Exhibit 2.1

Description of Services – 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

1.0 Introduction

This **Description of Services** sets forth the Services that Supplier will provide, as of the Commencement Date unless otherwise specified. Further, this Description of Services sets forth the processes and systems that Supplier will provide and describes Supplier's obligations to work with the other Suppliers to deliver integrated end-to-end Services to Customers.

Supplier confirms that unless otherwise specifically stated, it will provide a solution that supports all of the business processes described in this Description of Services and its Exhibits, and that all Services, unless otherwise specifically stated, are included within the Base Charges described in **Exhibit 4 (Pricing and Financial Provisions)**. Accordingly, Supplier also confirms that Customers will not incur any other Charges in relation to the Services described in this Description of Services. Many of the requirements contained in this Exhibit require the selected Supplier to document work instructions and procedures for meeting the requirements and cooperating within the Managed Environment through the use of Service Management Manuals (SMM) and Supplier procedure documentation.

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1.	**2.0 Common Services**		
R2.	*Common Services are meant to apply to all sections of this document.* *The Supplier's responsibilities common to all platforms are described in this Exhibit, which include:*		
R3.	*Supplier shall:*	Y	
R4.	1. Provide all required operations 24x7x365 in accordance with agreed procedures, including staffing Supplier Personnel to provide 24x7x365 monitoring.	Y	
R5.	2. Supplier will respond to and participate in VITA Joint Operations Center activities 24x7x365 as described in the SMM.	Y	
R6.	**2.1 General**		
R7.	*Supplier shall:*		
R8.	1. Maintain Security practices to secure data and Applications from threats outside the service center. Supplier to provide for their personnel and Services delivered:	Y	
R9.	1.1. Provide multifactor authentication.	Y	
R10.	1.2. Log all Customer changes and provisioning actions.	Y	
R11.	1.3. Log all administrative access and integrate to SIEM as required by VITA.	Y	
R12.	1.4. Retain and integrate and provide logs for VITA and VITA Customer specified retention periods.	Y	
R13.	1.5. Issue administrative credentials only in a secure fashion.	Y	

R14.	1.6. Encryption at rest will Support the forensic acquisition processes and Software utilized by the Managed Security Services Supplier.	Y	
R15.	1.7. Support and perform for both encryption in transit and encryption at rest.	Y	
R16.	2. Ensure data confidentiality standards and practices are in place to prevent the exposure of data to unauthorized personnel, as well as to manage and review access of Users and Administrative Users that have the ability to store data. Such standards and practices will be documented in agreed procedures as approved by VITA.	Y	
R17.	3. Deploy standard encryption technologies and options to protect Sensitive Data (while in transit and at rest), appropriate to the service models provided.	Y	
R18.	4. Manage Supplier relationships and provide a technical interface to MSI, VITA, VITA Customers, other Service Tower Suppliers (STS) and Third-Party Vendors.	Y	
R19.	**2.2 Operations, Maintenance, and Monitoring**		
R20.	*Supplier shall:*		
R21.	1. Control all In-Scope computer platforms and associated Infrastructure throughout the organization.	Y	
R22.	2. Perform periodic and emergency Systems maintenance in accordance with documented procedures to minimize the Impact to VITA and VITA Customers.	Y	
R23.	3. Maintain, administer, and provide necessary automated tools and processes for Systems management to the extent available in the tool suite jointly agreed by the Supplier and VITA.	Y	
R24.	4. Provide monitoring and management of Servers, Storage Equipment, Infrastructure and associated Devices not located at the Data Centers as indicated in **Exhibit 4.6 (Equipment Assets)**.	Y	
R25.	5. Perform preventive maintenance, including:	Y	

R26.	5.1. Perform all maintenance according to the manufacturer's Specifications.	Y	
R27.	5.2. Provide documentation to VITA (or its designee) and VITA Customers to verify that preventive maintenance has been completed.	Y	
R28.	6. Perform and Support Security audits and Configuration parameters reviews, and make password changes on all Systems as directed by VITA (or its designee) in accordance to agreed upon procedures.	Y	
R29.	7. Assist MSI, VITA and VITA Customers, other VITA Suppliers, Integrated Suppliers, or Third-Party Vendors in resolving End-User Problems and ongoing Application Support.	Y	
R30.	8. Report any potential System Problems in accordance with agreed upon processes.	Y	
R31.	9. 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.	Y	
R32.	**2.3 Patch Management**		
R33.	*Supplier shall:*		
R34.	1. Patch Systems in accordance with VITA Rules.	Y	
R35.	2. Ensure that all Devices and Enterprise Supported Software in the environment (Physical and Virtual) are Patched and maintained (e.g., Operating System Security Patches, performance Patches, firmware, service packs, Versions) in accordance with VITA Rules.	Y	
R36.	3. Supplier shall provide Reports on the status of Patching and vulnerability scans of the environment every 30 days and upon request .	Y	
R37.	4. Supplier shall Patch enterprise Equipment, Systems, Software, and other Devices that are part of Services.	Y	

R38.	5. In the event that the Patch process disrupts Customer operations the Supplier shall roll back the changes made.	Y	
R39.	6. Apply Patches to Devices & Applications within the timeframe guidelines in accordance with Customer's Security policies.	Y	
R40.	7. Communicate with and/or alert the Customer IT Security team when Patches are not Installed within the designated timeframe.	Y	
R41.	8. Integrate and have the ability to export Patch data associated with all Customer Devices.	Y	
R42.	**2.4 Technical Support**		
R43.	*Supplier shall:*		
R44.	1. Provide technical advice and Support to VITA (or its designee), VITA Customer, and other Supplier Application Development and Maintenance staffs as required.	Y	
R45.	2. Troubleshoot and perform Equipment Repairs and manage spare parts where applicable.	Y	
R46.	**2.5 User Support**	Y	
R47.	*Supplier shall:*		
R48.	1. Provide Support, advice, and assistance to VITA Users and Administrative Users in accordance with agreed procedures. This includes VITA Customers.	Y	
R49.	2. Perform analysis to provide optimal use of production resources.	Y	
R50.	3. Perform changes for programmers and Users as requested by an authorized VITA or VITA Customer representative in accordance with the agreed procedures.	Y	
R51.	4. Provide technical Support and administration for various products and Application rollouts to VITA and VITA Customers in accordance with the agreed procedures.	Y	

R52.	**2.6 Personnel/Clearance Management**		
R53.	*Supplier shall:*		
R54.	1. Grant VITA approval rights for key personnel interfacing with VITA and VITA Customers and the right to review qualifications for any-and-all staff servicing VITA and- VITA Customers.	Y	
R55.	2. Grant VITA Customers rights to review qualifications for any-and-all staff servicing that Customer.	Y	
R56.	3. Provide controls and ensure that advanced Security operations Functions and escalation roles are performed by senior staff cleared to conduct those Functions and roles.	Y	
R57.	4. Provide controls and ensure that personnel complete all mandatory training in accordance with the VITA, Commonwealth, & Federal requirements.	Y	
R58.	5. Ensure that all Supplier Personnel and the personnel working for a sub-contractor pass the VITA mandated security background check process.	Y	
R59.	6. Personnel shall disclose any changes that may Impact their background check results in accordance with VITA Rules.	Y	
R60.	**3.0 Enterprise Architecture**		
R61.	**3.1 General Architecture Requirements**		
R62.	*Supplier shall:*		
R63.	1. Track the lifecycle of all Software and Hardware used to deliver the Services. Supplier, in its response, should indicate how it will track Software and Hardware and construct services so that Customers only pay for what it needed/used.	Y	
R64.	2. Only use Approved versions of the technologies covered within the COV Technology Roadmaps. Please see: https://www.vita.virginia.gov/policy--	Y	

	governance/architecture/cov-technology-roadmaps/ for more information. The Supplier shall generate and maintain technology roadmaps to include Refresh schedule, Software Upgrades, and new technology to ensure Supplier service offerings stay current. Supplier shall perform in accordance with and adhere to the agreed upon roadmaps and schedules.		
R65.	3. For IT solutions and technologies that are not covered within COV Technology Roadmaps, only use versions or models of IT solutions and technologies that are current (N and N-1) and have vendor or equivalent support. Supplier's Systems and Services tool suite use of Versions of Software technologies must be OEM supportable, with deviations from the N or N-1 standard only as approved by VITA in advance. Note 1: "Support", for the purpose of this requirement, is defined as a minimum of having available and deployable security patching for IT software. Note 2: many N and N-1 versions are defined in the COV Technology Roadmaps	Y	
R66.	4. Comply with VITA Rules for all Supplier provided and managed technologies, such as IT solutions and services, as well as everything supporting Supplier provided or managed technologies, IT solutions, and services. This includes processes, IT solutions, technologies devices, personnel, etc.	Y	
	3.1.1 Design / Architecture Requirements		
R67.	*If required by VITA or necessitated by changes to the environment, the Supplier shall:*		
R68.	1. Coordinate all Architecture & Service, design, strategy, and planning activities with MSI, VITA, and VITA Customers (including business units and Project managers).	Y	
R69.	2. Have all new, changes, or updates to IT solutions go through a formal architecture review process (VITA Architecture Review or MSI HARP Process)) coordinated by the MSI. More information on the MSI HARP process is available in the following Environment overview documents:	Y	

	• ***EO Appendix Ia*** *(Architecture Review Charter)* • ***EO Appendix Ib*** *(Enterprise Services Architecture Overview Template)* • ***EO Appendix Ic*** *(New Architecture Review Process)* • ***EO Appendix Id*** *(Service Management Manual (HARP))*		
R70.	3. Have all changes to IT solutions go through the VITA Architecture Review process coordinated by the MSI.	Y	
R71.	4. Document the IT solution using a VITA approved template provided by the MSI or VITA. Besides the template information to be completed, the Documentation shall ensure Documentation is provided for: • Traceability of all Resource Units (RU) to the VARs • A requirements Traceability Matrix of Supplier contract **Exhibit 2.1 (Description – Mainframe Services)**	Y	
R72.	5. Ensure that all new IT solutions and technologies utilized by supplier or provided to COV Customers or Users shall appear on the Supplier's high-level service model diagram. This diagram shall include all technology and service components. Note: This applies to technology components not specific devices (Servers vs. a particular Dell model)	Y	
R73.	6. Ensure that all new and changes to Supplier provided or managed IT solutions and technologies shall be documented at the following three levels within an Architecture Overview Document (AOD). • High-level section (HL) - required to be approved prior to starting the project to build the architecture. • Detailed Design section (DD) - contains the information needed to build or rebuild the system and needs to be completed prior to service going live. It	Y	

	contains not only the system configuration, but also the configurations from any other suppliers that they need to do to bring your system online. • As built (AB) - contains any variances from the Detailed Design and their configurations. It needs to be completed prior to project closeout. Note: The three levels described above may be within separate sections of the same AOD.		
R74.	7. Provide an indication where that component is documented within the Supplier's high-level service model diagram for all Supplier provided or managed IT solutions or technologies.	Y	
R75.	8. Ensure all new and changes to Supplier provided or managed IT solutions and technologies shall go through a formal VITA approved architecture review process utilizing a template for high-level, detail-level, and as-built designs. The designs need to cover the following architectural viewpoints: • Context – describes the relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts) • Functional – describes the system's runtime elements, their responsibilities, interfaces, and primary interactions • Information – describes the way that the architecture stores, manipulates, manages, and distributes information • Concurrency – describes the concurrency structure of the system and maps functional elements to concurrency units to clearly identify the parts of the system that can execute concurrently and how this is coordinated and controlled • Development – describes the architecture that supports the software development process • Deployment – describes the environment into which the system will be deployed and the dependencies that the system has on elements of it	Y	

	• Operational – describes how the system will be operated, administered, and supported when it is running in its production environment.		
R76.	9. Provide design documents that shall also address the following architectural perspectives cut across all the views specified in the above requirement: • Security – the ability of the system to reliably control, monitor, and audit who can perform what actions on which resources and the ability to detect and recover from security breaches • Performance and Scalability – the ability of the system to predictably execute within its mandated performance role and to handle increased processing volumes in the future if required • Availability and Resilience – the ability of the system to be fully or partly operational as and when required and to effectively handle failures that could affect system availability • Accessibility – the ability of the system to be used by people with disabilities • Development Resource – the ability of the system to be designed, built, deployed, and operated within known constraints related to people, budget, time, and materials • Usability – the ease with which people who interact with the system can work effectively • Regulation – the ability of the system to conform to local and international laws, quasi-legal regulations, policies, and other rules and standards • Evolution – the ability to be flexible in the face of the inevitable change that all systems experience after deployment, balanced against the costs of providing such flexibility Reference: Viewpoints, perspectives, and their definitions are from, Software Systems Architecture, 2nd Edition, Nick Rozanski and Eoin Woods	Y	
R77.	10. Provide Architecture that Supports service continuity where required.	Y	
R78.	11. Isolate VITA environments as required to meet VITA Rules.	Y	

R79.	12. Isolate VITA Customer environments as required to meet VITA Rules.	Y	
R80.	13. Provide a configuration which optimizes the solution to meet a high availability outcome of the environment as dictated by required business outcomes.	Y	
R81.	14. Maintain and update the environment and supporting Documentation for their solution's full footprint at least annually. Supplier will continuously leverage new tools and technologies to improve VITA and VITA Customer business processes and performance in accordance with ITISP Governance processes and procedures as defined in the SMM with prior approval obtained by VITA.	Y	
R82.	**3.1.2 Technology Requirements**		
R83.	Supplier Shall		
R84.	1. Use components in solutions whose currency lifecycle phase includes update-level support. Do not use components that do not meet VITA Rules for currency, unless explicitly approved by VITA in advance.	Y	
R85.	2. Ensure the Supplier's System and Services use IT Hardware whose firmware has Update support.	Y	
R86.	3. Use Versions or models that have vendor or equivalent support. Support is defined as a minimum of having available and deployable Security Patching for IT Software.	Y	
R87.	4. Provide Support for heterogeneous platforms in various geographic locations within the Unites States.	Y	
R88.	5. The Supplier of COV Mainframe Services shall only use approved Versions of technologies as agreed by VITA and VITA Customer.	Y	
R89.	**3.1.3 Integration / Interoperability Requirements**		
R90.	*Supplier shall:*		

R91.	1. Ensure the Solution integrates into all System logging with VITA and/or other Service Tower Suppliers.		
R92.	2. Ensure the Solution integrates into all application logging with VITA and/or other Service Tower Suppliers.	Y	
R93.	3. Ensure the Solution complies with COV Event Log Management requirements.	Y	
R94.	4. Ensure the Solution is thoroughly tested for integration and meets VITA requirements.	Y	
R95.	5. Ensure the Solution is thoroughly tested for interoperability and meets VITA requirements.	Y	
R96.	6. Ensure the Solution enables all Services to interact regardless of where and how they are hosted.	Y	
R97.	7. Ensure the Solution Components integrate across all supported form factors, such that they seamlessly interact with each other while leveraging their native capabilities in a way where they do not require additional Configuration or administration.	Y	
R98.	8. Ensure the Solution supports the creation and update of all data types covered by VITA Rules.	Y	
R99.	**3.1.4 Availability/Performance Requirements**	Y	
R100.	The Supplier shall:	Y	
R101.	1. Have defined expected and quarterly measured Mean Time Between Failure (MTBF) metrics for supplier provided and managed IT solutions and technologies	Y	
R102.	2. Ensure that the Supplier's Systems and Services IT Components supporting COV IT services shall have better Availability than the SLAs for the services that consume those components.	Y	

R103.	3. Provide monitoring consistent with Service Level requirements and reporting of System performance, utilization, and efficiency in accordance with the agreed upon procedures	Y	
R104.	4. Establish System tuning and performance processes where necessary and Upgrade and tune Services Infrastructure to meet capacity changes in accordance with the agreed upon procedures.	Y	
R105.	5. Establish and maintain event management mechanisms which apply to the services, as per agreed upon procedures.	Y	
R106.	6. Establish and maintain monitoring Systems for their solutions, which apply to platforms and services.	Y	
R107.	7. Monitor all phases of their solution's Systems performance.	Y	
R108.	8. For all COV IT services, have SLA's or key measures for Availability and performance.	Y	
R109.	9. Provide appropriate real-time and analysis of historical performance data obtained through monitoring of all phases of their solution's Systems performance.	Y	
R110.	**3.1.5 Capacity and Performance Requirements**	Y	
R111.	The Supplier shall:	Y	
R112.	1. Per SMM 4.1.3.6 Capacity Management, perform strategic, tactical, and operational procedures.	Y	
R113.	2. Perform Infrastructure or Platform Upgrades of their solutions to provide effective capacity to meet VITA and VITA customer needs. Coordinate their Projects with VITA, VITA business partners, VITA Customers, Third Party vendors, and other vendors as appropriate to manage Infrastructure capacity.	Y	

R114.	3. Per SMM 4.1.6.3 Service Measurement, perform activities required for optimizing performance of their solutions to reduce costs.	Y	
R115.	4. Identify estimated bandwidth usage per Application. In addition to requirements stipulated in SMM's, the following shall be maintained in the Archer application for each Solution Application • Number of average concurrent Users on the Application (concurrent is defined as Users transmitting or receiving application data at the same time) • Amount of bandwidth required for each concurrent User • Amount of total Users for each Application • Number of concurrent Users during highest Application usage (i.e., visitors during tax season, hurricanes, document submissions, etc. • The Application throughput estimate (how much network traffic can be processed at once)	Y	
R116.	**3.1.6 Continuity Requirements**	Y	
R117.	The Supplier shall:	Y	
R118.	1. Support service continuity in accordance with SMM 4.1.3.5 IT Service Continuity Management.	Y	
R119.	2. Recommend service recovery point objectives (RPO) and recovery time objectives (RTO) for their services, on demand, for VITA to review and approve.	Y	
R120.	3. Design, configure and deploy, either supplier provided or managed IT solutions and technologies, which meet VITA defined service recovery point objectives (RPO) and recovery time objectives (RTO).	Y	
R121.	4. Ensure the Systems and Services meet defined service Recovery Time Objectives (RTO) as stipulated by agencies and/or Customers.	Y	

R122.	5. Test and determine that all their services are free of defects and compliant with VITA Rules.	Y	
R123.	6. Ensure that any vendors and VITA Customer approved maintenance providers used by the supplier, properly maintain all Hardware and Software.	Y	
R124.	7. Have a Technical Recovery Guide for all of its Application Components and Configurations.	Y	
R125.	8. Comply with the Virginia Public Records Act, Code of Virginia 42.1-76-42.1-91, which requires uniform management and preservation of public records in Commonwealth government agencies.	Y	
R126.	9. Consider and address the Impact on Commonwealth Data of both System outages and data corruption in meeting established RPOs.	Y	
R127.	10. Comply with COV ESA Data Availability requirements for all Commonwealth Data.	Y	
R128.	11. Ensure that the additional sites used for data replication and backup provide geo-diversity, including: • Data locations should be at least 400 miles away from each other • Data locations should be where the risk of natural disasters is acceptable to the COV. Natural disasters include but are not limited to forest fires, lightning storms, tornadoes, hurricanes, earthquakes and floods. Additionally, the Site needs to be located within the continental United States. • Data locations should be in an area where the possibility of man-made disaster is low. Man-made disasters include but are not limited to plane crashes, riots, explosions, and fires. The Site should not be adjacent to airports, prisons, freeways, stadiums, refineries, pipelines, tank farms.	Y	
R129.	12. Ensure the Systems and Services do not rely solely on replication as a technique to address data corruption.	Y	

R130.	13. Provide Customers the ability to perform backups and restores of their Commonwealth Data.	Y	
R131.	14. Test for data corruption and notify the Customer when corruption occurs.	Y	
R132.	**4.0 Security Requirements**		
R133.	**4.1 General Security Requirements**		
R134.	*Supplier shall:*		
R135.	1. Ensure the Supplier's Systems and Services will comply with Commonwealth security policies and standards and all Customers' individual Information Security Policies and applicable Federal standards (e.g., FedRAMP CJIS, FISMA,PCI, ISO27001, FERPA, FTI (IRS PUB-1075), SSA, HIPAA-HITECH).	Y	
R136.	2. Provide informed advice on Security policy, standards (including national security, international, customer and industry standards), practices, solutions and technologies, and threats.	Y	
R137.	3. Implement Security management processes, procedures and controls with other Integrated Suppliers to address interdependencies, use of tools and workflows required to operate integrated Security Management across the Services. Note: Due to the nature of the Mainframe Services and dependent upon the solution proposed, many of these processes may be focused on cooperation within the managed environment.	Y	
R138.	4. In the event VITA determines the Supplier's Systems and Services (or any third-party Software included therein), falls under the Commonwealth's Enterprise Cloud Oversight Services (ECOS) process, then the Supplier may be required to submit one or more ECOS assessments during the procurement solution reviews, and post implementation.	Y	

R139.	5. Implement Security management processes, procedures and controls with other Integrated Suppliers to address interdependencies, use of tools and workflows required to operate integrated Security Management across the Services.	Y	
R140.	6. Ensure the Supplier's Systems and Services is supported and maintained by US Citizens or those legally allowed to work in the US.	Y	
R141.	7. Ensure the Supplier's Systems and Services does not allow for commingling of Commonwealth data with non-Commonwealth data and data is reserved for the exclusive use of the Commonwealth.	Y	
R142.	8. Ensure all User activity and System administration activity is logged.	Y	
R143.	9. Ensure all logged Events are provided to the VITA Managed Security Service Provider SIEM, or subsequent replacement tool for analysis in a VITA approved format utilizing a VITA approved automated method.	Y	
R144.	10. Ensure that all Commonwealth Data remains in the United States and all Sensitive Data remains encrypted at rest and while in transit.	Y	
R145.	11. Ensure that the Commonwealth retains exclusive control and ownership of all encryption keys used in the solution, unless approved by VITA .	Y	
R146.	12. Ensure that encryption will allow for Time-based revocation of access/encryption keys based on the schedule defined by VITA and VITA Customers.	Y	
R147.	13. Ensure that Encryption will allow for User-based revocation of access/encryption keys.	Y	
R148.	14. Ensure that all data associated with the Supplier's Systems and Services is encrypted in transit between services and Systems.	Y	
R149.	15. Ensure that all encryption mechanisms in use by the Supplier's Systems and Services is compliant, at a minimum, with FIPS 140-3.	Y	

R150.	16. Establish and maintain mechanisms to ensure compliance with COV Data Security Standards, and safeguard against the unauthorized access, destruction, loss or alteration of Customer's data. Additional data security requirements may apply based on the sensitivity of data and State and Federal law.	Y	
R151.	17. Utilize controls and processes such that the Services are compliant with all VITA Rules for the processing, storage and transmission of information based on its sensitivity, protected status, classification and impact categorization and ensure that Customers are able to gain assurance and evidence that such compliance is being maintained upon request.	Y	
R152.	18. Disable or delete accounts in accordance with VITA Rules for standard expiration (e.g., 30 days without use) or promptly as requested.	Y	
R153.	19. Install, update, operate, and maintain malware prevention, unauthorized code prevention, Intrusion Detection System (IDS)/Intrusion Prevention System (/IPS, Phishing, Spamming, and denial of service Software and tools as applicable to comply with VITA Rules or Customer-specific rules and in accordance with industry best practices on all Equipment used to deliver or support the Services.	Y	
R154.	20. Maintain functional access to tools that can proactively announce vulnerability, Patch, and pattern Updates.	Y	
R155.	21. Install available Updates, in accordance with Change Management, to malicious-prevention Software and services as needed or as directed by VITA, within the timeframes specified by relevant Third Parties, vendors, or industry experts – except as otherwise approved by VITA.	Y	
R156.	22. Ensure that Supplier's Systems and Services will log all access attempts (successful or not successful) by an administrative User or by personnel supporting the solution from any service provider associated with the Supplier's Systems and Services and that the logs are automatically forwarded to the VITA Managed Security Services Provider or SIEM (per VITA direction) for analysis.	Y	

R157.	23. Ensure that Supplier's Systems and Services will log all actions taken by an administrative User or by personnel supporting the Supplier's Systems and Services from any service provider associated with the Supplier's Systems and Services and that the logs are automatically forwarded to the VITA Managed Security Services Provider for analysis.	Y	
R158.	24. Ensure that no personnel supporting or administrating the Supplier's Systems and Services can alter or delete any log associated with the support or operation of the Supplier's Systems and Services.	Y	
R159.	25. Ensure that no personnel supporting or administrating the Supplier's Systems and Services can alter or stop any logging service associated with the support or operation of the Supplier's Systems and Services.	Y	
R160.	26. Ensure that any service migration between platforms will ensure zero residual data on the originating platform once the Service is migrated and provide evidence of data removal in accordance with VITA Rules.	Y	
R161.	27. Ensure that all Supplier Personnel and the personnel working for a sub-contractor pass the VITA mandated security background check process.	Y	
R162.	28. Create, implement, and continuously maintain Security Baseline Configuration Standards that comply with VITA Rules, VITA approved hardening guides, the SMM, or as defined by specific Customer security requirements.	Y	
R163.	**4.1.1 Security Incident Response Requirements**		
R164.	*Supplier shall:*		
R165.	1. Maintain a Security Incident Response team equipped to respond to Security Incidents or emerging security requirements (which may arise as a result of changing security standards, threats or industry practices) in conformance with the requirements of this Agreement, VITA Rules, and agreed upon procedures. Supplier shall describe its Security Incident Response approach in its proposal.	Y	

R166.	2. Participate in the Security Incident response process as defined in SMM 4.1.5.7 and required by VITA and its Customers .	Y	
R167.	3. Submit and receive approval for a Security Incident Response Plan for the Supplier's Systems and Services from VITA on an annual basis.	Y	
R168.	4. Provide input into the Integrated Incident Response Plan used to conduct Security Incident response as required by VITA Rules.	Y	
R169.	5. Respond to and Resolve malware, unauthorized content, hacking, phishing, denial of service, and other Incidents as defined by VITA and the MSS. Upon detection of malware or unauthorized content, immediately notify VITA and the affected Customers.	Y	
R170.	6. Once the Incident is declared, work with the MSS, and VITA (and its designees) to assess the scope of damage.	Y	
R171.	7. Report status of the Security Incident and mitigation activities to VITA once every 24-hours or more frequently as required by the agreed procedures or VITA until the Incident is Resolved.	Y	
R172.	8. Arrest the spread and progressive damage from malware or unauthorized code in accordance with the VITA approved Incident response plan.	Y	
R173.	9. Eradicate malware or unauthorized code in accordance with the VITA approved Incident response plan.	Y	
R174.	10. Restore all data and software to its last-known operational state in accordance with the VITA approved Incident response plan.	Y	
R175.	1. Provide proactive alerts to VITA or Customers as appropriate relative to current code threats either specific to VITA’s environment, encountered in Supplier’s environment, or based on industry information.	Y	

R176.	2. Provide Mainframe Services information security expertise in the event of a major Security Incident so VITA's and Customers' performance does not degrade because of an unavailability of Supplier resources.	Y	
R177.	3. Respond to Security Incidents or emerging Security requirements (which may arise as a result of changing Security standards, threats or industry practices) under direction from Customers.	Y	
R178.	4. Provide data feeds or Reports to VITA's Security Incident and Event Management (SIEM) systems for purposes of data analytics in accordance with VITA Rules and support VITA's analysis as requested.	Y	
R179.	**4.1.2 Security Integration**		
R180.	*Supplier shall:*		
R181.	1. Submit and receive approval from VITA of a System Security Plan in accordance with VITA Rules.	Y	
R182.	2. Provide reporting to VITA and VITA Customers that highlights emerging threats and the status of known risks in accordance with VITA Rules.	Y	
R183.	3. Initiate Corrective Actions in respect of any potential or actual Security issues or noncompliance with the procedures in accordance with VITA Rules.	Y	
R184.	4. Participate in the integrated compliance and Security Management service performance plans and Reports for all Service Security requirements to meet VITA and VITA Customer's informational reporting requirements and Service Levels in a regular and timely manner.	Y	
R185.	5. Integrate with Managed Security Supplier via the MSI, or as otherwise directed by VITA, to Support Managed Security Services Platform toolset on the Services.	Y	

R186.	6. Install, operate, Configure, Support, and manage Security related toolset (e.g., ACF2) in support of the Managed Security Services Platform toolset in accordance VITA Rules.	Y	
R187.	7. Monitor the environment to detect and prevent Intrusions in accordance with the VITA Rules.	Y	
R188.	8. Communicate and report any intrusion detected in the environment in accordance with agreed procedures.	Y	
R189.	9. Supplier's Systems and Services will ensure all Events required by VITA Rules be logged and forwarded to the MSS SIEM for review and analysis.	Y	
R190.	10. Supplier's Systems and Services will provide integration with all required VITA and MSS security tools (SFTP, SIEM, etc.).	Y	
R191.	**4.1.3 Audit and Compliance**		
R192.	*Supplier shall:*		
R193.	1. Provide the non-redacted SOC 1 audit reports to VITA and VITA Customers at least once every 12-months.	Y	
R194.	2. Provide the non-redacted SOC 2, Type 2 audit reports to VITA and VITA Customers at least once every 12-months.	Y	
R195.	3. Provide quarterly status updates to Commonwealth Security on remediation steps taken for SOC1 and SOC2 Exceptions.	Y	
R196.	4. Cooperate with VITA, VITA Customers, and Integrated Suppliers on audits involving any of those parties that relate to the Mainframe Services. Supplier shall cooperate and provide information as required on both ad hoc and recurring schedules as communicated by VITA or its designee. Examples of such audits include but are not limited to: Federal Tax Information (FTI) audits and Social Security Administration (SSA) audits, Heath Insurance Portability and Accountability Act (HIPAA) audits,	Y	

	Health Information Technology for Economic and Clinical Health Act (HITECH) audits, Family Education Rights and Privacy Act (FERPA) audits, etc.		
R197.	**4.1.4 User Authentication**		
R198.	*Supplier responsibilities include:*		
R199.	1. Ensure that Supplier's Systems and Services will provide secure sign-on Functionality. Supplier should describe its proposed sign on functionality.	Y	
R200.	2. Ensure that Supplier's Systems and Services authentication process will integrate into COV Directory Service.	Y	
R201.	3. Ensure that the Supplier's Systems and Services will federate with the VITA approved single sign-on authority (e.g., OKTA).	Y	
R202.	4. Ensure that the Supplier's Systems and Services will enforce interactive re-authentication at regular intervals as defined by VITA and its Customers.	Y	
R203.	5. Ensure that the Supplier's Systems and Services will log and provide audit Events for all authentication attempts.	Y	
R204.	6. Utilize security clearance and access control processes to administer tools and environments used to support Customer's services for all staff.	Y	
R205.	7. Ensure that access privileges for Supplier Personnel are removed, within 30 days without use, or promptly as requested, when Supplier Personnel cease to require access to the Mainframe Services, such as upon departure the Supplier's employment or transitioning to work exclusively on other accounts, in accordance with VITA Rules.	Y	
R206.	**4.1.5 User Authorization**		
R207.	*Supplier shall:*		

R208.	1. Ensure that any required document Storage authentication or authorization is controlled via a centralized policy setting that can be applied at the Enterprise and Agency level.	Y	
R209.	2. Ensure that the Supplier's Systems and Services will log all User interactions.	Y	
R210.	3. Ensure that all logs are forwarded to the MSS SIEM.	Y	
R211.	4. Ensure that all logs are maintained according to VITA and Customer records retention policy.	Y	
R212.	**4.1.6 Full Disk Encryption**		
R213.	*Supplier shall:*		
R214.	1. Implement full disk encryption as required by VITA Rules and in accordance with the SMM.	Y	
R215.	2. Provide the ability to perform a forensic analysis of the encrypted data.	Y	
R216.	3. Ensure that the Device will be able to be decrypted with the forensic Software to support the forensic analysis.	Y	
R217.	**4.2 Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)**		
R218.	*Supplier shall:*		
R219.	1. Deploy IDS/IPS Systems and monitor alerts from a central logging system, and provide appropriate response to alerts from Systems based upon mutually agreed procedures as defined in the Service Management Manual.	Y	
R220.	2. Install as needed or as directed by VITA or other Customers, updates that address high-risks, as defined by the IDS/IPS systems manufacturer to IDS/IPS System Software within 4 hours or less after such updates are made available to Supplier (or	Y	

	a qualified Third-Party Vendor selected by Supplier) and approved by VITA or VITA Customer.		
R221.	3. Provide centralized logging of all system activity (user access, system modification, data transfer).	Y	
R222.	4. Provide a mechanism to securely transmit logging information to a log collection server or service under VITA's control.	Y	
R223.	5. Coordinate activities with VITA during incidents and provide on-going information security incident reporting during all security incidents.	Y	
R224.	6. Monitor all IDS/IPS Systems from a central logging system and provide appropriate response to alerts from Systems based upon mutually agreed procedures as defined in the Service Management Manual.	Y	
R225.	**4.3 Risk Management**		
R226.	*The goal of Risk Management is to quantify the impact to the business that a loss of Service or asset would have (the Impact), to determine the likelihood of a threat or exploitation of a vulnerability to actually occur, and then to manage activity against the identified risk.*		
R227.	*Supplier shall:*	Y	
R228.	1. Develop, maintain and execute a VITA approved Risk Management program, in accordance with the NIST Risk Management Framework, related to the Services. Including:	Y	
R229.	a) Utilize risk indicators across the Services to monitor risk and assist the detection of emerging trends and control failure.	Y	
R230.	b) Support risk escalation and reporting.	Y	
R231.	c) Address known control weaknesses.	Y	

R232.	d) Deploy and utilize a solution that provides access for VITA and Customers to common risk and controls information, including reports, risk logs, action plans, key controls and risk indicator data.	Y	
R233.	**5.0 Operations**		
R234.	*Supplier shall:*		
R235.	1. Assume responsibility for all master and subordinate console functions.	Y	
R236.	2. Lead and perform system hardware and software upgrades with VITA and other Customers.	Y	
R237.	3.	Y	
R238.	4. Issue commands to control all In-Scope computer platforms throughout the organization.	Y	
R239.	5. Provide automated monitoring and alerting for all in scope platforms.	Y	
R240.	6. Assume the responsibility for and perform all console functions:	Y	
R241.	a) Monitor all processing of all transactions (e.g., batch jobs, applications, utilities, etc.).	Y	
R242.	b) Monitor the environment, alarm systems, environmental controls, the transmission and reception of polling information from outside organizations and take appropriate action to resolve online-system-related Incidents, including escalating (as appropriate) the incidents and/or problems to the proper Level 2 Support group.	Y	
R243.	7. Manage, maintain, monitor, and control the performance of online interactive traffic and take appropriate action to resolve online-system-related Incidents, including escalating (as appropriate) the incidents and/or problems to the proper Level 2 Support group.	Y	

R244.	8. As needed, manage, maintain, monitor, and control the transmission of files to the Mainframe Services, from the Mainframe Services, between VITA and other Customers Sites and any other parties as designated by VITA.	Y	
R245.	9. Provide operational support for data transmission (send/receive), consistent with commercial or VITA and other Customers standards.	Y	
R246.	10. Manage, maintain, monitor, and control online and batch processes, both scheduled and unscheduled (including on-request processing).	Y	
R247.	11. Complete VITA and other Customers defined batch processing and backups in the correct sequence and within the time periods designated by VITA and other Customers.	Y	
R248.	12. Schedule batch jobs within VITA and other Customers defined windows to maintain maximum performance as long as required batch completion times are met.	Y	
R249.	13. Where practicable, provide for automated scheduling of batch and asynchronous task processes including backups.	Y	
R250.	14. On an ongoing basis, enhance processing capabilities and efficiencies through system tuning and other run-time improvements.	Y	
R251.	15. Perform regular monitoring of utilization needs and efficiencies, and report regularly on tuning initiatives.	Y	
R252.	16. Produce trend reports to highlight production issues and establish predetermined action and escalation procedures when batch window issues are encountered.	Y	
R253.	17. Monitor, verify, and make appropriate adjustments to support proper and timely Applications executions.	Y	
R254.	18. Notify VITA and affected other Customers in accordance with the notification procedures in the event that Applications do not execute properly.	Y	

R255.	19. Perform periodic and emergency systems maintenance in accordance with procedures, as documented in the SMM, established to minimize the impact to VITA and other Customers' businesses.	Y	
R256.	20. Perform computer shutdowns and restarts, as required, and execute customary utility functions.	Y	
R257.	21. Maintain, administer, and provide necessary automated tools and processes for systems management to the extent possible in the tool suite jointly agreed by the Parties.	Y	
R258.	22. Maintain tables, calendars, parameters, and definitions for tools used to automate manual procedures or to automate and improve the quality of the operations.	Y	
R259.	23. Provide remote monitoring and management of Mainframes, storage Equipment, and associated peripherals not located at the Supplier-operated Data Center as indicated in **Exhibit 4.6 (Equipment Assets).**	Y	
R260.	24. Maintain and update the documentation for all operations procedures and services, including maintaining accurate information about all Configuration Items (CIs) in the Configuration Management Database (CMDB).	Y	
R261.	25. Provide feedback to VITA and other Customers regarding the impact of potential architecture and design Changes through existing VITA processes.	Y	
R262.	26. Identify opportunities for VITA and other Customers to reduce Equipment and Software costs and/or improve system performance.	Y	
R263.	27. Run or terminate utilities that impact Users with VITA and other Customers approval.	Y	
R264.	28. Proactively monitor and report to VITA and other Customers on resource shortages, and report utilization statistics and trends to VITA and other Customers on a monthly basis.	Y	

R265.	29. Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs.	Y	
R266.	30. Resolve, in accordance with the Incident Management and Service Level requirements, abnormally ended jobs caused by conditions external to production programs.	Y	
R267.	31. Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual (SMM).	Y	
R268.	32. Check job outputs and print queues, and manage job priorities with VITA and other Customers.	Y	
R269.	33. Take printers in and out of service, start the spool and drain printers.	Y	
R270.	34. Define, create, and control all automated operation functions.	Y	
R271.	35. Work closely with the Customer Application Development & Maintenance (ADM) groups from the initial design all the way through and including production processing cycles.	Y	
R272.	**6.0 Production Control and Scheduling**		
R273.	*Supplier shall:*		
R274.	1. Assume responsibility for all production control and scheduling functions as applicable.	Y	
R275.	2. Production control and scheduling staff must be provided 24x7x365.	Y	
R276.	3. Integrate all production control and schedule functions in conformity with VITA and other Customers requirements.	Y	
R277.	4. Establish, document, and maintain standards for production jobs.	Y	
R278.	5. Create and maintain the master scheduling database.	Y	

R279.	6. Identify job dependencies, and create and maintain job and task dependencies on the master scheduling database.	Y	
R280.	7. Develop, distribute, and obtain VITA and other Customers approval of schedules prior to implementation.	Y	
R281.	8. Coordinate and modify schedules for special requests and comply with VITA and other Customers priorities.	Y	
R282.	9. Provide schedule status updates in accordance with the SMM.	Y	
R283.	10. Proactively prepare for User deadlines per customized user requirements.	Y	
R284.	11. Respond expeditiously to requests from VITA and other Customers for priority job execution.	Y	
R285.	12. Promptly notify VITA and other Customers if special requests will affect the timely completion of other tasks.	Y	
R286.	13. Prioritize and schedule batch jobs in accordance with VITA and other Customers schedule parameters, and report distribution to optimize the use of processing windows and the scheduled availability of online Applications that are dependent on batch processing, while verifying that batch completion times are met.	Y	
R287.	14. Take any other necessary steps to prepare Application job streams and scripts for production scheduling and execution.	Y	
R288.	15. Enter program control specifications (parameters) into Application job streams as directed by Users and Administrative Users.	Y	
R289.	16. Maintain system job streams and scripts, including indicating file usages, job dependencies/priorities, and program options available.	Y	
R290.	17. Monitor all jobs including jobs that are scheduled and adhoc requested jobs.	Y	

R291.	18. Promptly notify VITA and Applicable Customer of scheduling impacts due to any scheduled or unscheduled outages and processing delays.	Y	
R292.	19. Start jobs manually where automated processes do not exist or are not available.	Y	
R293.	20. Investigate and report, in accordance with VITA and other Customers approved documentation, on all jobs that end or perform abnormally.	Y	
R294.	21. Resolve interruptions caused by conditions external to production programs, not limited to, but including disk or tape issues.	Y	
R295.	22. Execute re-runs as requested by VITA and other Customers, and restart jobs, tasks and scripts according to Supplier-developed operational procedures (for example, procedures for successful back-outs, etc.).	Y	
R296.	23. Contact ADM staff, other technical staff, and/or Third Parties as necessary during off-hours and work with them on Level 2 Support and Level 3 Support issues.	Y	
R297.	24. Create Incident reports for job abnormalities using the Incident Management System, as described in **Exhibit 2.2 (Description of Service - Cross Functional).**	Y	
R298.	**7.0 Technical Support**		
R299.	*Supplier shall:*		
R300.	1. Provide all technical system support and reporting for operations including:	Y	
R301.	a) Storage management	Y	
R302.	b) System programming and management	Y	
R303.	c) Capacity planning and management	Y	
R304.	d) Performance tuning and management	Y	
R305.	e) Account management and provisioning	Y	

R306.	f) Interface management (data transfer)	Y	
R307.	g) Supplier performs billing record pre-processing on the Mainframe and provides supplier billing records and Customer chargeback records in support of IT Financial Management (ITFM) to the MSI for Supplier and Customer chargeback reporting. . Note: Supplier will be provided with the current pre-processing mainframe jobs during implementation. Supplier is responsible for making any and all adjustments required to the existing pre-processing jobs, and creating new jobs necessary to ensure the Supplier meets requirements in this Agreement. Adjustments made are considered Work Product.	Y	
R308.	2. Install, test, and maintain all System Software in accordance with VITA change management policies and procedures.	Y	
R309.	3. Provide regular monitoring and reporting of system performance, utilization, and efficiency.	Y	
R310.	4. Provide read only access to all monitoring tools and outputs to VITA and other Customers where possible.	Y	
R311.	5. Provide technical advice and support to the Application Development and Maintenance staffs as required by VITA and other Customers.	Y	
R312.	**7.1 General Technical Support**		
R313.	*Supplier shall:*		
R314.	1. Provide comprehensive (i.e., end to end responsibility) response to Incidents and Problems and continued support through resolution in order to meet scheduled availability.	Y	
R315.	2. Provide Level 2 Support and Level 3 Support to the Service Desk and/or Users and Administrative Users.	Y	

R316.	3. Provide technical advice and support, to include OEM input, to VITA and other Customers Application Development & Maintenance (ADM) and Database Administration (DBA) staffs as required.	Y	
R317.	4. Interface between the groups implementing Changes in accordance with the Change Management processes as defined in the SMM and described in **Exhibit 2.2 (Description of Services - Cross Functional)**	Y	
R318.	5. Monitor data storage and processor utilization and requirements.	Y	
R319.	6. Enforce documentation standards in compliance with Service Management Manual directives.	Y	
R320.	7. Develop, where appropriate, and install productivity tools/utilities, as well as performing all required operational modifications for the efficient and proper delivery of the Services.	Y	
R321.	8. Develop and maintain technical and functional Specifications and requirements for all environments and related interfaces, such that all Customer requirements established by VITA and other Customers are met.	Y	
R322.	9. Provide product research, project support, and advice on Equipment tuning and efficiency improvements.	Y	
R323.	10. Install, configure, maintain, and provide ongoing support for System Software products.	Y	
R324.	11. Install and support Software, as approved by VITA and Customers through processes, including the RFS process, defined in this contract and SMM, according to the Applications' specifications and/or VITA and other Customers standards.	Y	
R325.	12. Manage, prioritize, and coordinate all preventive and remedial maintenance and updates for System Software in accordance with VITA and other Customers approval.	Y	

R326.	13. As defined in the SMM, review all Software migration or conversion plans with VITA and other Customers for approval.	Y	
R327.	14. Report performance data and resource utilization statistics related to System Software release-level upgrades.	Y	
R328.	15. Provide consultation support, to include OEM input, as VITA reasonably requests (for example, product research, project support, Applications tuning and efficiency improvements).	Y	
R329.	16. Interface and integrate with the STS designated by VITA for the administration and implementation of Address Management (e.g., IP) needed for Services.	Y	
R330.	**7.2 Capacity and Performance Management**		
R331.	*Supplier shall:*		
R332.	1. The Supplier is required to assist VITA and other Customers in understanding the future business requirements, the organization's operation, and the IT infrastructure, as well as to provide all current and future capacity and performance aspects of the business requirements in a cost-effective manner.	Y	
R333.	2. Perform activities required for monitoring and optimizing performance in order to reduce costs or improve Service Levels.	Y	
R334.	3. Provide performance monitoring, tuning, and reporting.	Y	
R335.	4. Provide monitoring of OS for current capacity utilization.	Y	
R336.	5. Provide systems performance reviews and advice.	Y	
R337.	6. Assist 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 phases.	Y	

R338.	7. Conduct system performance testing and provide test results reporting to VITA and other Customers.	Y	
R339.	8. Using best practices and OEM recommendations configure partitions (LPARS) as requested by the VITA and other Customers.	Y	
R340.	9. Perform upgrades as required to provide effective capacity to maintain or improve consistent performance characteristics, and to meet Software architectural requirements.	Y	
R341.	10. Coordinate with Third Party Vendors, other Suppliers, VITA, and VITA Customers as appropriate on projects to install/upgrade hardware and software, including but not limited to CPU and storage devices.	Y	
R342.	11. Maintain and make available current, comprehensive, and complete: channel, DASD, network, server, and total system topography documentation to VITA and other Customers.	Y	
R343.	**7.3 Configuration Planning**		
R344.	*Supplier shall:*		
R345.	1. Manage and install hardware Input/Output Configuration Program (IOCP) definitions.	Y	
R346.	**8.0 Database Support and Management**		
R347.	*Supplier shall:*		
R348.	1. Plan for changes in the size of databases that result from business growth or reduction, and project implementation based on information supplied by VITA or other Customers, and review plans with VITA or other Customers on a regular basis for VITA or other Customers comment and approval.	Y	

R349.	2. Maintain, operate, and upgrade automated monitoring tools to monitor database performance. Upgrades are to be in accordance with Software Currency for Mainframe Software noted in **Exhibit 4.3 (Financial Responsibilities Matrix)**.	Y	
R350.	3. Perform database version upgrades when requested by Customers.	Y	
R351.	4. Perform database shutdowns and restarts as necessary in accordance with the Change Management processes and as documented in the SMM.	Y	
R352.	5. Maintain the databases, as directed by VITA and other Customers, to meet performance standards, to maximize efficiency, and to minimize Outages.	Y	
R353.	6. Maintain active logs at an agreed upon duration with Customer(s).	Y	
R354.	7. Maintain, update, and implement database archive tools, processes and procedures to maintain the integrity of the database and recover from an Outage or corruption in a timely manner in order to meet VITA and other Customers' business requirements.	Y	
R355.	8. Provide physical database management support, including providing backups and restores of data in a timely manner (e.g., point in time and full forward recovery for all databases with VITA and other Customers, read access to all log files and SMF data pertaining to VITA and other Customers).	Y	
R356.	9. Install, maintain, and support database Software products.	Y	
R357.	10. Test and implement database Environment Changes, as approved by VITA and other Customers.	Y	
R358.	11. Monitor database capacity and proactively provide capacity planning to prevent situations caused by lack of capacity (for example, dataset or table space capacity events, full log files, etc.) in coordination with VITA and other Customers.	Y	
R359.	12. In the event of unusual activity (e.g., resource intensive queries):	Y	

R360.	a) Correct situations caused by lack of capacity in a timely manner (for example, dataset or table space capacity events, full log files, etc.)	Y	
R361.	b) Assist the VITA and other Customers in analyzing and recommending improvements to prevent future occurrences.	Y	
R362.	**8.1 Database Administrative Support**		
R363.	*Supplier shall:*		
R364.	1. Employ database performance analysis to confirm physical database requirements in support of VITA and other Customers business systems.	Y	
R365.	2. Provide VITA and other Customers or its designees with documentation of files generated by the file management systems, including name, utilization statistics, and owning Applications.	Y	
R366.	3. Provide technical advice to the ADM and DBA groups and assist ADM groups in performance stress testing and operating system and database performance tuning.	Y	
R367.	4. Develop, document, and maintain physical database standards and procedures.	Y	
R368.	5. Participate in evaluating physical database changes; Implement necessary changes, recognizing system and network impact to relevant databases, subject to VITA Customer's review and approval.	Y	
R369.	6. Perform quarterly audits of #5 above (R315) jointly with VITA Customer counterpart and provide audit artifacts to VITA and VITA Customers to ensure compliance.	Y	
R370.	**9.0 Online Storage and Backup Management**		
R371.	**9.1 Storage and Backup Architecture**		
R372.	*Supplier shall:*		

R373.	1. Provide Storage and Backup infrastructure that satisfies the needs of all aspects of VITA and the other Customers.	Y	
R374.	2. Remain current in the knowledge and use of data storage technology and management products.	Y	
R375.	3. Coordinate all aspects of Storage and Backup based architecture, design, planning, and implementation within VITA and other Customers organization.	Y	
R376.	**9.2 Engineering**		
R377.	*Supplier shall:*		
R378.	1. Provide in-depth analysis of operations data environment on behalf of availability management, for example, to assist in service outage investigations.	Y	
R379.	2. Identify opportunities for continual improvement, through knowledge management and constant skill review.	Y	
R380.	3. Provide a robust and highly available Storage and Backup infrastructure.	Y	
R381.	4. Plan for changes in capacity requirements.	Y	
R382.	5. Schedule, lead and conduct disaster recovery tests. Supplier is to lead and perform the on-going disaster recovery plan management, maintenance, scheduling and testing so as to return the Services to a working state within Customer's recovery objectives.	Y	
R383.	6. Establish and maintain automated alerting mechanisms and monitoring systems.	Y	
R384.	7. Perform testing and benchmarking of new infrastructure or tools prior to deployment into production.	Y	
R385.	8. Implement performance and configuration tuning of the Storage and Backup infrastructure in conjunction with Capacity Management and Change Management.	Y	

R386.	9. Establish system tuning and performance programs and processes where necessary.	Y	
R387.	10. Provide appropriate security measures for the Storage and Backup infrastructure.	Y	
R388.	**9.3 Operations and Processing**		
R389.	*Supplier shall:*		
R390.	1. Remain current in the knowledge and use of data storage technology and management products.	Y	
R391.	2. Provide event, warning, alert, and alarm processing and management.	Y	
R392.	3. Provide resolution of all event, warning, alert, and alarm messages.	Y	
R393.	4. Provide Storage and Backup infrastructure configuration maintenance.	Y	
R394.	5. Assign and initialize online storage capacity as required.	Y	
R395.	6. Manage the archiving of inactive files and report on online storage directories for review by Mainframe operations and DBA staff.	Y	
R396.	7. Conduct monthly routine monitoring using Software tools to measure the efficiency of online storage access, and take corrective action as needed (including performance adjustments to Equipment and Software, or file placement as required and approved by Customers to improve service).	Y	
R397.	**9.4 Administration**		
R398.	*Supplier shall:*		
R399.	1. Manage online storage thresholds and data archives.	Y	
R400.	2. Monitor user directories for file inactivity and reporting monthly to VITA and other Customers.	Y	
R401.	3. Monitor and maintain file directories and catalogs.	Y	

R402.	4. Provide online storage compaction as needed and as possible within production processing schedules.	Y	
R403.	5. Provide data migration/archive management.	Y	
R404.	6. Monitoring data replication (synchronous and asynchronous) over the infrastructure	Y	
R405.	7. Perform quarterly audits of backup results jointly with VITA counterpart and provide audit artifacts to the VITA Customer	Y	
R406.	**10.0 User Support**		
R407.	*Supplier shall:*		
R408.	1. Provide support, advice, and assistance to Users and Administrative Users in a manner consistent with current practices.	Y	
R409.	2. Implement job control and parameter changes for Users.	Y	
R410.	3. Provide account provisioning in accordance with VITA standards and rules in **Exhibit 2.2 (Description of Service - Cross Functional)**.	Y	
R411.	**11.0Backup and Recovery Services**		
R412.	*Supplier shall:*		
R413.	1. Assume responsibility for VITA and other Customers' system data backup requirements, including:	Y	
R414.	a) Restoring data from the backups	Y	
R415.	2. Perform system data backup and recovery as required and in accordance with VITA and other Customers standards, policies, and Disaster Recovery requirements.	Y	
R416.	3. Perform backups on all defined systems in accordance with VITA and other Customers standards, policies and Disaster Recovery requirements.	Y	

R417.	4. Establish a process by which Users can request recovery of deleted or corrupted files and document the process in the Service Management Manual.	Y	
R418.	5. Report to VITA and Other Customers to validate backup success and processes.	Y	
R419.	**12.0 Middleware Administrative Services**		
R420.	Middleware Administration Services are the activities associated with the maintenance and support of existing and future Middleware specifically for Complete, NATURAL Development Server (Mainframe based), NaturalONE (PC based), Entire X Broker, Control-D/Web Access.		
R421.	*Supplier shall:*		
R422.	1. Manage requirements for users, roles, objects, etc.	Y	
R423.	2. Implement Middleware configurations.	Y	
R424.	3. Create, alter and delete Business Software object changes.	Y	
R425.	4. Establish and maintain configuration and system parameters in a consistent manner across like server environments.	Y	
R426.	5. Execute processes for the proper maintenance and functioning of Middleware systems (e.g., load balancing, tuning, configuration management).	Y	
R427.	6. Execute authorized change requests.	Y	
R428.	7. Execute Middleware installation, upgrade and refresh.	Y	
R429.	8. Execute all Middleware system level changes.	Y	
R430.	9. Execute all object changes for all instances.	Y	
R431.	10. Maintain consistent Middleware parameters and system settings across all like instances according to established development to QA to production life cycle.	Y	

R432.	11. Implement and administer appropriate Middleware management tools across all Middleware instances.	Y	
R433.	12. Patch Middleware software as needed according to established development to QA to production life cycle. Correlate internal change request to vendor tracking codes.	Y	
R434.	13. Provide Middleware communication software configuration, installation, and maintenance.	Y	
R435.	**13.0 Systems Network Architecture (SNA) and TCP/IP Technical Support**		
R436.	*Supplier shall:*		
R437.	1. Provide logical design and connectivity to VITA and other Customers and external client locations for the SNA and TCP/IP network, including support of all front-end processors and Third-Party Vendor protocol conversion boxes.	Y	
R438.	2. Monitor capacity; implement upgrades; and make SNA and TCP/IP modifications as required for VITA and other Customer projects (for example, building redesigns, department relocations, new office openings, etc.)	Y	
R439.	3. Support all System Software used to provide SNA and TCP/IP services, e.g., VTAM, OpenView, ACF/SSP, ACF/NCP, EP, Netview, Netview Access Services, and TCP/IP.	Y	
R440.	4. Establish standards for supported technologies in accordance with VITA Rules.	Y	
R441.	5. Design and maintain SNA configuration, including connectivity to Sites and other sites, as needed.	Y	
R442.	6. Participate in projects that involve or impact the supported technologies.	Y	
R443.	7. Coordinate with LAN and WAN groups and/or other Third-Party Vendors as required.	Y	

14.0 Service Management Manual (SMM) Responsibilities Table

This **SMM Responsibilities Table** sets forth the library of documents shared among the STSs and used within VITA's managed environment. All Suppliers will operate in accordance with and be subject to the terms therein. Suppliers shall reference **(MSA Mainframe Services), section 1.4.2 (Service Management Manual)** for additional information regarding the SMMs.

The contents of this table outline the Service Management Manual (SMM) and the responsibility of the Supplier. The SMMs are broken up into three (3) categories.

- Adhere: Suppliers shall conform and adhere to these SMMs in order to operate within VITA's managed environment. Note: Suppliers may request all "Adhere" SMMs from the Single Point of Contact for this RFP.
- Inform: These SMMs are for informational purposes. Suppliers may need to interface with other Suppliers and need to be aware of their contents.
- Create and Maintain: Suppliers shall create and maintain SMM documentation to align to the section topic prior to the Commencement date. Suppliers shall be responsible for updating their submitted SMMs upon changes.

Instructions: Supplier should enter a "Y" (Yes) or "N" (No) in "Comply (Y/N)" column to indicate if it complies with the SMM as written. Where a cell is shaded under the "Comply (Y/N)" column, no response is required. If Supplier does not comply with an "Adhere" SMM exactly as written, Supplier must enter an "N" in the "Comply (Y/N)" and provide Supplier's proposed changes to the SMM by utilizing the table provided in **Exhibit 2.3.1 (Solution Mainframe Services)**. Supplier should make proposed changes to text using "revisions" or some other method to clearly indicate changes to original text. Supplier should provide information to describe any deviations from the process for any SMMs marked "Adhere."

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
1	SMM Contents				
1.1	Purpose	X			Y
1.2	SMM Document Management	X			Y
2	Organization, Governance, and Contact Information		X		
2.1	WMM Case Management	X			Y
2.2.5	Governance				
2.2.5.1	PAG Charter	X			Y
2.2.5.2	Technical Review Board Charter	X			Y

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
2.2.5.3	Change Advisory Board Charter	X			Y
2.2.5.4	Platform Service Delivery Forum Charter	X			Y
2.2.5.5	Service Portfolio Life Cycle Management Charter	X			Y
2.2.5.6	Program Management Forum Charter	X			Y
2.2.5.7	Service Integration and Interoperability Forum Charter	X			Y
2.2.5.8	Architecture and Innovation Forum Charter	X			Y
2.2.5.9	IT Financial Management Forum Charter	X			Y
2.2.5.10	Cyber Security Operations Forum Charter	X			Y
2.2.5.11	IT Service Continuity Management Forum Charter	X			Y
2.2.5.13	Customer Operations Meetings Charter	X			Y
2.2.5.13a	Customer Relationship Management Forum Charter	X			Y
2.3+	STS XX Organization				
2.4	STS MF Organization Overview (Peraton)			X	Y
2.6	STS MSS - ATOS Organization		X		
2.7	STS SSDC Organization		X		
2.8	STS Managed Print Xerox Organization Overview Information		X		
2.9	STS EUC Organization Overview		X		
2.1	STS VRZN Organization Overview		X		
2.11	NTT Messaging Services Organization Overview		X		
2.1X	MCS Services Organization Overview		X		
3	Service Tower Supplier Implementation				
3.1	Deliverable Management	X			Y
4	IT Service Lifecycle Processes				
4.1	Common IT Service Lifecycle Processes				
4.1.1.1	Program Management Office	X			Y
4.1.1.2	Project Portfolio Management	X			Y
4.1.1.4	Ongoing Programs	X			Y
4.1.1.6	Resource Management	X			Y

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
4.1.1.8	Program Quality Management	X			Y
4.1.2	Service Strategy	X			Y
4.1.2.1	Strategy Generation and Management	X			Y
4.1.2.2	IT Technology Planning	X			Y
4.1.2.3	Financial Management	X			Y
4.1.2.4	Service Portfolio Management Process	X			Y
4.1.2.5	Demand Management	X			Y
4.1.2.6	Business Relationship Management	X			Y
4.1.3	Service Design	X			Y
4.1.3.1	Solution Design Management	X			Y
4.1.3.2	Service Catalog Management	X			Y
4.1.3.3	Service Level Management	X			Y
4.1.3.4	Availability Management	X			Y
4.1.3.5	IT Service Continuity Management	X			Y
4.1.3.6	Capacity Management	X			Y
4.1.3.7	Security Management	X			Y
4.1.3.8	Risk Management (RSKM) Process	X			Y
4.1.3.9	Supplier Management	X			Y
4.1.4	Service Transition	X			Y
4.1.4.1	Change Management	X			Y
4.1.4.2	Change Evaluation	X			Y
4.1.1.5	PMO Risk and Issue Management	X			Y
4.1.4.3	Release and Deployment Management	X			Y
4.1.4.4	Service Asset and Configuration Management (SACM)	X			Y
4.1.4.5	Knowledge Management	X			Y
4.1.5	Service Operation	X			Y
4.1.5.1	Service Desk Function	X			Y
4.1.5.2	Incident Management	X			Y

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
4.1.5.3	Monitoring and Event Management	X			Y
4.1.5.4	Problem Management	X			Y
4.1.5.5	Service Request Management and Fulfillment Process	X			Y
4.1.5.6	Access Management	X			Y
4.1.5.7	Security Incident Management Process	X			Y
4.1.5.8	Request For Solution and Estimate	X			Y
4.1.6	Continual Improvement	X			Y
4.1.6.1	Service Review and Reporting	X		X	Y
4.1.6.2	Process Evaluation Currency	X			Y
4.1.6.3	Service Measurement	X		X	Y
4.1.6.4	Continual Improvement Plan Process	X			Y
4.1.6.5	Technical Innovation	X			Y
5	Financial Management Processes				
5.1	Common Financial Management Processes				
5.1.1	Invoicing and Chargeback	X			Y
5.1.2	Disputes Process	X			Y
5.1.3	Financial Planning and Forecast	X			Y
5.1.5	Service Level Credits and Earnback	X	Note: (Earnback is Informational)		Y
5.1.6	Cost Savings Opportunity				
5.2+	STS XX ITFM RU Listing				
5.2.1	ITFM MSI RU Listing		X		
5.3	ITFM Mainframe RU Listing			X	Y
5.5	ITFM Managed Security RU Listing		X		
5.6	ITFM End User Services RU Listing		X		
5.7	ITFM Server Storage DC RU Listing		X		
5.8	ITFM Managed Print RU Listing		X		
5.1	ITFM VITA Internal RU Listing		X		
5.11	ITFM Data Network RU Listing		X		

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
5.12	ITFM Messaging-NTT RU Listing		X		
5.1X	ITFM MCS RU Listing		X		
6	Contract Management Processes				
6.1+	Common Contract Management Processes				
6.3	STS Contract Management (Peraton)			X	Y
6.5	STS MSS Contract Management		X		
6.6	STS SSDC Contract Management Information		X		
6.7	STS Xerox Contract Management Information		X		
6.8	STS EUC Contract Information		X		
6.9	STS Contract Management Information VRZN		X		
6.11	Messaging Services Contract Management		X		
6.1X	MCS Contract Management		X		
7	Relationship Management Processes				
7.1	Common Relationship Management Process				
7.1.1	Customer Satisfaction Surveys	X			Y
7.1.3	Third Party Vendors	X			Y
7.1.5	Complaint Handling Process	X			Y
8	Service Tower Supplier Operational Processes				
8.1	Common Service Tower Supplier Operational Processes				
8.1.3	Background Checks and Security Clearance Processes		X		
8.2+	Supplier Specific Processes				
8.2.2	Service Management Systems Support		X		
8.2.3	Security Clearance Tracking		X		
8.3.1.1	Mainframe Backup Process - Copy			X	Y
8.3.1.2	MF Job Request System Process			X	Y
8.3.1.3	Mainframe Access Request Process			X	Y
8.5.1.1	MSS Queue and Ticket Management		X		
8.5.1.2	MSS Security Response Plan		X		

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
8.5.1.3	MSS Security Monitoring Policy		X		
8.5.1.4	MSS Security Incident Response Process		X		
8.5.1.5	MSS Managed Security Services Comm Plan		X		
8.5.1.6	MSS Monitoring and Event Management		X		
8.5.2.1	MSS Managed IDS-IPS		X		
8.5.2.2	MSS Web Content Monitoring Process		X		
8.5.3.4	MSS Managed End-Point Security		X		
8.5.3.5	MSS Managed Firewall Service		X		
8.5.3.6	MSS Vulnerability and Compliance Management		X		
8.5.3.7	MSS Penetration Testing		X		
8.5.3.8	Data Security Process		X		
8.5.5.1	MSS Application and Source Code Security		X		
8.6.1	SSDC Server Provisioning		X		
8.6.2	SSDC Server Operations		X		
8.6.3	SSDC Storage Provisioning		X		
8.6.4	SSDC Storage Operations		X		
8.6.5	SSDC Database Provisioning		X		
8.6.6	SSDC Database Operations		X		
8.6.7	SSDC Enterprise Data Center LAN Provisioning		X		
8.6.8	SSDC Network Operations		X		
8.6.9	SSDC Enterprise Data Center and Facilities Management		X		
8.6.10	SSDC Backup and Recovery		X		
8.6.10	SSDC Backup and Recovery (GCP Review)		X		
8.6.11	SSDC Directory and Identity Management Services		X		
8.8.6	EUC Warehouse-Depot Asset Management		X		
8.6.13	SSDC Monitoring and Event Management		X		
8.6.14	SSDC Batch Management		X		
8.7.3.1	MPS Queue and Ticket Management		X		

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
8.7.3.2	MPS Desk Side Support		X		
8.7.3.3	MPS Asset Disposal Process		X		
8.7.3.4	MPS Consumables Management Process		X		
8.7.3.5	MPS Install Move Add Change Process		X		
8.8.1	EUC Queue and Ticket Management		X		
8.8.2	EUC Desk-Side Support Operations		X		
8.8.3	EUC Asset Recovery and Disposal		X		
8.8.4	EUC PC Refresh		X		
8.8.5	EUC Software Distribution		X		
8.6.12	SSDC Asset Management AND Recovery		X		
8.8.7	EUC Configuration Management Database (CMDB)		X		
8.8.8	EUC Agency-Specific Device		X		
8.8.9	EUC IMACs		X		
8.8.10	EUC Smart Hands		X		
8.8.11	EUC Request for Solution and Project Implementation		X		
8.9.21	VDN Engaging Verizon Subcontractors		X		
8.9.24	VDN Service Desk		X		
8.9.29	VDN Escalation Process		X		
8.9.38	NOC Operational Process		X		
8.9.56	VDN Configuration Management Database (CMDB) Processes		X		
8.9.57	VDN Queue and Ticket Management		X		
8.9.58	VDN Install and MACD (Moves, Adds, Change, De-installs)		X		
8.9.59	VDN Change Management		X		
8.9.60	VDN Request for Solution and Project Implementation		X		
8.9.62	VDN Event Management		X		
8.9.63	VDN Network Engineering		X		
8.9.64	VDN Security Management		X		
8.9.65	VDN Chronic Problem Management		X		

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
8.9.67	VDN Knowledge Management		X		
8.11.1	Messaging Queue and Ticket Management Process		X		
8.11.2	MSG Services Operations and Maintenance		X		
8.11.3	Software License Management		X		
8.11.4	MSG-NTT Data Lifecycle Management Plan		X		
8.1X.1+	MCS Supplier Specific Processes		X		
9	Customer Process and Documents				
9.1	Common Customer Processes				
9.1.2	Customer on-boarding		X		
	For SMM 9.1.2 - Supplier Service Requirements/Criteria			X	Y
9.1.3	Customer off-boarding		X		
	For SMM 9.1.3 - Supplier Service Requirements/Criteria			X	Y
10	Operational Reports - Reserved				
11	Communications				
11.1	Customer Communications Management	X			Y
OLAs	Operating Level Agreements				
	Atos - Iron Bow OLA		X		
	ATOS - Verizon OLA		X		
	Iron Bow - Verizon OLA		X		
	Iron Bow - Unisys OLA		X		
	Iron Bow - Xerox OLA		X		
	MSI - Atos (MSS) OLA		X		
	MSI - Peraton (MF) OLA			X	Y
	MSI - Unisys (SSDC) OLA		X		
	MSI - Xerox MP OLA		X		
	MSI - NTTDATA (MSG) OLA		X		
	MSI - Iron Bow EUC OLA		X		
	MSI - Verizon OLA		X		

Ref #	Requirement	Adhere to Enterprise Level Process	Inform STS how other STSs work	Supplier to Create and Maintain	Comply (Y/N)
	NTTDATA (MSG) - ATOS (MSS) OLA		X		
	NTTDATA (MSG) - IronBow OLA		X		
	NTTDATA (MSG) - MSI OLA		X		
	NTTDATA (MSG) - Unisys (SSDC) OLA		X		
	NTTDATA (MSG) - Verizon (VDN) OLA		X		
	Peraton - ATOS - OLA			X	Y
	Unisys - Peraton OLA			X	Y
	Unisys - Verizon OLA		X		
	Xerox - ATOS OLA		X		
	Xerox - Unisys OLA		X		
	Xerox - Verizon OLA		X		
	MCS - XXXXXX OLA(s)		X		