manage known errors and track actions to closure • Identify permanent solutions and corresponding request for change (if justifiable according to risk/cost/benefit) • Notify users and verify that problem has been fixed • Evaluate effectiveness and provide feedback

009.66609_VA VITA

Figure 4: Proactive Problem Management Process – *minimizes the impact of problems and prevents recurrence.*

analysis approaches, we focus on root causes and contributing factors. From this deep understanding, we transform ambiguities about why an incident occurred into actions for correction, reoccurrence prevention, and proactive systemic improvement.

We track and report problem backlog and status for quick access and transparency to VITA. We document lessons learned, process improvements, and innovations to reduce the probability of similar problems occurring in the future.

Problem management works together with incident management and change management to increase IT service availability and quality. When problems are resolved, we record information about the resolution. Over time, we use this information to enhance resolution times and identify permanent solutions, reducing the quantity and resolution time of incidents, which results in less downtime and less disruption to business-critical systems, and provides:

- Higher availability of IT services.
- Higher productivity of business and IT staff.
- Reduced expenditure on workarounds or fixes that do not work.
- Reduction in cost of effort in firefighting or resolving repeat incidents.

Level 2 & 3 Support

Peraton provides Level 2 & 3 support, to include technical advice and support by the Mainframe Services Team staffed with mainframe environment SMEs to address support issues. As the primary interface with OEM vendors, the Mainframe Services Team responds to issues, incidents, problems, and support requests. VITA personnel interface with Peraton technical teams to implement changes required to support the Mainframe environment. Specific responsibilities of the Mainframe Services Team include:

- **Change Management Support** – Participating in CAB meetings enables Peraton Team members to proactively review, plan, approve, schedule, and support VITA's application changes. VITA notifies and coordinates with Peraton for application software updates.
- **System Threshold Monitoring** – Peraton establishes threshold levels to measure elements, such as processor, memory, disk, and I/O as required to meet service levels and prevent incidents. In the event thresholds are exceeded, we generate alerts and, if required, create an incident ticket. We notify all appropriate team members to resolve the event and update the ticket as required.
- **System Software Support, Database & CICS Support** – We install, configure, maintain, and provide ongoing support for system software products. Peraton modifies system software to provide interfaces to VITA systems and applications while maintaining any existing special user interfaces as required.

For DB2, ADABAS, and CICS support services that maintains the system-level components of the software environment, support activities include:

- Resolving system software and cross-product interface problems
- Analyzing and tuning system files and overall system performance
- Performing backup and recovery of system files

- Providing for database subsystem availability following agreed start and stop times.
- Creating, maintaining, and executing DB2, ADABASE, and CICS system startup/shutdown scripts and operational processes
- Performing startup/shutdown of the DB2 and CICS subsystems
- Providing configuration information for initial setup and ongoing support
- Synchronizing VITA data and applications with DB2 and CICS files or any catalog restore processes.
- Configuring, installing, testing, supporting, and maintaining DB2, ADABASE, and CICS system-level software
- Providing system integration support

Additional Support Activities: Other support activities performed by Peraton include testing new products and standard software versions prior to releasing into the VITA Mainframe environment. Working with our corporate engineering resources and alliance partners, we help test new device firmware, tools, and software, which enables us to leverage potentially high-level production issues in a controlled environment.

TN3270 Emulator Support

Non-COV/Locality and other users connect to the VITA Mainframe to access DMV and DSS business applications using the terminal emulator software that implements the TN3270 protocol. Non-COV or "locality" users are defined as Mainframe users under organizations other than DSS (765) or DMV (154) according to their respective entry in the Mainframe Access Coordinator (AC) list.

In support of users connecting to the VITA Mainframe Peraton will:

- Respond to incident tickets and service requests in KSE submitted by or on behalf of users.
- Provide issue resolution support for
  – TN3270 emulator configuration and software recommendations
  – Authentication and authorization issues such as password resets and account suspensions on the Mainframe
- Provide guidance, as reflected in KSE tickets, on details for creation and modification of firewall rules within locality IT and COV enterprise.
- If firewall modifications are required, advise locality on the process to submit a COV enterprise firewall change request via CAM or BRM
- Process Access Request service requests submitted through the "Logon ID Request – IBM Mainframe" form located on the VITA website to add, modify, suspend, and delete accounts and authorize access.
- Reassign incident tickets and service requests related to Business Application issues to respective customer agency, either the Department of Motor Vehicles (DMV) or Department of Social Services (DSS).
- Provide guidance on engaging the user's IT support organization to resolve issues that Peraton cannot directly address such as DNS resolution, local network configuration, firewall configurations, internet service provider (ISP) related issues, software installation and licensing.
- Will inform a locality if it has an outdated/unsupported version TN3270 emulator client software, advise as to the steps necessary to secure current software; and that the software is necessary for system access; Peraton will continue to support users of the locality to the extent possible until current software is secured.

Peraton assumes:

- VITA will retain ownership and governance responsibility over the Mainframe Access Coordinator (AC) list and its management applicable to all users of the VITA Mainframe.
- VITA will review, validate, and update the AC list at least annually.
- VITA will maintain a Customer Account Manager (CAM) and Business Relationship Manager (BRM) responsible for managing communication and as a point of escalation for localities.
- CAM or BRM will submit firewall rule management requests on behalf of localities as required.

- User's IT support organizations are responsible for procuring and installing TN3270 emulator client software which maintains compatibility with applicable security and encryption protocols required by applicable COV standards and policies.
- Locality users are subject to the applicable Policies published and managed by the respective Business Application owner - the Department of Motor Vehicles (DMV) or Department of Social Services (DSS).
- Business Application owning agencies which are hosted on the Mainframe are responsible for ensuring locality users accessing those Business Applications via Time Sharing Option (TSO) connections are made aware of and adhere to applicable standards and policies published and managed by the user's respective customer agencies, either DMV or DSS, as they pertain to use and access of the VITA Mainframe and other COV resources.

Peraton reports performance data and resource utilization statistics related to system software release level upgrades as required, approved, and available. Activities include the following:

- Providing information on planned changes in product functions that may impact VITA applications before scheduling software maintenance.
- Testing the applied software preventive maintenance before it is released for production processing.
- Scheduling all software maintenance changes using the approved CM process.
- Scheduling downtime as appropriate to perform required software preventive maintenance, installation, and testing.

Finally, Peraton interfaces and integrate with third-party software vendors for system software changes. We develop and maintain a software refresh template by evaluating and selecting software products based on the defined Mainframe services. Peraton implements the software refresh process as required to maintain third-party vendor software support.

7.2   Capacity and Performance Management

Peraton provides capacity and performance management support to VITA through a systematic approach that includes the following activities:

- Interactive and collaborative planning for future processing requirements, and system configurations
- Monitor and measure VITA and its Customer service levels, compare to short- and long-term objectives and identify overall resource usage estimates comparing historical actuals, and projecting future utilization.
- Collect reliable and relevant data to analyze and drive decisions.
- Assess data relevancy including current and future demand patterns, bottlenecks, and gaps, and evaluated scenarios, use cases, and trade-offs.
- Monitor and analyze Mainframe metrics and trends.
- Identify new technologies that can improve the performance, reliability, or efficiency of the Mainframe applications and service at acceptable implementation costs.

Through the above activities Peraton will assist VITA in understanding the future mainframe business requirements and provide systems performance reviews and advice on VITA's operation and IT infrastructure, as well as providing current and future capacity and performance aspects of the mainframe business requirements in a cost-effective manner.

We work with VITA to quantify the impact of capacity-related decisions, workflows, and dependencies on critical VITA business functions and capacity targets established within agreed SLAs. Our technical professionals perform activities required for monitoring and optimizing performance in order to reduce costs and improve Service Levels. We research and identify and qualify opportunities to improve capacity by evolving technology and to forecast future capacity requirements. We provide performance monitoring, tuning, and reporting across all capacity items including OS and application levels. We provide recommendations for improving capacity supporting Mainframe services to VITA through our monthly

reporting and annual planning cycles. Our performance testing and analysis of the resulting information provides input to the continual service improvement process.

Peraton establishes a measurement structure to capture, analyze, and report on capacity usage, trends, and risk areas on an ongoing basis, which includes implementing thresholds and triggers that promote identification and response to capacity issues. The resulting information is input for our continual service improvement process. We also use information from our analysis of trends in customer demand for service to recommend modifications and improvements to service capacity and hardware configuration. For example, balancing capacity requirements between online transactions and batch scheduling may require reallocating CPU resources to accommodate different load requirements. Our capacity professionals supply support to resolve capacity-related incidents and problems. We make sure that capacity planning is an integral part of activities to develop or enhance Mainframe services We will further assist the ADM and DBA groups in the analysis of application requirements to determine the impact on the mainframe capacity while in the application design and test phase.

Peraton will continue to conduct system performance testing and provide test results reporting to VITA. Using best practices and OEM recommendations we will configure the logical partitions (LPARS) as requested by VITA to maximize capacity utilization.

Peraton will perform appropriate projects to install and upgrade hardware and software required to provide effective capacity to maintain and improve performance while continuing to meet architectural requirements. These projects can include CPU, storage devices and other capacity items. All upgrades will be coordinated with VITA, third party vendors and other suppliers as appropriate.

Peraton will maintain and make available current, comprehensive, and complete channel, DASD, network, server, and total system documentation to VITA to support capacity and performance management.

7.3   Configuration Planning

Using Peraton's Hardware Asset Management processes, we manage and fully document system configurations, to include processor configuration and input/output completion port (IOCP) data, storage and tape configurations, and configurations of all related I/O and network devices. We maintain configurations within our asset management tool and include configuration specifics for the Mainframe itself, as well as Tape, Disk, Network, LPARS, CICS Regions, and Database instances. As an example of our data gathering tools, we use Tivoli Asset Discovery for z/OS (TADz) for asset discovery. Peraton also maintains and documents software configurations for all Mainframe software and tools, including all source code required to support the VITA application processing environments.

8.0   Database Support and Management

Peraton provides VITA and VITA Customers with database management, administration, and support, including the planning, maintaining, and monitoring of databases in the z/OS system environments. Within our Mainframe Services Team, we staff database SMEs to provide support for VITA Customer databases. As application needs change, Peraton plans for changes in the size of databases and implements these based on information supplied by VITA or VITA Customers. Peraton technical support and operations team maintain, operate, and upgrade automated monitoring tools to monitor database performance, perform database shutdowns and restarts as necessary, and perform database reorganizations to optimize performance when required. We maintain databases to meet performance standards, maximize efficiency, and minimize outages. Peraton tests and implements database environment changes, monitors database capacity, corrects out-of-capacity situations, and provides performance analysis to confirm physical database requirements to support VITA's business systems.

Peraton provides technical advice to the VITA Customer application teams and database administration groups and help application DBAs perform testing and operating system and database performance tuning. Along with the day-to-day support of the database systems, Peraton develops, documents, and maintains physical database standards and procedures; participates in determining physical database changes associated with application development and maintenance efforts; and implements the necessary changes to relevant databases, subject to VITA's review and approval.

Peraton performs physical database application administration functions required for production databases. These functions include storage management services, installation and maintenance, configuration and monitoring of database software products, backup and recovery, and database log management. We maintain, update, and implement database archive processes and procedures to recover from an outage or corruption and provide physical database management support, including providing backups and restores of application data. Peraton maintains documentation on files generated by the file management systems and provide technical advice to VITA application DBAs in performance testing and operating system. **Table 6** provides Peraton's database support activities.

Table 6: Peraton's Data Support Activities

SUPPORTING DATABASE ACTIVITY	TASK
Availability	▪ Maintain the DB2 and ADABASE subsystem procedures and JCL. ▪ Startup and shutdown DB2 and ADABASE regions ▪ Support DB2 Distributed Data Facility ▪ Provide emergency system restart and problem resolution to maintain online availability of database system software and licensed vendor supported software products. ▪ Support system software–related issues, 24x7x365. ▪ Schedule the availability of application databases, tables, tablespaces, and indexes ▪ Request schedule changes for the startup and shutdown of database regions
Tuning	▪ Allocate, maintain, move, and tune database environments and related subproduct system datasets. ▪ Monitor usage of trace facilities and System Management Facility (SMF) data to monitor performance and audit guidelines. ▪ Perform regular system tuning and review of memory/resource consumption based on performance reporting and online monitoring. We coordinate these activities with various software support groups and the customer support staff. ▪ Provide application storage support, including application dataset placement and movement and performance. ▪ Tune and monitor application files, databases, and programs. ▪ Execute image copies and backups of application catalogs and directories with reorganizations as required
Problem Resolution	▪ Provide problem research and resolution of system software–related issues. ▪ Interface with change support and vendor software support as necessary to resolve system software problems or issues. ▪ Communicate system software problems or issues to DBAs, software support, operations, and software support management for DB2. ▪ Provide the first level of contact from application engineers if an application is experiencing a problem and escalate the problem to the appropriate Peraton technical resource. ▪ Diagnose and support application program problems
Software Maintenance	▪ Install new database subsystems and related subproducts. ▪ Install upgrades of existing database subsystems and related subproducts ▪ Maintain DB2 subsystem and related subproduct system software parameters. ▪ Maintain the appropriate System Modification Program Extended (SMP/E) environments. ▪ Apply preventive/corrective maintenance Program Temporary Fixes (PTF) and High-Impact Pervasive (HIPER) PTFs on test and production system software libraries.

SUPPORTING DATABASE ACTIVITY	TASK
	▪ Support a database online monitor, including batch reporting tools, where applicable, for use by DBAs
	▪ Perform application file/database allocation, loading, backup, image copies, restore, recovery, reorganization, and other application-related utilities.
	▪ Provide application-level support, such as creating databases, tables, tablespaces, indexes, and any application-specific tuning and monitoring.
	▪ Maintain application-owned database storage groups and support all application-owned objects.
	▪ Participate in maintenance and CM of application objects, including programs, JCL, Data Definition Language (DDL), and plans.
	▪ Perform functional testing of applications after software changes
Security	▪ Enforce database system security and audit conformance.
	▪ Use database trace facilities and SMF data to monitor conformance to audit guidelines.
	▪ Provide a security exit, if applicable, by which the account can maintain secondary authorizations if used.
	▪ Administer application-level database security.
	▪ Administer application-owned security rules
Disaster Recovery	▪ Execute image copies and backups of database system software catalogs and directories.
	▪ Provide disaster recovery of system catalogs, directories, logs, bootstrap datasets, and related DB2 and ADABASE and subproduct system software.
	▪ Execute image copies and backups of application catalogs and directories.
	▪ Participate in periodic disaster recovery drills.
	▪ Assist with application-level disaster recovery

8.1 Database Administrative Support

Peraton's approach for providing database administrative support includes the tasks detailed in **Table 4**, Database Administrative (DBA) Support Activities and Tasks in Section 8.0 Database Support and Management. Using database SMEs from the Mainframe Services Team, our DBA support focuses on providing administrative support that maintains database performance through ongoing performance analysis. This includes evaluating and implementing physical database changes, assessing, and optimizing system and networks to lower latency impacts to relevant databases. We support quarterly audit of the database administrative and maintenance function by collecting and providing evidence and artifacts and physical inspections as necessary. Additionally, we evaluate existing documentation, with documentation updates created and applied through the course of normal operations and integrated into the change management process. Physical database standards and procedures used to monitor, maintain, and operate the databases are included with documentation and reduce the risk of database operations by providing all staff that with clear and comprehensive documentation.

Our SMEs provide the necessary support for database testing and performance tuning and rely on their knowledge and VITA experience obtained over the past 7 years. All of these activities contribute to maintaining availability, performance, problem resolution, software maintenance, security, and resilience/DR.

9.0   Online Storage and Backup Management

Peraton's System Backup and Restore Services enables the creation of copies of operating system and data files that can be used to perform system-level and interactive region and subsystem recovery in the event that system data is not accessible in the primary compute environment. This service addresses the operating system files and user catalogs and ensures that the data is replicated to the DR site.

Peraton provides Online Storage and Backup management following our VITA customized storage management process, which is part of our larger Mainframe Delivery Framework and has proven successful to VITA over the last 5 years. We have managed over 15 TBs of disk storage and over 170TBs of virtual tape to meet and exceed SLAs. Peraton's processes align with VITA's requirements, architecture, and ITSM policies and support the VITA Mainframe roadmap.

Peraton manages VITA's integrated storage infrastructure within the z/OS environment, providing a storage service that facilitates direct and reliable access to VITA's application data. Peraton remains current in the knowledge and use of data storage technology and management products and provides day-to-day delivery of the Mainframe storage system, including installation, facility management, project management, operations monitoring, storage system maintenance, and ongoing operational support of online and tape storage. This activity involves providing file-naming standards, enforcing standards, and maintaining online storage and virtual tape services. Peraton also provides media management services, such as appropriate device-naming standards, usage guidelines, and the storage and archiving of files and data, including offsite disaster recovery storage. These services include performance management, DASD-related product support, catalog management, and media maintenance.

9.1 Storage and Backup Architecture

Storage and Backup Management provides the DASD, virtual tape storage environments and backups, and needed support operations and administration to support Mainframe application data and retention requirements. Peraton provides day-to-day delivery activities from a VITA experienced team that includes a specialist knowledgeable about VITA's environment. Activities performed to provide Mainframe and storage management are as follows:

- Manage assets and procurement to provide the scalability required to respond to increasing capacity requirements.
- Leverage technical and operational monitoring staff to provide ongoing support for the Mainframe storage infrastructure.
- Investigate incidents and problems, interface with Incident and Problem Management processes, and provide reporting to VITA as required.
- Maintain and manage tape and DASD replication between production and DR sites.
- Maintain and communicate Mainframe storage policies and processes.
- Help determine the level of required service that will maximize data performance.
- Establish Mainframe storage thresholds for batch and online environments.
- Document, track, record, and report the capacity of Mainframe storage consumed.
- Plan for required Mainframe storage change activities and configuration of new hardware.
- Participate in disaster recovery planning exercises and tests.
- Migrate data to/from existing and new environments.
- Remove and de-install equipment being replaced.

9.2 Engineering

Peraton provides the engineering, architecture, design, and planning processes and support to develop and install mainframe infrastructure including compute, storage and backup capabilities that satisfies the needs of all aspects of VITA's business. Our engineering approach includes a comprehensive review of the entire mainframe environment including Operations, Availability, Automation, Capacity, Performance and Tuning as wells as Security and developing a solution to meet requirements.

Operations: Peraton will perform and provide in-depth analysis of operations data environment for availability management to assist in service outage investigations.

Availability: Peraton will provide a robust and highly available Compute, Storage and Backup infrastructure. Our Mainframe technical support teams continually stay abreast of current and emerging products. Transitioning into the new contract, our solution includes a refresh of the existing Mainframe and storage hardware. To determine this next generation of hardware, and the accompanying sizing, we have analyzed the historical utilization and trends. As a result, we provide refreshed hardware to support VITA over the contract term. This solution eliminates issues with vendor hardware end of support life timing and provides VITA with current technology to meet capacity and performance requirements. Our engineering, planning, and implementation process drives to a nondisruptive refresh that eliminates business disruption.

Automation: After deploying the refreshed infrastructure Peraton will establish and maintain automated alerting mechanisms and monitoring systems for the new infrastructure.

Capacity: Peraton will plan for changes in capacity requirements as outlined in Sections 3.1.5 Enterprise Architecture and Capacity and Performance Requirements and 7.2 Technical Support Capacity and Performance Management.

Performance and Tuning: Peraton will implement performance and configuration tuning of the compute, storage, and backup infrastructure in conjunction with Capacity Management and Change Management processes and establish system tuning and performance programs and processes. Our performance and configuration management will be consistent with Sections 3.1.4 Availability/Performance requirements and 7.2 Capacity and Performance Management.

Security: Peraton will provide appropriate security measures for the Compute and Storage and Backup infrastructure consistent with Section 4 Security Requirements. All engineering activities will include the identification of opportunities for continual improvement, through knowledge management and skill reviews as well as business continuity and disaster exercises. As such Peraton will schedule, lead, and conduct disaster recovery tests. Peraton will lead and perform the on-going disaster recovery plan, maintenance, scheduling and testing to verify mainframe operations can be returned to service and meet recovery objectives.

Peraton identifies opportunities for continual improvement and provides quarterly reports to VITA Customers. We maintain the integrity of compute, storage media catalogs and identify and correct deviations from established system and storage resource performance thresholds and targets, including virtual tape backup functions and processes. We gather technical requirements, establish a work plan, and develop a test plan for all planned change within the Mainframe storage infrastructure. We conduct technical assessments to evaluate risk and impact of the proposed change, consisting of complexity, dependencies, and backout recovery procedures, as well as the feasibility of implementing planned changes.

9.3   Operations and Processing

Peraton remains current in the knowledge and use of data storage technology and management products. We successfully manage storage and backup operations and processing to facilitate direct and reliable access to agency application data. This includes providing event warning, alerting and alarm processing and management across all compute and storage devices and resolving these event warnings, alert, and alarm messages. Additionally, Peraton provides storage and backup infrastructure configuration maintenance, assigns, and initializes online storage capacity, manages the archiving of inactive files and reporting on online storage directories and pools for review by operations and DBA staff.

Peraton will conduct a thorough monthly monitoring review of the mainframe storage operational processing environment using automation software and tools to measure the efficiency of online storage environments and access, and take corrective action as needed. These actions may include performance adjustments to physical equipment and software, file placement and re-placement across directories and pools to improve service performance. All changes will follow the change management process and receive VITA approval.

9.4   Administration

Peraton will provide full and complete administration of the online storage and backup environment for DASD, virtual tape, and supporting operations and administration as needed to meet VITA's Mainframe application data and retention requirements and availability SLAs.

Peraton storage administration manages storage thresholds and data archives and monitors and reports user directories for inactivity. We monitor and maintain file directories and catalogs and administer storage compaction as required, and administer data migration, backup, and archive management. Peraton's storage administration includes monitoring data replication between production and disaster recovery environments (synchronous and asynchronous as applicable) to ensure disaster recovery capabilities are maintained.

Peraton will perform quarterly audits of backup results and jointly review with VITA and provide audit artifacts as needed to support audit and compliance programs.

10.0   User Support

Peraton's approach to providing user support to VITA users, administrative users, and VITA Customers includes providing overall support, advice, and assistance to Mainframe environment users on all aspects of the environment, consistent with the processes and practices currently being delivered by our team. We manage, track, and implement requests for job control and parameter changes with tools to record and track requests, including using the VITA KSE. Following established change, incident, and problem procedures, and in compliance with the SMM and VITA governance processes, we support programmers and users.

As part of user support activities, Peraton provides user account and manages authorization and authentication in accordance with VITA policies and SMM 4.1.5.6, applying access authorization controls following centralized policy, including requests for accounts, permission changes, and other changes as required from originating agency or locality Mainframe ACC. VITA's KSE provides the request system for users, which preserves tickets and actions for logging and management. In addition, ACF2 creates SMF records logging changes to accounts and account creation. Users are authorized based on role and responsibilities assigned, which translates to rights authorizing and restricting them from performing tasks, including document storage. As part of our ongoing improvement to the user authorization verification process, we work with VITA to include user authorizations reviews within the quarterly user access review process. In addition, as part of the user access and authorization review, we capture real-time user activity logs for all Mainframe interactions and transactions. We securely store and maintain logs in virtual tape backups for at least 7 years based on VITA and its customer retention policies.

11.0   Backup and Recovery Services

Peraton's backup and recovery services focuses on maintaining data integrity and availability through comprehensive set of proven methods and services. Our backup and recovery solution enables the creation of copies of the operating system and data files that can be used to perform system-level and interactive region and subsystem recovery in the event the system data is not accessible in the primary compute environment. This service addresses the operating system files and user catalogs. As part of this service, Peraton performs the following tasks and activities:

- Identify backup schedule requirements for operating system files and user catalogs.
- Back up operating system files and user catalog pointers.
- Document and maintain operating system backup processes.
- Adjust system backup functions and processes as and new components are added or deleted, or as operating system requirements change.
- If failure occurs, recover the operating system files and user catalog in the primary or recovery compute facility.

- Maintain databases to meet performance standards and to maximize efficiency and minimize outages.
- Maintain, update, and implement database archive processes and procedures to recover from an outage or corruption.
- Provide physical database management support, including providing backup and restore of application data.
- Provide cataloging of offsite content
- Manage and coordinate offsite virtual tape volumes vaulting.
- Retrieve offsite virtual tape volumes.
- Perform system virtual tape data backup and recovery as required and in accordance with VITA and agency standards, policies, and Disaster Recovery Services requirements.

Upon receiving a valid restoration request, we locate the specific stored data and perform the restoration activity. We maintain a list of end users authorized to request the restoration of stored data. We retrieve backup data images as requested, working as necessary between backup, system administration, and DBA personnel to restore the data and check for restoration accuracy. We then notify the requestor of restoration request completion. Peraton follows established process by which VITA agencies can request recovery of data or files, and document that process for their use.

12.0 Middleware Administrative Services

Peraton provides administrative middleware services for the Mainframe-based tools listed in Section 12.0 of **Exhibit 2.1 (Description of Services – Mainframe)** using our tailored VITA ITIL-based processes. Peraton tracks and monitors the software that supports the VITA middleware environment, including license compliance and usage and software performance monitoring; and provides maintenance, technical refresh, security updates and patches, and release updates requirements. We coordinate with VITA to prioritize, schedule, and execute the required periodic patching and upgrades of the middleware software portfolio following the patch management process described in Section 2.3 Patch Management. Our middleware administrative services fall into three areas: product support, configuration and functional support, and problem resolution support, as described below.

Product Support: Peraton support starts with the set of middleware products identified in the Agreement. We continue to evaluate the software products within the VITA Mainframe software stack, including those identified as middleware, to identify products that are or may be candidates for replacement. As appropriate, we provide recommendations to VITA on middleware product replacements and changes based on replacement criteria focused on cost/benefit and functionality. No product is replaced without following the established VITA approval process.

Peraton installs, upgrades, and changes middleware software to agreed upon release levels. We use standard maintenance windows agreed to by VITA and Customers to apply software updates (installation, upgrade, and refresh) according to established development to QA to production life cycle. Approved middleware system-level changes are executed across all in-scope product instances. We evaluate and coordinate major patches with Customers to minimize impact to the established development and production environments. Peraton implements and administers appropriate middleware management tools on the Mainframe to manage the in-scope middleware instances and provide middleware communication software configuration, installation, and maintenance as applicable.

Configuration and Functional Support: We review and monitor middleware configurations and system parameters, identify potential gaps, and formulate questions and recommendations to present to VITA to maintain a middleware environment with a minimal number of configurations; this, in turn, enables consistent management of the middleware environment in a cost-effective manner. We use ITIL-based processes and procedures to implement approved middleware configurations to ensure consistency across like environments throughout the development to QA to production lifecycle.

We use VITA processes and procedures to manage requirements and changes to middleware users, roles, objects, and other elements, including creating, updating, deleting, and maintaining business software object changes, as authorized by Customers using the change management process. We implement changes for all instances as specified in approved change requests.

Peraton implements processes for the proper maintenance and functioning of middleware systems including load balancing, tuning, and configuration management. Peraton implements changes to modify the configuration subject to VITA's architecture review process. We tune the system subject to the change management process to optimize the effectiveness and efficiency of the middleware environment.

Problem Resolution Support: We perform problem diagnostics and problem resolution on middleware issues using the approved Incident and Problem Management processes. Based on the nature of the issue, problem management involves appropriate Customer stakeholders and could include detailed discussions and participation with the middleware software vendor. We coordinate problem resolution regarding middleware issues at the overall infrastructure level to identify and properly accommodate impacts to other areas of the infrastructure supporting VITA.

13.0 Systems Network Architecture (SNA) and TCP/IP Technical Support

Peraton has implemented logical network design that will provide a Multiprotocol Label Switching (MPLS) network to connect Peraton data centers with the primary VITA data center in Sandston, VA, and the secondary VITA data center in Ashburn, VA. Dual MPLS circuits connect the primary VITA data center and the primary Peraton data center to the Peraton MPLS cloud. A single MPLS circuit provides connectivity from the secondary VITA data center to the Peraton MPLS cloud. Another single MPLS circuit provides connectivity from the backup Peraton data center in Colorado Springs, CO. This configuration provides flexibility and growth by allowing additional circuits and sites to be added to the MPLS configuration without redesign. The bandwidth of the MPLS circuits can be increased within an expedited timeframe from traditional telecommunications circuits.

Peraton's dual MPLS circuits into the primary VITA data center in Sandston, VA and the primary Peraton data center in Clarksville, VA are implemented with geographic diversity to mitigate risk of a single event such as physical damage to carrier equipment and infrastructure impacting both circuits.

Peraton support engineers monitor the health and utilization of Mainframe network connections and use the data as the basis for network trend analysis and capacity planning. Additionally, Peraton will perform SNA and TCP/IP upgrades, redesigns and modifications as required by VITA or VITA Customers.

Peraton has deployed a redundant stack of dual firewalls and routers in the primary VITA data center and both Peraton data centers to manage and secure connectivity between the COV network and the dedicated VITA Mainframe network enclave within the Peraton data center infrastructure.

SNA & TCP/IP Support: Peraton supports Systems Network Architecture (SNA)–based communication and configuration within the Mainframe and between LPAR. Direct external SNA communication was eliminated during the current service contract by retiring all front-end processors and third-party vendor protocol conversion boxes. Peraton network engineers continue to support a small number of external SNA customer connections using IBM Enterprise Extender (EE) technology to extend SNA over TCP/IP networks between legacy SNA locations.

To achieve effective and efficient operations and maintenance for VITA's system software, the TCP/IP support engineers provide comprehensive, day-to-day administration, and support services for the base SNA and TCP/IP services. The TCP/IP support team also perform the following tasks:

- Analyze VITA's current technologies to support this contract and develop standard topologies, diagrams, and documentation.
- Maintain a comprehensive network perspective to apply creative thinking and problem-solving techniques and identify opportunities for innovation.
- Participate and collaborate with VITA teams to implement improvements that solve near-term concerns while advancing the support technologies along the path set by VITA's overall strategic mission.

We collaborate with VITA's local area network (LAN) and wide area network (WAN) groups and third-party vendors, as it is crucial to maintain logical and physical changes to the network infrastructure. Peraton has established standards for all supported network technologies in accordance with VITA rules and will continue to comply with VITA rules.

Peraton Additional Information

Over the past few years, Peraton has successfully acquired a number of complementary businesses, including Perspecta Inc. Our combination has created a leading government mission capability integrator and enterprise IT provider focused on delivering high-end technology-enabled services. The combination also gives us, and our customers access to a wealth of additional resources and capabilities.

Through all of the aforementioned transactions, we have retained the key personnel, management, contracts, and other resources and assets (including the financial resources, employees, subcontracts, materials, facilities, and other infrastructure support) of all of the acquired businesses. We manage our combined business enterprise with a centralized leadership structure, consolidated business systems, and common policies, practices, and resources to effectively serve multiple government customers worldwide. Accordingly, the personnel, resources and qualifications offered and committed in this Agreement, as well as the corporate experience and past performance citations relied upon herein, remain fully available and attributable to Peraton for the successful performance to this Agreement.

Peraton has carefully reviewed all SMM Responsibilities and attempted to identify possible deviations from requirements that would remove overhead and provide innovative services to the Agencies. Our assessment is that most of the SMM requirements are critical to provide necessary and high-quality services to VITA and the Agencies and therefore should not be changed. Since these critical SMM requirements drive most of the cost, we do not see an opportunity for a material reduction in overhead/costs.