★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

EXHIBIT F

MAINTENANCE AND SUPPORT (M&S) PLAN

FOR THE VIRGINIA STATEWIDE VOTER REGISTRATION AND ELECTION MANAGEMENT SYSTEM (SVRS)

Table of Contents

Introduction

This Maintenance and Support Plan (M&S Plan) describes the Services and Deliverables the Canton Group will provide related to Warranty Services and Maintenance & Support (M&S) Services of the Statewide Voter Registration System (SVRS).

1.0 Warranty

Warranty Services and M&S Services requirements will be identical except that the Commonwealth will pay an annual fee for these services during the M&S period. During Warranty, the services will be provided at no additional cost to the Commonwealth and will comply with §6 General Warranty, (B) Coverage Period of the Contract,

1.1 Warranty Term and Initiation

The Warranty period for the SVRS will be 60 days from the date the Application goes live.

1.1.1 Third-Party Warranty Terms

The Warranty period for third-party software provided by The Canton Group will be the duration as provided by the third-party manufacturer.

2.0 Maintenance and Support

The Canton Group provides M&S services after completion of the Warranty period. The Commonwealth will pay an annual fee invoiced monthly in arrears for such services as determined in the Contract.

2.1 Plan and Prepare for Maintenance and Support Services

Team members from The Canton Group and the Commonwealth will be introduced, and their specific roles described. The Canton Group will provide training, as required, for the Commonwealth resources related to M&S Services and will introduce its tools, existing M&S-related artifacts, M&S methodologies, and best practices that it will use throughout this M&S Plan.

After successful implementation and preparing for the ongoing M&S services, The Canton Group will follow our best practices for project transitions. This would include spending time working with both the implementation and M&S teams, reinforcing the Agile software methodology approach, reviewing existing documentation, looking through the code, working with the Commonwealth for identification of resources, and developing an agenda and meeting objectives for the M&S services kickoff meeting.

The M&S services kickoff meeting would be attended by all key stakeholders and team members to ensure all members are aligned on the upcoming project goals. During this meeting, there will be a thorough review of a project plan to cover the tasks, deliverables, and milestones for the M&S services. While reviewing the plan, the team and stakeholders would be strongly encouraged to speak up and add, modify, and/or remove tasks to ensure the project plan covers all necessary elements.

Additionally, the meeting would cover the full scope of M&S services including any licensed modules or third-party products, M&S Plan dependencies, and roles and respective responsibilities of both The Canton Group and the Commonwealth. Finally, a preliminary review of the backlog would be done, and the first M&S Quarterly Road Mapping Session would be scheduled.

The focus of this first M&S Quarterly Road Mapping Session would be to review the backlog and determine planned work and priority is still relevant and correct.

After the M&S services kickoff meeting is completed, The Canton Group will prepare and distribute a summary report noting the meeting attendance, notes and observations, areas for improvement and opportunities, challenges, and any action items or outcomes identified as a part of the kickoff meeting.

2.2 Conduct Maintenance and Support Planning

The Canton Group has a robust M&S plan which is based on our Manage Change and Release Management processes. Our team's change management process ensures that changes to the supported software are understood, planned, communicated, and implemented in a controlled and organized manner with minimal impact on operational activities. All M&S services provided by The Canton Group follow our Agile software delivery method including collaboration with the client to determine and refine the backlog and assign priorities based on requirements and timelines, where tasks will follow our development, QA (Quality Assurance), User Acceptance Testing, and demonstrations for approval and deployment.

Our comprehensive M&S services will include as part of the fixed price, the implementation of new releases and software upgrades, defect resolution, and ongoing training for both inexperienced staff orientation and reinforcing training for existing staff. Training would cover new functionality because of SVRS enhancements, releases, and upgrades. Maintenance of the system, documentation, and reporting frequencies and methods are covered as well. The Canton Group's M&S plan provides team roles and responsibilities and ensure the team will follow the model and processes used by our implementation team with interactions with the Commonwealth (including adherence to all applicable Service Level Agreements (SLAs) and requirements as specified in the Contract).

Our M&S team will be staffed with a team of highly skilled resources that are either part of the development and implementation team or personnel that have worked on similar engagements in the past. A critical component for project success is the seamless substitution of qualified personnel. The Canton Group provides rapid substitution of personnel by maintaining a full roster of our own, using efficient and proven recruitment strategies, vetting, selection, and onboarding of talented people. If needed, we can also reassign qualified personnel from other projects as we recruit the right replacement.

Customer satisfaction is of the upmost importance to The Canton Group and as a result, our executive team is committed to engaging as sponsors for this project. Our dedicated effort ensures direct lines of communication remain open should any critical issues arise and allows us to resolve them quickly and effectively.

2.3 Provide Application Management Services

The Canton Group will provide M&S Services per the Contract, including this M&S Plan.

2.3.1 Provide Application Support

Our help desk will provide a single point of ingress for advanced support for the Commonwealth users. The Canton Group works with the Commonwealth to ensure there is a mutual understanding of the tools, processes, and escalation procedures necessary to create a seamless end-user experience for advanced application support.

Under The Canton Group's support model, Level 1 help desk support is provided by the Commonwealth and includes initial triage and primary contact with the end users reporting any problems/incident. Level 2 and 3 support is provided by The Canton Group. Level 2 support consists of expert/super user resources that can provide troubleshooting. Level 2 support attempts to provide a resolution, and if unable to do so the issue is escalated to Level 3. Level 3 support consists of product subject matter experts who are involved in product development. Level 3 support typically addresses problems believed to be related to a code defect. The exhibit below shows the escalation process.

All applications support requests and incidents are logged, tracked, and reported using IT Service Management tool. The Application Support Manager reviews the status with the Commonwealth PM on a weekly basis and provides reports on the same monthly.

The Canton Group will provide both application monitoring and management services. These services include monitoring and managing all licensed software and any third-party products used throughout the system; notifying the Commonwealth Help Desk of any reported issues and relevant next steps; taking any required action, performing, and implementing software updates, and validating software updates and/or application enhancements and fixes; monitoring and managing interface activities; and reviewing and providing feedback to proposed changes to the Commonwealth's integration platform.

The Canton Group provides operations management services including monitoring scheduled jobs, detecting abnormal operational conditions, logging failures and relevant corrective actions, restarting, adding, or removing operations jobs, and documenting and reporting operations jobs and issues.

Performance Standard	SLA #4 - Standard Maintenance Except in cases of emergency, ELECT shall be provided a 2-business day advance notification of such maintenance and/or upgrade.
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of the notifications provided to ELECT for maintenance and/or upgrade performed the previous month.

Delivery Frequency	Monthly

Performance Standard	SLA # 5 - Standard Maintenance Maintenance or upgrades are not to exceed 36 hours in duration in a single month and cannot occur Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. ET
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of the duration, to include length of time/hours, for each maintenance and/or upgrades performed the previous month.
Delivery Frequency	Monthly

2.3.2 Provide Incident / Problem Management and Resolution

The Canton Group will provide incident/problem management and resolution services to include notifying the Commonwealth, assessment of operational impacts, triaging, tracking, escalation, and resolution of all incidents. By following the M&S Plan, SLAs, and any other applicable sections of the Contract, The Canton Group will maintain ownership of all issues through their resolution and closure. We will utilize multiple communications channels (e.g., email, telephone) for incident reporting, escalation, and resolution through a single point of contact to the Commonwealth and the Commonwealth Help Desk. The Canton Group will provide root cause analysis documentation on problems as well as provide on-call staff for any incident and problem management (staff to be available 24x7x365).

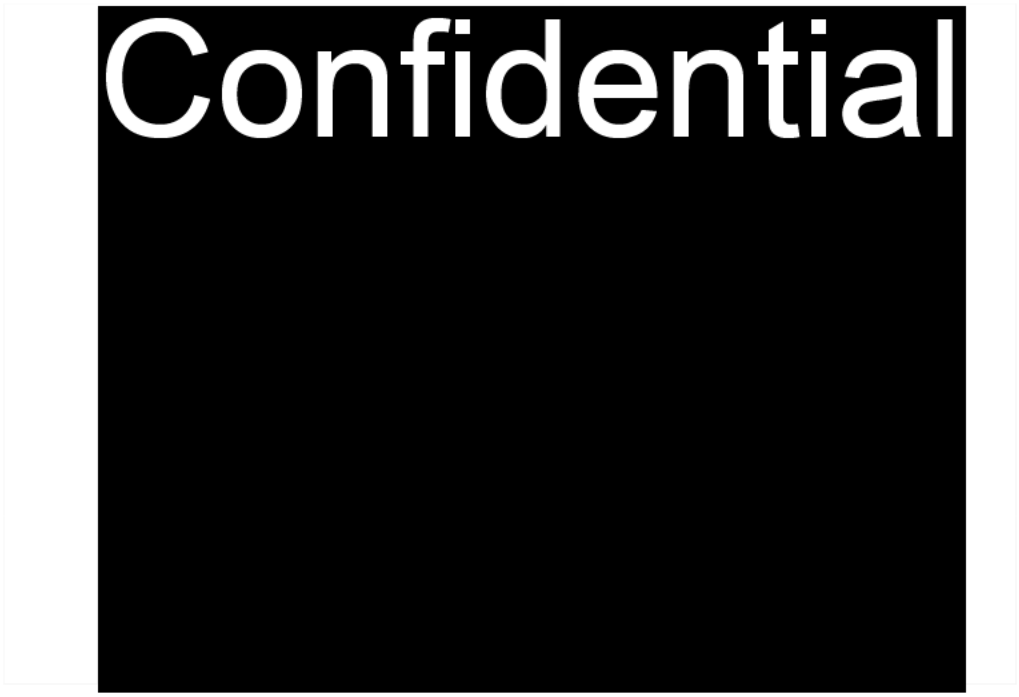
Given our solution's monitoring and logging capabilities, we can easily query metrics and provide accurate and real-time monitoring and reports to meet the incident response requirements of the Commonwealth.

Performance Standard	SLA #3 -Incident Response and Resolution Incident Response and Resolution Time Service Levels will be performed in the time periods set forth in the contract: Respond to problems with the solution identified by ELECT in no more than one (1) hour after notification. i) Priority 1 / Critical (entire location down or security threat or incident) corrected within four(4) hours; ii) Priority 2 / High (critical failure w/ certain processing interrupted or malfunctioning, but system able to process with ELECT approved/ workaround) corrected within thirty-six (36) hours. iii) Priority 3 / Medium (system functioning with minimal impact or malfunction, system able to process data) corrected within two (2) calendar days;

	iv) Priority 4 / Low (minor intermittent malfunctioning, system able to process data) within three (3) calendar days. The level of severity (e.g., 1, 2, 3, etc.), shall be determined by ELECT.
Deliverable	Monthly Incident Response and Resolution Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of all incidents occurring in the previous month.
Delivery Frequency	Monthly

2.3.3 Implement New Releases and Software Upgrades

The Canton Group uses the following structured Release Management Process to manage software changes. As noted, our team follows an Agile software delivery method for our development, testing, and deployment process.



Each stage of this process has its own set of activities.

1. Confidential [redacted]
2. Confidential [redacted]
3. Confidential [redacted]

4. Confidential [redacted]
5. Confidential [redacted]
6. Confidential [redacted]
7. Confidential [redacted]
8. Confidential [redacted]

The Canton Group's approach is based on transparent and open communication as our backlog and product evolves. We will collaborate with the Commonwealth to jointly determine Release and Upgrade schedule and time of implementation. The Canton Group provides up to Confidential [redacted]

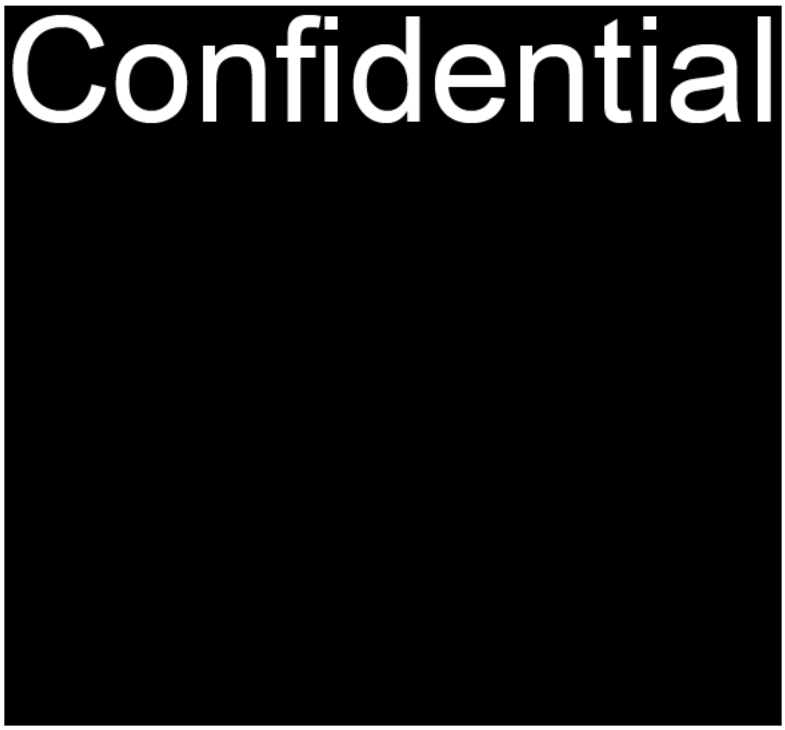
Performance Standard	SLA#7 - Operational Use The associated technical data, code, documentation and other necessary information about such system customizations shall be provided by Supplier to ELECT within5 business days of the customizations' operational use.
Deliverable	Operational Details – within 5 business days of the customization to system being implemented and in operational use, Supplier will deliver to ELECT the system implementation details.
Delivery Frequency	Within 5 business days upon customization to system being Operational

Performance Standard	SLA#10 - Software Modifications and Release Management During the course of the Contract, analyses and cost estimates for ELECT initiated modifications, configuration changes, , and change orders shall be completed by the Supplier at no additional charge and provided in writing to ELECT, within ELECT prescribed timeframes (including turn-around timeframes as short as 72 hours as well as responses on weekends and holidays). During the course of the Contract, analysis and cost estimates for proposed legislative changes, and legislation related change orders shall be completed by the Supplier at no additional charge and provided in writing to ELECT within ELECT prescribed timeframes (including turn-around timeframes as short as 24 hours including weekends and holidays.)

Deliverable	Modifications shall be documented and provided to the Supplier for analyses and cost estimation to be completed in the timeframe prescribed by ELECT.
Delivery Frequency	Per Instance

2.3.4 Provide Application Change Control

The Canton Group's manage change process ensures that changes to the supported software are understood, planned, communicated, and implemented in a controlled and organized manner with minimal impact on operational activities. The following figure shows the core activities.



- Log Change Request: Initiated by Commonwealth staff, or The Canton Group's Application Support Staff. This maybe also be legislatively driven changes. All changes are logged in the backlog by the help desk. The changes may belong to any of the following categories:
    - Corrective: Rectify defects observed while the solution or to enhance the performance of the system.
    - Adaptive: Modifications and updates for the product to run on new platforms, on new operating systems, or when the product needs to interface with new hardware and software.
    - Perfective: Support new features or change different types of functionalities of the system.
- Assess & Approve: After the request is recorded, it is assessed to verify The Canton Group's understanding of all details and analyzes the associated impacts. This involves ensuring the request is legitimate (not already duplicated with another request),

compliant with the scope of the contract, and issued by an authorized end-user, client, or a representative from The Canton Group. The Commonwealth PM approves the change.

- Plan & Schedule: Activities are supported by the Release Management Process.
- Implement: Activities are supported by the Release Management Process.
- Report: Report to the Commonwealth monthly the status of the change requests on the Configuration and Technology Change Report.

Performance Standard	SLA#6 - Standard Maintenance Supplier shall be required to notify ELECT in writing at least sixty (60) prior to of any planned change(s) or Update(s) to the Application; its functionality; Content storage/ backup/disaster recovery, including physical location; security architecture, features or settings; terminations and/or replacement of any Supplier subcontractor when such changes are not routine or minor, or when such changes have the potential to materially impact the secure and efficient use of the Application, as understood and agreed to between Supplier and ELECT at Contract award. The purpose of this notice is to allow sufficient time for Supplier and ELECT to discuss any technical/functional considerations and/or changes that would require action by the Commonwealth e.g. the proposed use of a new cloud provider, which would require an ECOS assessment, or an Update that would require the loss of use of functionality during a primary or election event.
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of the planned change(s) or update(s) to the system performed the previous month, along with the notification date to ELECT.
Delivery Frequency	Monthly

2.3.5 Manage Authorization Controls and Processes

The Canton Group manages access controls to the application. Our solution uses Role Base Access Control (RBAC) for user authorization. Confidential [redacted]

Confidential [redacted]

Confidential [redacted]

Confidential [redacted] These two pieces of information allow for auditability of the requests to the system. These logs are fully exportable and easy to interpret.

The Canton Group will provide a change control process for the creation and modification of user accounts to the Commonwealth for their approval.

Performance Standard	SLA#8 - Access Removal In the event ELECT is unable to remove access authorization of a system user, and requests assistance of supplier, Supplier shall remove access authorization of said system user from its server within one (1) hours of receipt of such notification from an ELECT authorized user.
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of access authorization removals performed the previous month, along with the notification timeline to ELECT.
Delivery Frequency	Monthly

Performance Standard	SLA#9 - Provisioning In the event ELECT is unable to make incremental adds, access authorizations, moves or reductions, including disabled access updates, in the scope of the Licensed Service (e.g., USERIDs), and request assistance of Supplier, Supplier shall complete within one (1) hour of a written request (including e-mail or submission to Supplier's provisioning website) from ELECT.
Deliverable	Monthly Provisioning Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of Provisioning Performed for the previous month.
Delivery Frequency	Monthly

2.4 Provide Hosting Services

2.4.1 Operate Hosting Environment

The Canton Group will provide the Commonwealth with 24x7x365 access to their data via the EMS and hosting services over dedicated and secure internet connections. We will operate both the licensed software and hosting services on a 24x7x365 basis. Our hosting services include providing, monitoring, and maintaining the hardware, software, and communications infrastructure. This includes shared networking and application infrastructure, computer systems, and end-to-end connectivity. We will coordinate with the Maintenance and Support (M&S) team to provide and maintain all applicable licenses and software required to provide the Hosting Services.

As this is a full cloud-based solution, The Canton Group does not anticipate needing to store any company equipment at the Commonwealth's facilities. Our team will provide technical support regarding the installation, maintenance, and troubleshooting of network termination devices. The Canton Group will maintain all necessary environments and when needing to integrate with the Commonwealth's infrastructure, we will provide direction and feedback.

Performance Standard	SLA#1 - Availability "Available" has the meaning set forth in Section 10 of the Contract. Service Levels and Remedies and Reporting for Cloud Services. "Excusable Downtime" has the meaning set forth in section 10 of the contract. Service Levels and Remedies and Reporting for Cloud Services Actual Availability > 99.99% 99.98 – 97% 96.99 – 95% 94.99 – 0%
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of the Actual Availability of the licensed service for the previous month.
Delivery Frequency	Monthly

2.4.2 Maintain Security Services

The Canton Group will maintain security to the application. This will include providing and maintaining virus/malware protection and monitoring for security errors and attempted violations. All security violations will be reported to the Commonwealth. Our security services will comply with all applicable Commonwealth, State, and Federal requirements.

Cloud Security

The Canton Group's solution deploys in Microsoft Azure Government, one of the top Cloud Secure Cloud Services Providers in the world.

Incident Detection

Our Solution uses Azure Firewall, a highly available Firewall that protects the entire solution from external threats. Among other features, the Azure Firewall supports monitoring of incoming and outgoing traffic. We can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. The Azure Firewall Rules enforce and log across subscriptions and virtual networks.

We can detect irregularities such as multiple log-in attempts, above average traffic, large amounts of data transmission with our logs, metrics and monitoring implementation. In addition to that, we recommend enabling Azure diagnostics logging, to allow Azure to notify us of these types of threats as soon as they occur.

Deploying our Solution in Azure also gives us the advantage of getting protection at the infrastructure level, including network and resources. Azure will notify us and tell us what actions we should take in case of attacks. If Azure detects, for example, a distributed denial-of-service (DDOS) attack, it immediately closes the connection to the IP address of the resource where the attack is happening. Fortunately, we do not expose public IP addresses and all the solution resources are private and the only way of entry is via the Firewall.

A typical mitigation plan is to put out of service (turn off) the affected resource, determine if we need to use the Disaster Recovery Site to route the traffic to that system, or maybe we just need to re-instantiate a new resource using our creation scripts. Then forensics process is applied to the affected resource to determine the degree of the attack and what was compromised. We believe that by having only one point of entry to our application, we largely minimize this risk.

Data Encryption

Our solution uses industry standards for data encryption. We encrypt data both at rest and in transit. We encrypt data at rest using Transparent Data Encryption (TDE) within MS SQL Server database. TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key. Our Security Microservice encrypts the passwords using sha512 as specified in FIPS 180-4 and NIST SHS standards (SHA-2 type).

For data in transit, we use a secure channel using security certificates with at least TLS 1.2 to implement HTTPS protocol. We encrypt the data inside the secure channel using FIPS 140-2 encryption mechanism. Non-relational data is persisted in Azure Storage. We encrypt the data in using Azure Storage 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

At the infrastructure level, we take advantage of Azure Government Security services. Data encryption at the server side uses service-managed keys in compliance with FIPS 140.

Vulnerability Scanning

To keep the system as secure as possible, our security policy is to conduct semi-annual third-party penetration tests. We can conduct more frequent scheduled pen tests to meet the Commonwealth's requirements. We also get regular Vulnerability reports from Azure Security Center. These reports show for example patches needed to be applied to our software, versions of software used in the solution that are getting close to their end of support, Database and OS

version updates, etc. We are continually monitoring these reports and we create user stories to fix them in the next sprints or in the current sprint as a hot fix if needed.

Security Monitoring

Confidential [redacted].

Confidential [redacted].

Confidential [redacted]

Confidential [redacted]

We capture not only the history of the events that modified a record, but also who, when, and what was done to that record. This model is very useful and allows us to get answers to questions such as “what happened to Voter ABC after the last election?” and enables us to view the state of the system at any point in time.

We follow the Open Web Application Security Project (OWASP) and other security sources such as Firewall vendor reports. We rely in Azure Government Security Center to monitor ongoing security threat changes. The Azure Security Center reports are continuously (real time) being updated, with an administrator task to review the reports to react to potential threats. The Canton Group will coordinate with different sharing networks including the Sector Coordinating Council of the Elections Infrastructure Subsector (EIS-SSC), the Information Technology Information Sharing & Analysis Center (IT-ISAC), the Election Infrastructure ISAC (EI-ISAC), and others.

Cybersecurity/Threat Identification

The main threats to the solution in Azure Government are DDOS, unauthorized access, and some of the OWASP top 10 application security Risks. Our risk management iterative process involves identification, impact assessment, prioritization analysis, tracking, and mitigation planning implementation and progress management.

Infrastructure and Application Security

All the database IP addresses and all the solution resources (VMS, Containers, VNETS, SUBNETS etc.) are private. As a result, direct network, application, and data level access to databases are restricted. Only an administrator has access to the Production environment. Application users access the application via authentication in the user interface (UI). The database can be accessed directly by the administrator or the application. The application accesses the database only when a request from an authorized user reaches the data services. The data service uses a private connection with the database to execute the user requests. Our logging and journal tables capture – using database triggers – any activity requested to the database, either from the application or from connections external to the application, such as the administrator.

All the database IP addresses and all the Solution resources (VMS, Containers, VNETS, SUBNETS etc.) are private. As a result, direct network level access to databases is restricted. We are protecting our solution using the Firewall, which is the only resource with public IP.

The Canton Group will ensure all security services comply with all applicable County, State, and Federal requirements, and regulations.

Performance Standard	SL#11 - Vulnerabilities Scanning for vulnerabilities is performed every thirty (30) days; vulnerabilities identified by the supplier, ELECT or other third-party, shall be timely remediated.
Deliverable	The Supplier shall remediate legitimate vulnerabilities within thirty (30) days in accordance with SEC 525 Hosted Environment Information Security Standard RA-5 VULNERABILITY SCANNING, unless ELECT provides a written extension prior to expiration of the thirty (30) day period.
Delivery Frequency	Monthly

Performance Standard	SLA#14 - Licensed Services Reporting In addition to the SLA reporting previously mentioned, the following reporting shall be provided by the Supplier: i) Summary of Intrusion Detection and Prevention Scans that demonstrates the Supplier protects ELECT data with intrusion monitoring tools from unauthorized access, modification and deletion.
Deliverable	Quarterly Reporting - on a quarterly basis, by the 5th of the first month of the calendar quarter, Supplier will deliver each report to ELECT, for the previous quarter.
Delivery Frequency	Quarterly

Performance Standard	SLA#13 - Licensed Services Reporting In addition to the SLA reporting previously mentioned, the following reporting shall be provided by the Supplier:

	i) System/Application Patching Compliance Report – a report that illustrates that the supplier has installed security relevant software and firmware updates within 30 days of the release of the updates. ii) Scanning Reports that illustrates vulnerability scanning of Cloud Service Providers Operating System/Infrastructure, databased and web applications.
Deliverable	Monthly Reporting - on a monthly basis, by the 5th of the month, Supplier will deliver each report to ELECT, for the previous month.
Delivery Frequency	Monthly

2.5 Business Continuity and Disaster Recovery

2.5.1 Perform Backups and Restores

The Canton Group's solution is deployed in the Azure Government, and we use Azure Backup managed services for voter and election management databases, as well as application configurations. Once The Canton Group deploys the solution in Azure Management, we turn on the backup services and automatically Azure backs up the database and storage. This solution for built-in backups of Azure provides security to the process and reduces costs by not having infrastructure and management overhead.

Azure backup protects the data from ransomware and only authorized users create critical backups. Azure sends a notification to the administrator in the case of any suspicious activity allowing us to react immediately. If for some reason data is erased, Azure keeps a copy of the backups for up to two weeks so data can be recovered during that period.

2.5.2 Provide Disaster Recovery

Business Continuity and Disaster Recovery (BC/DR) is a very important process we implement in our solution. Confidential [redacted]

Recovery Time Objective (RTO) refers to the duration of time needed to recover the application after a disaster occurs. To meet the 15 minutes or less requirement, the Recovery Site is ready for use anytime (Active-Active DR strategy). Confidential [redacted]

Confidential [redacted].

Performance Standard	SLA #2 - Failover Automatic failover events take place in less than one (1) minute; the failover activities shall complete and the system shall be available to Users within 15 minutes.
Deliverable	Monthly Service Level Performance Report - on a monthly basis, by the 5th of the month, Supplier will deliver to ELECT a report of the failover of the licensed service for the previous month.
Delivery Frequency	Monthly

Performance Standard	SLA #17 - Content Privacy and Security Supplier shall provide a report to confirm the exact geographic location of any Content not stored in a Commonwealth facility monthly.
Deliverable	Monthly Reporting - on a monthly basis, by the 5th day of the month, Supplier will deliver the geographic location of content to ELECT, for the previous month.
Delivery Frequency	Monthly

2.6 Provide Transition Services

The Canton Group develops a written exit plan, as provided in §3(G) of the Contract, ("Transition Out Plan") within six (6) months of execution of the Contract. The plan details each Party's respective tasks for the orderly transition and migration of all Content stored by The Canton Group to ELECT's archive and/or to a system or application maintained by ELECT. The Canton Group maintains the Transition Out Plan, throughout the Term and updates the Transition Out Plan as needed and subject to ELECT's approval.

During the Transition Out period, The Canton Group:

- Returns to ELECT all contents in its possession and stored by the application on behalf of ELECT.
- Provide all assistance as ELECT may reasonably require transitioning the licenses services to any other supplier with whom ELECT contracts to provision the same.
- Continue to provide Licenses Services.

Performance Standard	SLA #15 - Content Privacy and Security Within 30 business days after the expiration or termination of this Contract, Supplier shall confirm in writing to ELECT that all content has been removed from all systems where the Content resided during performance of this Contract in a manner that

	complies with and/or exceeds the Commonwealth Data Removal standard located at the following URL: https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/
Deliverable	Content Privacy and Security – within 30 calendar days of Contract expiration or termination, Supplier will deliver to ELECT, in writing, the removal of all ELECT content and Commonwealth data from their systems.
Delivery Frequency	Within 30 calendar days of Contract expiration or termination

Performance Standard	SLA #16 - Content Privacy and Security Supplier shall have 15 business days to cure its noncompliance, or with agreement from ELECT and VITA, in its governance role, may request a reasonable extension for time to cure providing ELECT, and a copy to VITA at: enterpriseservices@vita.virginia.gov, with a written plan of action to cure.
Deliverable	Content Privacy and Security – within 15 business days Supplier will have the noncompliance addressed or the Supplier will deliver to ELECT the written plan of action to cure ELECT noncompliance issue.
Delivery Frequency	Within 30 calendar days of Contract expiration or termination

3.0 Additional Services

3.1 Provide Additional Goods and Services (Based on a Negotiated Work Order)

Additional Goods and Services will allow the Commonwealth flexibility to use the Contract to have The Canton Group perform tasks not anticipated at the time of contract execution but identified later. The Deliverable(s) will be determined based on a negotiated statement of work.