Appendix 1 to
Fourth Amendment of
Master Services Agreement

Exhibit 2.8.3
Statement of Work
Risk and Compliance Services – Request for Revised Offer

DIR-MSS-SCP-001
June 26, 2019

Exhibit to Managed Security Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-MSS-SCP-001

Between

The State of Texas, acting by and through the Texas Department of Information Resources

and

AT&T Corp.

Exhibit 2.8.3

Statement of Work

Risk and Compliance Services – Request for Revised Offer

June 26, 2019

Change Log			
CCR/CN	Amendment	Date	Description
CCR-00314 CCR-00XXX	Amendment 1 Amendment 4	09/19/2018 6/26/2019	• Added RU definition for Election Security Assessments in Section 3.1.2.1 • Cosmetic updates (e.g., footer, revision number, etc.) • Section 3.1: Adds DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for Local Government Entities. • Section 3.1.2: Corrects typographic error in first sentence. • Section 3.1.6: Adds language to describe DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for Local Government Entities.

Table of Contents

1.0 Managed Security Services – Risk and Compliance

1.1 Services Overview

This **Exhibit 2.8.3 -** Managed Security Services – Risk and Compliance sets forth the roles and responsibilities of the Parties for the Services provided under the Agreement.

DIR is seeking a Service Provider to deliver the following types of services:

1. Risk and Compliance Services (RC)
    - Services assist Customers in assessing, managing, and mitigating risks and meeting compliance requirements of state, federal, or industry regulations

The type and scope of work will be determined by the Customer and agreed between the Service Provider and Customer.

1.2 Service Strategies and Objectives

Managed Security Services (MSS) is a procurement and service delivery mechanism to be offered by Texas DIR for customers to engage providers to obtain governed security services. Customers may request specific solution proposals that assume the responsibilities defined in this Statement of Work that will be applied to a specific scope of work. The service level requirements are described and documented in **Exhibit 3** and its attachments; pricing is described and documented in **Exhibit 4** and its attachments.

2.0 Service Environment

2.1 Scope of the Infrastructure to Be Supported

The following sub-sections and related Appendices further describe and scope the Services to be supported and/or with which Service Provider shall comply. The Service Environment will be specifically defined at the time the Service Provider is engaged by a Customer to propose or deliver Services.

To provide general context across potential Service Environments, the following sections may reference general lists, descriptions or guidance to be considered by the Service Provider in responding to the DIR RFO.

2.1.1 Services and Data

1. All support services must be situated and all agency-related data must reside within the contiguous United States at all times. DIR will not consider any support services situated outside the United States nor will DIR allow any agency-related data to be stored outside the contiguous United States
2. All data or other information generated as a result of services provided by any Service Component Provider must be protected and shared only with relevant stakeholders and may not be shared for the purposes of additional sales opportunities. All data must be protected in accordance with the MSA.

2.1.2 Service Hours and Locations

All services listed below must be offered based on the following service hour options:

1. 24x7x365: all Services to be provided 24 hours a day, 7 days a week, all 365 days per year. **NOTE:** No off-shoring of resources or services is allowed.
2. 7am-7pm weekdays: all Services to be provided from 7am to 7pm weekdays, with on-call resource support provided during off hours.

All services may be offered remotely, from the Service Provider's facilities. Service Provider must provide Services at Customer locations, if a Customer requests such services through the Request Management system, in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

Reference **Attachment 4-A**, Service Provider Pricing Forms, for resource unit pricing models for the Services required in this Statement of Work.

2.1.3 Personnel

Service Provider will be responsible for providing appropriately skilled staffing to meet the Roles and Responsibilities and service levels set forth in this SOW.

NOTE: Customers may request, through the Request Management process, dedicated resources to provide Services at the Customer's location. Service Provider shall provide dedicated, onsite resources to support Customer's needs in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

2.1.4 Policies, Procedures and Standards

The general policies, procedures and standards with which Services will comply are provided in **Attachment 6-B** Service Management Manual. Additional requirements will be determined if the Service Provider is engaged by a Customer to propose or deliver services.

2.1.5 Network Connectivity

Service Provider is responsible for providing the necessary network connectivity to DIR Facilities required to support the Services in accordance with the established Service Levels.

2.1.6 Dashboard

Service Provider shall provide a dashboard for use by DIR and each Customer as defined in **Exhibit 2.1.2**, Cross-Functional Services. The dashboard shall provide a real-time user interface, showing a graphical presentation of the current status and historical trends of DIR's, the Customer's, or computer appliances key performance indicators necessary to enable instantaneous and informed decisions to be made at a glance.

Customers will require a single tenant dashboard. However, DIR will require a multi-tenant dashboard allowing DIR to access the dashboard for any of the Customers.

2.1.7 Centralized Data Repository

Service Provider shall provide an on-line and secure Centralized Data Repository to store, at a minimum, all DIR Data, log files, and documentation generated as part of and required to perform the Services. All DIR Data shall be kept in accordance with the Customer's applicable record retention requirements. The Centralized Data Repository shall be single tenant for each Customer. DIR requires a multi-tenant Centralized Data Repository allowing access to the repository for other Customers. Service Provider is responsible per **Exhibit 2.1.2**, Cross-

Functional Services, and **Exhibit 13**, Reports, to provide timely and integrated data feeds to the MSI for reports placed on the DCS Portal, including Configuration Management.

2.1.8 Systems and Tools

Service Provider is required to provide any tools (both hardware and software) necessary for the execution of the Services. Service Provider shall maintain tools to meet performance standards, processes and policies requirements, to maximize efficiency, and to minimize outages, as necessary.

Customers may request, through the Request Management process, that the Service Provider use the Customer's tools to provide the Services. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

Service Provider shall use the systems and tools provided by the MSI in delivering Services.

2.1.9 Operational Support

Service Provider is responsible for managing the technical operations that support the delivery of the services according to best practices, including regular backups, capacity management, availability management, and Service Provider's own disaster recovery and business continuity. Operational support must be provided for any systems, services, or components on a 24x7x365 basis, in accordance with DIR published processes in the Service Management Manual, including but not limited to maintaining current Hardware and Software version levels on all Systems, Services, and Components in compliance with 1 TAC 202, Customer published standards and processes, and DIR governance board. Reference **Exhibit 4-B** for hardware and software version requirements.

2.1.10 Transition Status Meetings

As directed by DIR, Status meetings will be held at DIR offices to update progress made, seek input from DIR, and to ensure that work is proceeding in the desired direction. Any issues affecting this project shall be addressed at these meetings. Initially, it is intended that these meetings will be held at least weekly. The frequency of these meetings may be altered to fit the then current need. At a minimum, the Status Meetings shall include:

1. Agenda – Service Provider shall provide a written agenda to DIR Project Manager at least 24 hours prior to meeting. This will allow DIR Project Manager the opportunity to include any additional topics.
2. Minutes - Service Provider shall keep minutes of each meeting and provide a written copy to DIR Project Manager within two business days of the meeting. As a minimum, minutes shall address topics discussed, issues raised, and intended resolution of those issues.
3. Status Reports - Service Provider shall provide weekly written status reports to the DIR Project Manager. The written status reports shall address Tasks Completed, Tasks in Progress, Work to be Initiated During the Next Period, identified Risks with Risk Management approach, and Issues Requiring Management Attention. Issues Requiring Management Attention shall include, but not be limited to, any problems that may delay performance along with proposed corrective action, any failure of Service Provider or DIR to perform, any delay of Service Provider or DIR in performing, and any inadequacy in the performance of Service Provider or DIR.

In the event the Service Provider fails to timely specify in writing, within the applicable weekly reporting period, an Issue Requiring Management Attention for the Weekly Status Report, Service Provider shall not be entitled to rely upon such Issue as a purported justification for either (1) claiming Service Provider is entitled to receive any amount (including, without limitation, damages or additional charges arising out of a breach by DIR or Customer of a DIR or Customer obligation) with respect to Service Provider's obligations hereunder in excess of those previously agreed to; (2) failing to complete any of Service Provider's obligations hereunder or (3) requesting any reduction in or avoidance of damages or penalties. Submission of the above referenced status reports shall not alter, amend or modify Service Provider's or DIR's rights or obligations pursuant to any provision of the Contract.

2.1.11 Key Service Provider Personnel

Service Provider shall designate Key Personnel for the Service Component and each of the service areas in accordance with the MSA, **Section 8.1**, Key Service Provider Personnel. At a minimum, Key personnel shall include:

- Account Manager
- Executive Sponsor
- Transition Manager (TM)
- Technical Subject Matter Experts or Leads

All proposed personnel shall be immediately available to provide services as required. Key Service Provider Personnel may not be removed from the project without DIR's written permission.

2.1.12 Confidentiality

In providing services under this contract, the Service Provider will have access to confidential information related to each Customer. Therefore, Service Provider may be required to execute a non-disclosure/confidentiality agreement with each Customer.

Information obtained by Service Provider in the performance of this Contract shall be used only for the purposes of carrying out the provisions of this Contract. Inspection by or disclosure of any such information to anyone other than an officer or employee of Service Provider or Customer, other than for the purposes of carrying out, and in accordance with, the provisions of this Contract, shall require prior written approval of the Customer.

Service Provider shall implement and document a comprehensive information security program. Service Provider shall use, implement, and document reasonable and appropriate security practices to make information secure. If the security of any shared data is compromised or breached by Service Provider, subcontractors, or third-party, Service Provider shall notify DIR and Customer immediately, but no later than 12 hours after discovery of the potential compromise or breach. Service Provider shall be liable to Customer for any compromise or breach whatsoever and shall be liable for all reasonable and appropriate costs (as determined by DIR or the Customer) associated with remediating the compromise or breach, as defined in the Master Services Agreement.

2.1.13 Background Checks

Prior to commencement of any services, Service Provider is required to conduct background and/or criminal history investigation of the Service Provider's employees and subcontractors

who will be providing services under the resulting contract in accordance with MSA, **Section 8.6(g)**, Background and/or Criminal History Investigations, and **Exhibit 17**, Safety and Security.

3.0 Service Descriptions – Risk and Compliance

3.1 Risk and Compliance Service Component

Risk and Compliance Services assist Customers in assessing, managing, and mitigating risks and meeting compliance requirements of state, federal, or industry regulations. The Risk and Compliance Service Provider (RC Service Provider) shall help the Customer identify, remediate, monitor, exploit, and manage enterprise risks in addition to coordinating the utilization of people, process and technology to improve program effectiveness and help manage costs.

The RC Service Component is divided into five (6) Service Areas:

1. Penetration Testing
2. Security Risk Assessment
3. Cloud Compliance
4. Vulnerability Scanning
5. Web Application Vulnerability Scanning
6. DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for Local Government Entities

3.1.1 Penetration Testing Services

This section identifies requirements for penetration testing of a designated set of devices, systems, networks, subnets, or mobile applications. All penetration tests shall be assessed and rated against two (2) objectives:

1. Identify and retrieve proprietary or confidential information
2. Gain unauthorized access to a system or device

3.1.1.1 Penetration Testing Service Requirements

At a minimum, the RC Service Provider shall meet or exceed the following requirements for both Black Box and White Box Penetration Testing:

1. Perform external penetration testing from outside of the Customer Environment using Service Provider provided equipment and including the use of automated vulnerability scans and Web Application Vulnerability Scans (WAVS), as well as manual exercises in order to identify as many vulnerabilities as possible. For clarity, the cost of performing one WAVS with the penetration test is included in the penetration test resource unit. Additional WAVS performed would be subject to an additional charge of the WAVS resource unit.
2. Perform vulnerability and penetration testing on Internet websites or mobile applications in accordance with applicable state, federal, or industry regulations.
3. Conduct penetration testing based on the objectives defined in section 3.1.1 and provide the Customer with reports detailing the findings.
4. Attempt to test and probe for security vulnerabilities and exploit vulnerabilities on all discoverable devices and hosts within the specified IP range and/or the Customer's primary URLs listed and all sub-links attached to the Customer's network.

5. Use commercially available software, freeware, shareware, and custom scripts to conduct network reconnaissance, vulnerability analysis, and limited exploits of areas deemed most vulnerable.
6. Conduct redundant automated vulnerability scanning of the network range and URLs provided by the Customer
7. Probe for firewalls, intrusion detection systems, and access control lists and search for back doors.
8. Collect user accounts and passwords, where accessible, and attempt privilege escalation. This may require that software be transferred to, compiled on, or temporarily installed on the Customer's systems. The Service Provider shall remove all tools, utilities, and/or files, with the exception of authorized artifacts or files/tools necessary to be shown or demonstrated in the subsequent results report.
9. Artifacts that should be left behind for the Customer:
    9.1. User accounts added by the penetration tester
    9.2. Password modification (changing end user passwords)
    9.3. Text files indicating that the DIR Office of the CISO gained access (a new file created containing the text "DIR WAS HERE" or a similar variation)
    9.4. Inert executable file(s) such as dir.cmd, dir.sh, or related tools/files
10. Items the Service Provider is authorized to retrieve:
    10.1. Mirroring or scraping the website (collecting all web pages and information associated with the Customer's site.)
    10.2. Collection of documents/files (may include files with doc, txt, xls, pdf, ppt, etc., extensions)
    10.3. DNS zone files (transfer of internal Domain Name Service zone files that identify internal systems)
    10.4. Router/infrastructure equipment configuration files
    10.5. Database query results.
11. Services that the Service Provider may redirect:
    11.1. DNS traffic
    11.2. Intrusion detection systems (IDS)
    11.3. Login services
    11.4. Printer/scanning storage devices
    11.5. Simple Network Management Protocol (SNMP)
    11.6. System logging
12. The Service Provider shall disclose to DIR any objectional material discovered during the penetration test, such as obscene, excessively violent, harassing, or otherwise objectional material that may violate State or Federal law.
13. The Service Provider shall disclose to DIR any child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110.
14. The Service Provider shall endeavor not to disrupt the Customer's services during the penetration test to the extent possible.
15. The Service Provider shall not conduct any deliberate Denial-of-Service attack.
16. Produce penetration test results report, including but not limited to:
    16.1. Custom report providing Customer with findings, a summary of activities, vulnerabilities identified, and all exploit cases describing how objectives were met.
    16.2. Reports generated from the automated vulnerability scanning tools
    16.3. Analysis, descriptions of, and recommendations for protecting against confirmed vulnerabilities and, if applicable, exploits used during the penetration test.
    16.4. All other vulnerabilities discovered during the penetration test.

17. Request that the Customer place DIR's IP ranges in the Customer's non-shun list (whitelist) within the Customer's IDS/IPS if the Service Provider detects that the Customer is "shunning" or otherwise preventing the test from completing network mapping, scanning, or any other related testing activities during a White Box test.
18. Notify the Customer if anomalies such as system failure, inappropriate use of resources, or actual malicious attack are discovered during the penetration test.
19. Notify DIR's Communications Technology Services Division and/or Network and Security Operations Center if vulnerabilities are discovered during the penetration test on network equipment owned or maintained by the Communications Technology Services Division.
20. This service shall include, at no additional cost, a follow up scan of any identified vulnerabilities after remediation by the Customer to ensure the vulnerability was remediated.
21. Provide a method for Customer's authorized internal users to submit a request for a follow up scan.
22. RC Service Provider shall provide the final test results and all related work products and documentation to DIR and the Customer.
23. For each Penetration Test, the RC Service Provider shall provide, at a minimum, the following reports:
    A. Scan results (raw data report) (Excel) and automated scan results to be provided in a CSV file format for DIR to upload into the DIR SPECTRIM/Archer system.
    B. Penetration Test Report to be provided as a PDF. At a minimum, the Report shall be structured as follows unless changed through mutual agreement of DIR and the Service Provider:
        1. Section I- Introduction. At a minimum, the Introduction shall include:
            a. Deliverables, Usage, Contents
                i. Audience, Usage and Contents
                ii. List of Network Security Assessment Files Posted to HSIN Security Portal
        2. Section II- Assessment Process. At a minimum, the Assessment Process shall include:
            a. Assessment Objectives
            b. Engagement Assumptions
            c. Methodology
        3. Section III- Executive Summary. At a minimum, the Executive Summary shall include:
            a. Scope
            b. Results
            c. Assessment Analysis
            d. Conclusion
                i. Findings
                ii. Recommendations
        4. Section IV- Analysis and Recommendations. At a minimum, the Analysis and Recommendations shall include:
            a. Vulnerability Summary
            b. Vulnerability Detail Analysis and Recommendations
            c. Exploit Analysis
    C. Remediation Survey to be provided as a Word file. At a minimum, the Remediation Survey shall meet the following requirements:

1. Listing of all the vulnerabilities found in the manual testing process and associated IP addresses
2. Each vulnerability shall include a check box with the following options so that the customer can return the survey to DIR reporting the final status of each vulnerability:
    a. Remediated
    b. Mitigated
    c. Inaction
    d. Acceptable Risk
    e. False Positive
3. Notes section included to add addition information for each vulnerability.

23. Meet with Customer to explain report and answer questions.

3.1.2 Security Risk Assessment

RC Service Provider shall assess vulnerabilities and threats associated with and including, but not limited to, how the vulnerabilities and threats combine to form risks and recommending steps for remediation of the risks. RC Service Provider shall provide recommendations to the Customer on timeframes for conducting periodic reviews, remediation, audits, security vulnerability assessments, and security Risk Assessments of the Customer's environment, processes, and practices. Customer and RC Service Provider will mutually determine the frequency of these services.

3.1.2.1 Security Risk Assessment Service Requirements

At a minimum, the RC Service Provider shall meet or exceed the following Risk Assessment requirements:

1. Work with Customer to identify key assets and their current protections
2. Identify and document Customer's security policies and processes
3. Based on Customer's security policies and procedures, analyze the security threats to Customer's environment and evaluate the level of compliance with the Texas Cybersecurity Framework, Payment Card Industry Data Security Standard (PCI DSS) [1], Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), or other standards as applicable and required by Customer.
4. Identify any discovered vulnerabilities and any critical or high risk vulnerabilities including the potential impact of vulnerabilities; likelihood of the vulnerability being exploited; and suggested remediation of the vulnerability.
5. Develop a roadmap for improving Customer's maturity and provide a Risk Register as a repository for all risks identified and any additional information required by the Customer concerning each risk, including risk management measures
6. RC Service Provider shall provide the assessment, analyses, and all related work products and documentation to DIR and the Customer.
7. For Customers with Payment Card Industry data, the Service Provider shall perform assessments and provide assessment results to support the Customer's completion of the PCI DSS Report on Compliance. Service Provider will function as the "Assessor" for the PCI DSS Report on Compliance. Service Provider will be

[1] For reference, the Payment Card Industry Data Security Standards are documented at: https://www.pcisecuritystandards.org/

responsible for assessing all areas and functions required on the PCI DSS Report on Compliance as per Customer's request.

8. For Security Risk Assessments, it is anticipated that the following process will be used:
   A. The RC Service Provider will communicate directly with each agency engaged in security assessments and schedule assessments.
   B. The RC Service Provider will conduct a kickoff meeting with each identified agency to establish and ensure mutual understanding of the project objectives, scope, schedule and milestones, roles, responsibilities, communication plan, logistics and required resources for the RC Service Provider and each agency.
   C. The RC Service Provider will conduct security and risk assessments for each identified agency including interview of participants, identifying anticipated risks, mitigation plans, lessons learned and gathering relevant background information/material from each agency.
   D. The RC Service Provider will establish and maintain a project tracking document that details which agencies are being assessed, the dates/phases of the assessment, and the status of each assessment.
   E. The RC Service Provider will establish a single point of contact for questions/clarifications; document project timelines, milestones, roles, responsibilities, communication plan, logistics; and provide and deliver all relevant documentation supporting material to the agency.
   F. For agency Security Risk Assessments authorized and paid for by DIR, the RC Service Provider shall also:
      1. Work with DIR to identify agencies and institutions of higher education that may be assessed.
      2. Provide DIR with the required data to be used for statewide reporting on the overall security posture of the State of Texas
      3. Provide and deliver all relevant documentation supporting material to DIR and the agency.
   G. For Texas Cybersecurity Framework Risk Assessments, the Service Provider shall also:
      1. Based on Customer's security policies and procedures, analyze the security threats to Customer's environment and evaluate the level of compliance with the Texas Cybersecurity Framework.
      2. Analyze the effectiveness and provide a maturity level, based on the Texas Cybersecurity Framework, of Customer's current controls.
      3. The RC Service Provider shall provide the items detailed in the following "Deliverables" table:

Deliverables for Texas Cybersecurity Framework Risk Assessments			
No.	**Deliverable Name**	**Task**	**Due Date**
1	Project Work Plan	Provide a break down at the task level that is consistent (i.e., everything must roll up to a subtask or task) and of a manageable size (no more than 40 work hours per task or must break in to smaller tasks). At a minimum, tasks shall include: • Duration	4 weeks from project start date

		• Dependencies • Start/Finish • Deliverables • Deliverable Dates • Schedule • Milestones • Critical Path	
2	Baseline Report	Provide an assessment of the current-state of the infrastructure, the business drivers, and the strategic future-state requirements. The RC Service Provider shall document the current-state baseline IT environment as it relates to security, including the people, processes, and technologies. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	Per Agency Assessment
3	Recommend ations Report	Provide a Recommendations Report to identify the relevant vulnerabilities by conducting a gap analysis between the identified current state (baseline report) and best industry-leading practices, as well as the Maturity Levels' recommendations provided in the Texas Security Framework. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	Per Agency Assessment
4	Security Roadmap	ProSecurity Roadmap providing a strategic high-level deployment roadmap for the identified recommendations, including baseline description, drivers and requirements, gap analysis, recommendations and deployment roadmap. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	Per Agency Assessment
5	Closeout and Final Executive Report	Executive Report providing a one to three page roadmap and conduct an overview presentation of the results of this engagement to participating agency's management and stakeholders	Per Agency Assessment

		including: prioritization of the roadmap recommendations; timelines for implementation of recommendations; estimated cost of recommendations, based on industry standard, not the amount the Service Provider would charge; resources involved; any other critical information; and use trends from other Security assessments results to show comparison of the Security posture of the agency to the rest of the State. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	
6	Quarterly Aggregate Report	Quarterly aggregate view of assessments completed. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	Quarterly
	Trends Analysis Report	Measures on trends and shortcomings from multiple, anonymized agencies. This deliverable shall be provided in an electronic document form and will be presented to the project team for final delivery to the State as a completed deliverable.	Quarterly

H. For Election Security Assessments, the Service Provider shall also:
   1. Provide a comprehensive assessment of election cybersecurity
      i. Provide technical evaluation, including threat analysis, vulnerability analysis, penetration testing, darknet investigation and analysis
         1. Provide detailed analysis of processes, procedures, systems and personnel
         2. Detection of any existing threats or malware
         3. Evaluate darknet (Threat Intel) for compromised assets and targeted threats
         4. Perform technical scans by skilled cybersecurity analysts
         5. Perform penetration test
         6. Perform vulnerability scan and provide an assessment
         7. Identify security devices and review configurations and logs to assess security posture
         8. Evaluate networking plans

9. Provide an assessment of vendor maintenance capabilities and remote support mechanisms

ii. Interview & Evaluate processes as led by industry experts with deep Risk Assessment experience and Elections knowledge to include evaluation of staff on process adherence.

iii. Perform onsite evaluation included for every county

iv. Perform personnel interviews

v. Each election system shall be evaluated against:

1. DHS Elections Guidelines
2. CIS Elections Best Practices
3. NIST Cyber Security Framework (CSF)
4. Aligned with Texas Cyber Security Framework (CSF)
5. Industry Best Practices

2. Compile findings and provide recommendations to address the findings.
3. MSS RC SCP will process all findings and assign each a value to determine the impact that issue may have on the county and the overall probability that the issue may happen

Deliverables for Election Security Assessments			
No.	**Deliverable Name**	**Task**	**Due Date**
1	Election Security Assessment (ESA) Scorecard	The ESA Scorecard provides the county with a four-page scorecard of the current high-level security concerns and recommendations. Results will be presented visually and in language that does not require specific cybersecurity experience and knowledge.	4 to 10 weeks from project start date based on project size
2	Election Security Assessment (ESA) Report	The ESA Report provides technical detail to support the findings presented in the Scorecard and to provide a detailed set of recommendations that can be provided to an IT or security provider to improve the overall security of the county. The ESA Report also includes a detailed risk assessment and review of cybersecurity control maturity.	Per Assessment

10. Acceptance of Deliverables

The RC Service Provider shall deliver each completed deliverable on the corresponding due date as specified in the SOW. DIR will have seven (7) business days to review and either accept or reject each deliverable. In the event that a deliverable is not acceptable due to a material and substantial non-conformity, DIR will provide to the RC Service Provider a written notice of such non-acceptance with sufficient detail to clearly identify the reason for non-acceptance. The RC Service Provider shall have seven (7) business days following receipt of such notice of non-acceptance to use reasonable commercial efforts to cure or remedy the problems detailed therein, and resubmit the deliverable to DIR. The parties shall repeat this procedure until acceptance of the deliverables.

3.1.3 Cloud Compliance

RC Service Provider will perform, in accordance with Customer's audit requirements, security compliance reviews of hosted service providers (and other Cloud service providers), provide validation of certifications for new hosted service providers, and perform annual re-certifications.

3.1.3.1 Cloud Compliance Service Requirements

At a minimum, the RC Service Provider shall meet or exceed the following Cloud Compliance requirements:

1. Coordinate Customer security requirements based on the level of security compliance required by Customer's internal policies, audit requirements, or other statutory mandates.
2. Based on Customer's identified security requirements, RC Service Provider shall develop a security compliance checklist for use in assessing hosted service providers.
3. Perform a security assessment and verification of hosted service providers in alignment with the security compliance checklist.
4. Document the risks, and where applicable identify risk management strategy, identified from the security assessment for Customer's review.
5. Report detected deficiencies or vulnerabilities to the Customer.
6. RC Service Provider shall provide the assessments and all related work products and documentation to DIR and the Customer.

3.1.4 Vulnerability Scanning

The RC Service Provider shall scan network ranges or specified devices, including mobile applications, for known vulnerabilities. RC Service Provider shall be able to perform these services with either credentialed or non-credentialed access.

3.1.4.1 Vulnerability Scanning Service Requirements

At a minimum, the RC Service Provider shall meet or exceed the following Vulnerability Scanning requirements:

1. Scan any applicable new Systems or Application Software (or any Systems or Software to be deployed as part of a new project). Scans shall include both an operating system scan, as well as a scan of all application components.
2. Conduct pre-production meetings with the project teams responsible for the assets subject to vulnerability scanning on an ad-hoc basis.
3. Perform security vulnerability assessments (i.e., review of scans, code, server, software, etc.) of the Customer Environment in accordance with Customer's security requirements.
4. Perform scheduled vulnerability scans as required by Customer policy, state statute and federal program guidelines.
5. Conduct scheduled scans of Customer's databases, shares, and files systems for Customer Payment Card Industry Data, Personal Identifiable Information, protected healthcare information, and account password or other data as specified by Customer.
6. Scan Customer's network devices in order to identify any deviations from default configurations, misconfigurations, or device vulnerabilities.
7. Report all detected vulnerabilities to the Customer IT Security team in accordance with the Customer's required timeframe(s).

8. RC Service Provider shall provide the final test results and all related work products and documentation to DIR and the Customer.
9. RC Service Provider shall perform one (1) rescan after the Customer has remediated vulnerabilities at no additional cost to the Customer.
10. Perform vulnerability scans in accordance with the most current PCI-DSS requirements for Customers with payment processing infrastructures, including performing scans via an Approved Scanning Vendor as required.

3.1.5 Web Application Vulnerability Scanning (WAVS)

This section identifies requirements for managing web application and URL scanning in the environment, including updates and support both for base software and signatures.

3.1.5.1 WAVS Service Requirements

At a minimum, the RC Service Provider shall meet or exceed the following WAVS service requirements:

1. Perform comprehensive scanning of web-based applications for known security flaws, vulnerabilities, or software code that could be used to disrupt service or expose Customer data.
2. Perform authenticated and un-authenticated testing, as directed by Customer.
3. Perform validation of SSL implementation and certificates, if applicable.
4. Report all detected vulnerabilities to the Customer IT Security team in accordance with Customer's required timeframe(s).
5. RC Service Provider shall save the final test results and all related work products and documentation for review by Customer, Customer's external auditor, or other authorized third-party.

3.1.6 DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for Local Government Entities

DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) system is available for local government entities and is being offered as a Software as a Service (SaaS) solution, hosted and maintained on the RSA® Archer® platform. The RC Service Provider will provide the RSA® Archer® platform SaaS and maintain the hosting service.

3.1.6.1 SPECTRIM Requirements

At a minimum, the RC Service Provider shall meet or exceed the following SPECTRIM service requirements:

The local government subscriptions will have functionality to cover the following Use Cases:

1. Business Asset Catalog (organization application, division application, contacts application)
2. IT Asset Catalog (applications, networks, locations, IT Inventory, information types)
3. Risk Catalog (risk register, risk library, risk hierarchy)
4. Bottom-Up Risk Assessment (risk accessible unit, application assessment, organizational security assessment, location assessment, network assessment)
5. Federal Assessment & Authorization (authorization package, control catalog, assessment objectives, allocated controls, control overlay, privacy threshold

analysis, privacy impact analysis, ports/protocols/services management, interconnections)
6. Incident Management (incidents)
7. Issues Management (findings, remediation plans, exception requests)
8. Policy Program Management (policies, control standards, authoritative sources)
9. Risk Inventory and Top-Down Assessment (same as risk catalog)
10. Security Plan Template (security plan template, security plan template overall record)
11. Miscellaneous Applications (Archer or SPECTRIM support request, document repository, user admin approval.)

Functionality will cover the applications specified under these use cases as replicated within the existing state of Texas instance. Future implementation of use cases and applications within the current DIR statewide SPECTRIM instance may become available through this SaaS solution for local government entities.

Subscriptions are limited to what has been stated above as in the current DIR statewide SPECTRIM instance.

All customization to the use cases will be outside the scope of the RC Service Provider.

Application upgrades, patches, revisions, or additions to the Hosting Services will be maintained by the RC Service Provider but will not follow the MSS Change Management Process as the patches are applied based on an existing schedule managed by RSA.

Backup shall be performed on a regular basis. In the event of a Force Majeure Event, the RC Service Provider will recover Hosting Services and Customer Data within a 72 hours period. Customer Data will be recovered from the latest nightly backup that is available.