

AUG 12 2019

Presented

**REQUEST FOR AGENDA PLACEMENT FORM**

Submission Deadline - Tuesday, 12:00 PM before Court Dates

**SUBMITTED BY:**

**TODAY'S DATE: 8-6-19**

**DEPARTMENT:**

**SIGNATURE OF DEPARTMENT HEAD:**

**REQUESTED AGENDA DATE: 8-12-19**

**SPECIFIC AGENDA WORDING:** Consideration for Soctt Baxley or a representative form AT&T to speak to CC.

**PERSON(S) TO PRESENT ITEM:** Patty Bourgeois

**SUPPORT MATERIAL: (Must enclose supporting documentation)**

**TIME: 20**

(Anticipated number of minutes needed to discuss item)

**ACTION ITEM:** \_\_\_\_\_

**WORKSHOP:** \_\_\_\_\_

**CONSENT:** \_\_\_\_\_

**EXECUTIVE:** \_\_\_\_\_

**STAFF NOTICE:**

**COUNTY ATTORNEY:** \_\_\_\_\_

**AUDITOR:** \_\_\_\_\_

**PERSONNEL:** \_\_\_\_\_

**BUDGET COORDINATOR:** \_\_\_\_\_

**IT DEPARTMENT:** \_\_\_\_\_

**PURCHASING DEPARTMENT:** \_\_\_\_\_

**PUBLIC WORKS:** \_\_\_\_\_

**OTHER:** \_\_\_\_\_

\*\*\*\*\*This Section to be Completed by County Judge's Office\*\*\*\*\*

ASSIGNED AGENDA DATE: \_\_\_\_\_

REQUEST RECEIVED BY COUNTY JUDGE'S OFFICE \_\_\_\_\_

COURT MEMBER APPROVAL \_\_\_\_\_

Date \_\_\_\_\_

## MANAGED SECURITY SERVICES TERMS AND CONDITIONS

This agreement is part of and incorporated within the Interagency/Interlocal Contract ("Contract") that has been entered into by the contracting parties. DIR Customer acknowledges and agrees that this Contract is with DIR and, therefore, DIR Customer does not have privity of contract with the SCPs.

Capitalized terms not defined herein shall have the meaning set forth in the relevant DIR Shared Services Contract.

DIR Customer agrees to the following conditions for receiving Managed Security Services:

### 1. Conditions for Providing Security Services

#### 1.1 Access

DIR and/or Service Component Provider (SCP) shall use the Internet for primary access to DIR Customer's systems unless otherwise noted and agreed upon. DIR Customer shall not employ special access restrictions against DIR and/or Service Component Provider that it does not apply to the rest of the public network over the course of regular business.

#### 1.2 Network Control

DIR Customer must inform DIR if DIR Customer does not control its network access and/or its Internet service is provided via a third party. DIR Customer is responsible for obtaining all necessary approvals. DIR Customer shall provide all necessary contact information for the third parties that control its network access, Internet service, and/or web applications. DIR Customer's emergency contact list shall include primary and secondary staff capable of administering DIR Customer computer systems specific to the type of services being requested or required.

#### 1.3 Disclosure of Objectionable Material

In conducting the services authorized by DIR Customer, DIR may inadvertently uncover obscene, excessively violent, harassing, or otherwise objectionable material that may violate State or Federal law, including material that may infringe the intellectual property of a third party on DIR Customer devices or networks. DIR shall notify DIR Customer's Executive Director or highest level executive of the existence of all such objectionable and/or potentially illicit material so that DIR Customer may deal with the objectionable and/or potentially illicit material as it deems appropriate.

If DIR accesses child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110, in conducting approved Services, DIR shall report such to DIR Customer's Executive Director or highest level executive and an appropriate law enforcement agency and provide the law enforcement agency access to the visual depictions of child pornography.

If DIR accesses information that they perceive as a serious threat to human life or safety in conducting the approved Services, DIR shall report such threat to an appropriate law enforcement agency and DIR Customer's Executive Director or highest-level executive.

#### 1.4 No Warranties and Limitation of Liability

DIR makes no representation or warranty that its security services will disclose, identify, or prevent all vulnerabilities. DIR hereby disclaims all warranties, both express and implied, including without limitation, the implied warranties of merchantability and fitness for a particular purpose. In no event shall DIR be liable for damages of any kind or nature that may arise from the services provided by DIR or DIR's Service Component Provider or Service Provider.

## **1.5 Service Interruption**

DIR will endeavor not to disrupt DIR Customer's services and to adhere to best practices for all work performed. However, tools or services may affect the serviceability of poorly configured or overextended systems or services. It is possible that control of DIR Customer's system may be lost. For any testing that DIR may be conducting, DIR endeavors to use the safest methods to compromise DIR Customer's systems; however, DIR Customer should be prepared to restore a damaged system from a recent, acceptable backup within an acceptable time as determined by DIR Customer. During any testing DIR may conduct, DIR will NOT conduct any deliberate Denial-of-Service attack. DIR Customer agrees not to hold DIR liable in the event of any service interruption(s) that may arise as a result of performance of any Services. If either party becomes aware of a service interruption, that party will notify the other party's emergency contact.

## **1.6 Termination of Services**

If DIR Customer terminates certain Services, that it requested and approved, for convenience, DIR Customer shall pay the remaining requisite unrecovered costs that have already been incurred prior to the notice of termination, such unrecovered costs will be calculated in accordance with the relevant DIR Shared Services Contract, SMM, or other DIR Customer approved terms. DIR Customer understands that it may not be able to terminate services or receive any refund of a pre-payment after approving the relevant financial solution.

## **2. DIR and DIR Customer Responsibilities**

### **2.1 DIR Customer agrees as follows to the extent assessment Services are requested or required:**

- a) DIR Customer responses to information requests and artifacts gathering pertinent to this security and risk assessment will be timely;
- b) The artifacts data are reasonably available via interviews and documents review;
- c) DIR Customer will make available the necessary Subject Matter Expert (SME) with required expertise to work with the SCP Assessment Team and will remain available thru the duration of the assessment;
- d) DIR Customer SME will be available when required for interaction with the SCP Assessment Team and that all the interviews will be conducted over the number of consecutive days as established during the project planning and scheduling phase;
- e) DIR Customer is responsible for the coordination and scheduling of resources and providing meeting facilities as necessary;
- f) Deliverables will be complete when DIR Customer has approved in writing that the deliverable meets the acceptance criteria;
- g) All document deliverables must be in formats (hard copy and/or electronic) as specified by DIR Customer. At a minimum, the formats must be in industry-accepted standards (e.g., MS Word, MS PowerPoint MS Project);
- h) DIR Customer will assist with meeting coordination for meetings between DIR Customer Key Personnel and DIR and the Service Provider and other staff to gather requirements and other activities;
- i) DIR may receive final copies of reports if DIR is paying for the assessment.

## **2.2 Penetration Testing**

**2.2.1 DIR Customer agrees as follows to the extent penetration testing ("PT") is requested or required:**

- a) SCP may conduct a passive scan to determine the number of live IPs within the Customer designated IP range.
- b) DIR Customer shall not intentionally place an unsecured system or device in the test scope.
- c) If DIR Customer detects SCP testing activities, DIR Customer technical staff shall follow standard operating procedures and policies.

## **2.3 DIR Customer Compliance**

DIR Customer shall comply with all policies, procedures, and processes in the relevant SMM(s) and as provided by DIR.



CYBERDEFENSES

# Election Security Assessment Scorecard

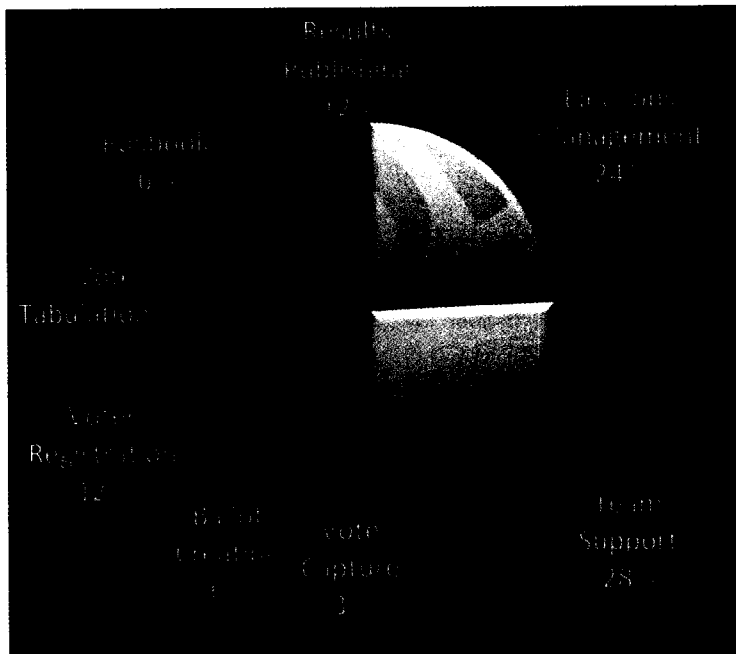
Fictitious Sample County – July 12, 2018

Revision 1.0

## Election Security Assessment

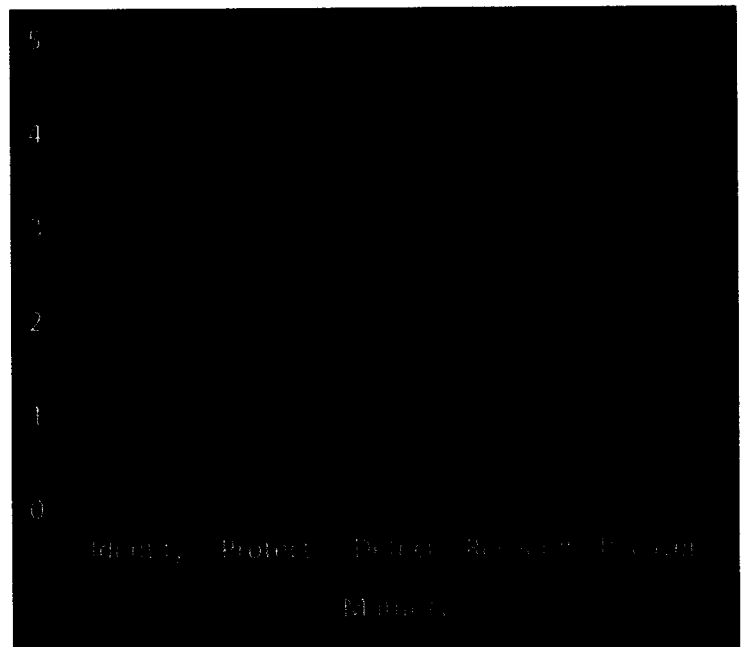
Risk Severity	Key Concerns	Security Readiness Score
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Critical</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">High</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Moderate</div> <div style="border: 1px solid black; padding: 5px;">Low</div>	<ul style="list-style-type: none"> <li>Malware discovered on County Chair and employee laptops</li> <li>Three critical vulnerabilities found on key applications</li> <li>Indicators of activist attack targeting region found on darknet</li> <li>Training required for leadership and employees</li> <li>Security policies not defined or followed</li> <li>VR application security involves risk-sensitive citizen data</li> <li>Vote aggregation PC not isolated from network activity</li> </ul>	<h1>2.6</h1> <p>Maturity Level</p>

### Critical & High Risks by Elections Area



Critical/ High Risks Discovered: 33  
Total Risks: 112

### Cyber Security Objective Maturity Levels




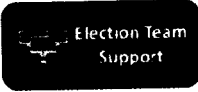


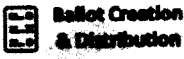
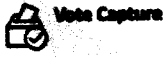

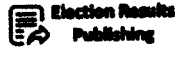
42 out of 80 NIST Objectives met with at least CMMI Maturity Level 1

See Page 4 for definitions related to these graphs

Please see the full assessment report for additional details

# Scorecard Per Elections Area

Fictitious Sample County, Texas

Elections Area	Description	Risk Severity	Key Risks
	The county supports a distinct EA function and manages interactions through email, sharing important files on a single file server. Total of three servers in use.	<b>Critical</b>	<ul style="list-style-type: none"> <li>Malware discovered on County Chair laptop</li> <li>Three critical vulnerabilities found on key applications</li> <li>Communication channels are not encrypted</li> <li>Insufficient leadership training</li> <li>Security policies not defined</li> </ul>
	County team includes a total of 24 county employees and 46 part-time. Six employees F/T focused on election admin. 26 PC's and three Servers supporting.	<b>Critical</b>	<ul style="list-style-type: none"> <li>Malware discovered on one employee PC</li> <li>312 stolen employee credentials discovered</li> <li>Insufficient training opens staff as key attack vector</li> <li>Staff not prepared for social engineering attacks</li> </ul>
	The County supports voter registration through the online use of TEAM. Applications are stored on a single Windows File Server.	<b>High</b>	<ul style="list-style-type: none"> <li>VR Applications stored insecurely</li> <li>TEAM Access systems not monitored or controlled</li> </ul>
	ePollbook support and voter check-in managed via HART application using user county provided tablets and laptops. Voter information in ePollbook is not sensitive.	<b>High</b>	<ul style="list-style-type: none"> <li>Tablets / Laptops not monitored or tightly controlled</li> <li>HART application security lacks encryption and key controls</li> </ul>
	Ballot design process performed in scanner vendor tools. Ballot distribution handled via email.	<b>High</b>	<ul style="list-style-type: none"> <li>Ballot storage and transmission need encryption</li> <li>Ballot creation policy and process require definition</li> </ul>
	Vote Capture is performed via paper ballot marking and in some precincts supported by Automark Ballot Markers	<b>Low</b>	<ul style="list-style-type: none"> <li>Automark firmware requires validation and reset before each election</li> </ul>
	Vote tabulation supported by M100 and M650 scanners	<b>Low</b>	<ul style="list-style-type: none"> <li>Scanner firmware requires validation and reset before each election</li> <li>LNA process requires security checks</li> </ul>
	Elections results taken from scanner and aggregated on single air-gapped PC. Results transferred to SoS and County website via USB.	<b>High</b>	<ul style="list-style-type: none"> <li>Aggregation PC not properly isolated from network activity</li> <li>USB keys in use not certified safe</li> </ul>

Cybersecurity services are available to support making the recommended improvements

Risk Severity	Count
Critical	4
High	37
Moderate	54
Low	122

Number of Recommendations

## Critical Recommendations

Total: 4

- Investigate and remove malware on County Chair's laptop
- Investigate and remove malware on election team member's laptop
- Change default admin passwords on election file servers
- Remove county VR Application Storage from general internet access

## Selected High Recommendations

Total: 37

- Create and implement election-focused security policies
- Implement security training program for election leadership and team members
- Update implementation of vote count aggregation PC to eliminate all network traffic
- Reset passwords of all 312 users that have had passwords stolen and are being traded on the darknet
- Implement security monitoring of all elections-based systems (that are not isolated)
- Implement network segmentation for all elections systems with IPS and Firewall features
- Disable 32 user accounts that belong to employees that have left the County but still retain network access
- Create updated inventory of all elections-related PC's and mobile devices

See the full report for a detailed listing of all recommendations

Fictitious Sample County, Texas

## Election Assessment Process

### The Elections Cybersecurity Assessment provides:

- Detailed testing and analysis designed by experienced elections and cybersecurity experts
- Onsite technical scans, penetration tests and analysis to identify malware, compromises and vulnerabilities
- Prioritized Recommendations for improvements

## The Standards used for Analysis

### Analysis is based on the following standards:

- DHS Cybersecurity Guidance and assessment standards
- CIS Elections Handbook
- NIST Cyber Security Framework (CSF), adapted to align with Texas CSF
- Industry Best Practices from decades of experience

## Risk Severity Definitions

Each detected concern is assigned a risk severity based upon the impact to the county and the probability that the concern may be a part of a cybersecurity attack. The table below illustrates how the combination of perceived impact and probability of each issue map to the assigned Risk Severity.

Risk Severity	Impact	Probability
<b>Critical</b>	High	High
<b>High</b>	Moderate	High
	High	Moderate
<b>Low</b>	Moderate	Moderate
	Moderate	Low
	Low	Moderate
	Low	Low

## Security Readiness & Maturity Index

The following CMMI Maturity levels are commonly used with the NIST CSF and used in calculating the County readiness grade and in Figure 2.

NIST Maturity Level	Name	Short Definition
5	Optimized	Efficient, Optimized, Economized
4	Advanced	Risk-Based, Measured
3	Strong	Managed, Consistent
2	Moderate	Compliant, Defined, Repeatable
1	Basic	Ad-hoc, Initial
0	Minimal	None, Non-Existent

Cybersecurity services are available to support making the recommended improvements from Texas DIR



**INTERLOCAL CONTRACT  
BETWEEN  
THE DEPARTMENT OF INFORMATION RESOURCES  
AND  
XXXX  
RELATING TO THE USE OF THE DIR SHARED SERVICES MASTER SERVICE  
AGREEMENTS**

This Interlocal Contract ("ILC" or "Contract") is entered into by the governmental entities shown above as contracting parties (referred to individually as a "Party" and collectively as the "Parties") pursuant to the provisions of the Interlocal Cooperation Act, Chapter 791, Texas Government Code. This ILC is created to give effect to the intent and purpose of Subchapter L, Chapter 2054, Texas Government Code, concerning statewide technology centers, specifically sections 2054.376(a)(3), 2054.3771, and 2054.3851.

The entity receiving services under the DIR Shared Services Contracts through this ILC is hereinafter referred to as the "Receiving Entity" or the "DIR Customer."

This ILC authorizes DIR Customer to participate in the Department of Information Resources ("DIR" or "Performing Agency") Shared Services Program. The DIR Shared Services Program includes contracts that have been competitively procured by DIR. All specific services and products are purchased through the DIR Shared Services Program contracts and subject to the processes and terms therein.

DIR's Shared Services Program provides for a Multisourcing Service Integrator (MSI) service provider ("MSI SCP") and various Service Component Providers ("SCP"). The Shared Services Master Service Agreements, as amended, are defined on the Shared Services web page on the DIR website ("DIR Shared Services Contracts") and are incorporated herein. Unless otherwise referenced, the references to Exhibits and Attachments herein are references to Exhibits and Attachments of the DIR Shared Services Contracts.

DIR Customer acknowledges and agrees that this ILC is with DIR and, therefore, DIR Customer does not have privity of contract with the SCPs.

Capitalized terms not defined herein shall have the meaning set forth in the relevant DIR Shared Services Contract.

**SECTION I  
CONTRACTING PARTIES**

**DIR CUSTOMER:** XXXX

**PERFORMING AGENCY:** Department of Information Resources

## **SECTION II STATEMENT OF SERVICES TO BE PERFORMED**

### **2.1 Effect of ILC and General Process**

The DIR Shared Services Program offers a variety of services and related support and products. The list of such services is provided through the DIR Shared Services Catalog and the DIR Shared Services portal. Further, SCPs may work with third-party vendors to provide additional services or products within the requirements of the relevant DIR Shared Services Contract.

This ILC describes the rights and responsibilities of the Parties relating to implementation, operation, maintenance, use, payment, and other associated issues by and between DIR Customer and DIR related to the Services to be provided through the DIR Shared Services Contracts. DIR Customer shall receive the Services described in the DIR Shared Services Contracts, subject to the terms of the relevant DIR Shared Services Contracts and this ILC. DIR Customer is only subject to those specific terms to the extent DIR Customer requests services or products through those specific DIR Shared Services Contracts.

The details of specific processes and procedures are contained in the relevant Service Management Manual ("SMM"), developed by the MSI and/or SCPs, approved by DIR, and incorporated herein. The DIR Shared Services Contracts require the MSI and SCPs to develop appropriately documented policies, processes, and procedures and to provide training to DIR Customer personnel where required to ensure effective service interfaces, before approval and adoption of the SMM.

The terms of the relevant DIR Shared Services Contracts will apply to this ILC and will remain in full force and effect except as may be expressly modified by any amendment to the specific DIR Shared Services Contract. Such amendments will automatically apply to this ILC with no further action by the Parties. DIR shall keep DIR Customer generally informed of such amendments and provide the opportunity to provide input to DIR through the Shared Services portal as well as the DIR Shared Services Program Governance structure described below.

### **2.2 DIR Shared Services Program Process**

To obtain Services, DIR Customer shall either order services directly through the MSI Marketplace portal where certain services and pricing are established or request certain services and products through the Request for Services process. This process is detailed in the relevant SMM for each SCP. SCP(s) will respond with a proposal, including the proposed solution or service, estimated cost or other financial obligations, if any, and any other relevant program-specific terms and conditions related to the services provided for in response to the Request for Service. DIR Customer may accept or decline those terms and services at that time. The final DIR Customer approved technical solution, financial solution, and related terms are contractually binding terms that incorporate the terms of

this ILC and the relevant Shared Services Contract(s). Later termination of a Service or solution after an original approval or any pre-payment, may result in additional cost to the DIR Customer and may not allow for any refund of payments already made.

### **2.3 Change Orders and Change Control**

In accordance with the relevant SMM and Shared Services Contract requirements, DIR Customer will coordinate with the MSI and/or SCP for all change requests. Change Control processes and authority may vary between DIR Shared Services Contracts as it relates to the rights of Customers to request changes. Further, Change Control does not allow DIR Customers to alter terms and conditions of the DIR Shared Services Contracts.

## **SECTION III DIR CUSTOMER PARTICIPATION**

### **3.1 General Shared Services Governance**

Governance of the DIR Shared Services Program is based on an owner-operator approach in which DIR Customers, in the role of operator, actively work with all SCPs to resolve local operational issues and participate in committees to address enterprise matters. Enterprise-level decisions, DIR Customer issues, and resolution of escalated DIR Customer-specific issues are carried out by standing governance committees, organized by subject area and comprised of representatives from DIR Customers, DIR management, SCP management, MSI management, and subject-matter experts. DIR Customers are structured into partner groups that select representatives to participate in these committees. DIR Customer shall participate within this Governance structure as described above and within the relevant SMM(s) ("Shared Services Governance").

### **3.2 DIR Customer and SCP Interaction and Issue Escalation**

In accordance with the relevant SMM(s), DIR Customer shall interface with SCPs on the performance of "day-to-day" operations, including work practices requiring SCP and DIR Customer interaction, issues resolution, training, planning/coordination, and "sign-off." All issues are intended to be resolved at the lowest level possible. In those instances where it becomes necessary, the following escalation path is utilized. If DIR Customer is not able to resolve an issue directly with SCP staff, DIR customer escalates the issue to SCP management. If the issue cannot be resolved by SCP management, DIR Customer escalates to DIR. If the issue cannot be resolved by DIR, DIR Customer escalates to the appropriate DIR Shared Services Program Governance committee.

### **3.3 DIR Customer Specific Laws**

Per the Compliance with Laws section of the DIR Shared Services Contracts, DIR Customer shall notify DIR, in writing, of all DIR Customer-specific laws ("DIR Customer-Specific Laws"), other than SCP Laws, that pertain to any part of DIR Customer's business that is supported by SCPs under the DIR Shared Services Contracts, and DIR

will notify SCPs, in writing, of such DIR Customer-Specific Laws. The Parties intend that such DIR Customer-Specific Laws will be identified and included in the portion of the SMM specific to DIR Customer. DIR Customer shall use commercially reasonable efforts to notify DIR, in writing, of any changes to DIR Customer-Specific Laws that may, in any way, impact the performance, provision, receipt and use of Services under the DIR Shared Services Contracts. DIR shall advise SCPs of such change and require that any changes to DIR Customer-Specific Laws are identified and included in the SMM. If necessary to facilitate DIR compliance with the requirements of the DIR Shared Services Contracts, DIR Customer shall provide written interpretation to DIR of any DIR Customer-Specific Law.

### **3.4 DIR Customer responsibilities**

Where appropriate, DIR Customer shall support the following:

- (a) Software currency standards are established for the Shared Services environment through the owner operator governance model. DIR Customers will be engaged in approval of these standards and the development of technology roadmaps that employ these software currency standards. DIR Customers are expected to remediate applications in order to comply with the standards
- (b) Technology standards (e.g. server naming standards, reference hardware architectures, operating system platforms) are established through Shared Services Governance. DIR Customers will adhere to these standards. Any exceptions will follow governance request processes.
- (c) DIR Customer shall ensure network connectivity and sufficient bandwidth to meet DIR Customer's needs.
- (d) DIR Customers will collaborate with SCPs to establish and leverage standard, regular change windows to support changes to enterprise systems. These change windows will be constructed to support varying degrees of service impact, from planned down-time to no service impact. Standard enterprise changes during these windows may affect all systems in one or more of the consolidated data centers simultaneously.
- (e) DIR Customers will support the consolidation of commodity services into shared enterprise solutions that leverage common management and configuration practices delivered by the service providers. Examples of such commodity services are SMTP mail relay and DNS management.
- (f) DIR Customers will support and align with standard enterprise Service Responsibilities Matrixes and associated processes for obtaining an exception or making improvements to the standard enterprise Service Responsibility Matrixes.

### **3.5 DIR Customer Equipment and Facilities**

Any use by SCPs of DIR Customer Equipment and/or Facilities shall be limited to the purpose of fulfilling the requirements of this ILC or the DIR Shared Services Contracts.

DIR Customer will retain ownership of DIR Customer Equipment. DIR Customer shall comply with DIR refresh policies, as amended from time to time by DIR.

### **3.6 DIR Customer Contracts, Leases, and Software with Third Parties**

DIR Customer will make available for use or use its best efforts to cause to be made available for use by DIR and/or SCPs the DIR Customer Contracts and Leases with third parties ("DIR Customer Third Party Contracts and Leases") and DIR Customer third party software ("DIR Customer-Licensed Third Party Software") that pertain to the Shared Services. Any use by DIR and/or SCPs of DIR Customer Third Party Contracts and Leases and/or DIR Customer-Licensed Third Party Software shall be limited to fulfilling the requirements of this ILC or the DIR Shared Services Contracts.

SCPs shall obtain all Required Consents in accordance with DIR Shared Services Contracts. DIR Customer will use its best efforts to assist SCPs to obtain from each Third Party Software licensor the right to use the DIR Customer-Licensed Third Party Software for Services provided under the DIR Shared Services Contracts. Except to the extent expressly provided otherwise and in accordance with the DIR Shared Services Contracts, SCPs shall pay all transfer, re-licensing, termination charges and other costs or expenses associated with obtaining any Required Consents or obtaining any licenses or agreements as to which SCPs are unable to obtain such Required Consents. If requested by DIR, DIR Customer shall cooperate with SCPs in obtaining the Required Consents by executing appropriate DIR approved written communications and other documents prepared or provided by SCPs.

### **3.7 Security**

DIR Customer shall comply with recommended relevant security standards and relevant SCP security guides, as amended from time to time by DIR, the MSI, or the SCP. DIR Customer shall inform DIR as to any DIR Customer specific security considerations.

DIR Customer acknowledges that any failure on its part to follow recommended security standards, policies, and procedures may place its own data and operations at risk as well as those of SCP(s) and other governmental entities. DIR Customer accepts the related potential risks and liabilities that are created by DIR Customer's failure to comply with the recommendations if it is determined such recommendations would have prevented an issue. DIR accepts no responsibility for the risk or liability incurred due to a DIR Customer's decision to not follow DIR's recommendations. SCP will not be liable for violations of security policies and procedures by DIR Customer. Additionally, failure to comply with security standards, policies, and procedures may lead to the suspension or

termination of the availability of certain Applications and services. SCP will give DIR and the DIR Customer notification of non-compliance.

#### **SECTION IV CONTRACT AMOUNT**

In accordance with terms of the DIR Shared Services Contracts, including all relevant pricing and accepted Request for Services proposals, and this ILC, DIR Customer shall be responsible for and agrees to pay DIR the applicable Charges for Services received from the SCPs and the MSI, Services DIR Customer agrees to pre-pay, the DIR recovery fees, any allocated charges, and any Pass Through Expenses incurred by DIR or SCPs on behalf of DIR Customer. The applicable fees are set out in the relevant DIR Shared Services Contracts as incorporated herein and, if applicable, specifically addressed in response to any Request for Services. Certain pricing is based upon DIR Customer's specific consumption; therefore, DIR Customer controls the amounts and duration of the contract amounts. It is understood and agreed that amounts are subject to change depending upon Services required and/or requested and approved and further dependent upon legislative direction and appropriations available for such Services.

Attachment A provides the estimated spend for services as approved by DIR Customer. This form may be revised and updated by DIR Customer as needed without a formal amendment from DIR by DIR Customer submitting to DIR an updated form. DIR Customer must adhere to its own policies and processes for authorizing an adjustment to such amounts internally. DIR Customer is solely responsible for monitoring compliance with Attachment A and to communicate any changes to Attachment A to DIR. DIR shall not be responsible for monitoring or ensuring such compliance.

#### **SECTION V PAYMENT FOR SERVICES**

DIR shall electronically invoice DIR Customer for Services on a monthly basis. Each invoice shall include the applicable monthly charges for Services received from the SCPs, the DIR recovery fees, all allocated charges, and any Pass-Through Expenses incurred by DIR or SCPs on behalf of DIR Customer in accordance with the DIR Shared Services Contracts.

The DIR recovery fees shall be reviewed at least annually in accordance with the requirements for billed statewide central services as set forth in OMB Circular A-87, Cost Principles for State, Local and Indian Tribal Governments (as updated, revised or restated) and other applicable statutes, rules, regulations and guidelines. DIR shall retain documentation for the DIR recovery fees. DIR fees are also determined and reported in accordance with DIR processes and sections 2054.0345-0346 of the Texas Government Code.

Each invoice shall include sufficient detail for DIR Customer to allocate costs to all federal and state programs in accordance with the relative benefits received and to make federal claims according to the federal cost plan of DIR Customer.

In order to allow DIR to meet the statutory payment requirements in Chapter 2251, Texas Government Code, DIR Customer shall make monthly payments by check or Electronic Funds Transfer (EFT) within twenty (20) days following receipt of each invoice from DIR. For purposes of determination of the payment due date, DIR and DIR Customer shall use the date when the invoice is electronically transmitted by DIR to DIR Customer and posted on the chargeback system along with reports that substantiate the service volumes and associated charges. Although cash flow considerations require timely payments as required herein, the rights of DIR Customer and DIR to dispute charges shall be consistent with Texas law.

The MSI SCP is required to develop and maintain a chargeback system. DIR shall coordinate requirements and functionality for the chargeback system with DIR Customer needs and requirements under federal and state requirements for invoiced charges generated through the system. DIR Customer shall utilize this chargeback system to link the designated measurable activity indicators (such as applications or print jobs) with the appropriate financial coding streams. DIR Customer shall update this information monthly, or at such other intervals as are necessary, to enable the MSI SCP to generate accurate invoices reflecting the appropriate distribution of costs as designated by DIR Customer.

DIR Customer is liable for all costs and expenses associated with providing Services under the ILC to the extent such costs and expenses have been incurred by DIR and such Services have been provided to DIR Customer or DIR Customer agrees to pay for such Services prior to receiving them.

Except as allowed in Texas Government Code, Chapter 2251, DIR Customer shall have no right to set off, withhold or otherwise reduce payment on an invoice. In accordance with Texas Government Code, Section 791.015, to ensure enforceability of payment obligations, DIR Customer consents to DIR presenting this ILC and all unpaid invoices to the alternate dispute resolution process, as set forth in Chapter 2009, Texas Government Code. Provided, however, that such consent shall not constitute an agreement or stipulation that Services have been provided or that the invoices are correct. DIR Customer expressly retains all rights to which it is entitled under Texas Government Code, Chapter 2251, in the event of a disagreement with DIR as to whether Services have been provided and accepted or an invoice contains an error.

If DIR Customer disputes an invoice, it shall present the billing dispute in writing directly to the MSI through the Service Catalog within four (4) invoice cycles after the date DIR Customer receives the invoice and reports that substantiate the service volumes and associated Charges from DIR. DIR Customer will provide to the MSI all relevant documentation to justify the billing dispute.

**SECTION VI  
TERM AND TERMINATION OF CONTRACT AND SERVICES**

**6.1 Term and Termination of ILC**

The term of this ILC shall commence upon start of services or execution of this ILC, whichever shall come earlier, and shall terminate upon mutual agreement of the Parties.

This ILC is contingent on the continued appropriation of sufficient funds to pay the amounts specified in DIR Customer's Requests for Services, including the continued availability of sufficient relevant federal funds if applicable. Continuation of the ILC is also contingent on the continued statutory authority of the Parties to contract for the Services. If this ILC is terminated for any reason other than lack of sufficient funds, lack of statutory authority, or material breach by DIR, DIR Customer shall pay DIR an amount sufficient to reimburse DIR for any termination charges and any termination assistance charges incurred under the DIR Shared Services Contracts and this ILC as a result of such termination by DIR Customer. DIR Customer shall provide at least ninety (90) days' written notice to DIR prior to termination. Payment of such compensation by DIR Customer to DIR shall be a condition precedent to DIR Customer's termination.

DIR and DIR Customer acknowledge and agree that compliance with federal law and ongoing cooperation with federal authorities concerning the expenditure of federal funds in connection with the DIR Shared Services Contracts and this ILC are essential to the continued receipt of any relevant federal funds.

**6.2 Termination of Services**

If DIR Customer terminates certain Services, that it requested and approved, for convenience, DIR Customer shall pay the remaining requisite unrecovered costs that have already been incurred prior to the notice of termination, such unrecovered costs will be calculated in accordance with the relevant Shared Services Contract, SMM, or the approved services proposal and related terms. DIR Customer understands that it may not be able to terminate services or receive any refund of a pre-payment after approving the relevant financial solution.

**SECTION VII  
MISCELLANEOUS PROVISIONS**

**7.1 Public Information Act Requests**

Under Chapter 552, Texas Government Code (the Public Information Act), information held by SCPs in connection with the DIR Shared Services Contracts is information collected, assembled, and maintained for DIR. DIR shall respond to Public Information Act requests for SCP information. If DIR Customer receives a Public Information Act request for SCP information that DIR Customer possesses, DIR Customer shall respond



to the request as it relates to the information held by DIR Customer. Responses to requests for confidential information shall be handled in accordance with the provisions of the Public Information Act relating to Attorney General Decisions. Neither Party is authorized to receive or respond to Public Information Act requests on behalf of the other. If SCP or DIR receives a Public Information Act request for information or data owned by DIR Customer, DIR or SCP will refer the requestor to DIR Customer.

## **7.2 Inventory Control**

DIR shall coordinate financial accounting and control processes between DIR Customer and SCPs and ensure inclusion of reasonable control and reporting mechanisms, including any control and reporting mechanisms specifically required by DIR Customer, in the Service Management Manual. Such procedures shall specifically recognize DIR Customer requirements for inventory control and accounting for state owned and leased equipment and facilities, including hardware, software, contracts, and other items of value that may be utilized by, or authorized for use under the direction and control of SCPs.

## **7.3 Confidential Information**

DIR shall require SCPs to maintain the confidentiality of DIR Customer information to the same extent that DIR Customer is required to maintain the confidentiality of the information, and with the same degree of care SCPs use to protect their own confidential information. DIR acknowledges that DIR Customer may be legally prohibited from disclosing or allowing access to certain confidential data in its possession to any third party, including DIR and SCPs. The relevant SMM shall document detailed confidentiality procedures, including the process DIR Customer shall follow to identify confidential information it is legally prohibited from disclosing or allowing access to by DIR and SCPs and including confidentiality procedures required that are specific to DIR Customer. The DIR Shared Services Contracts sets forth the confidentiality obligations of SCPs.

DIR Customer shall notify DIR, in writing, (1) if DIR Customer is a covered entity subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations at 45 Code of Federal Regulations Parts 160 and 164, that is required to enter into a business associate agreement with DIR or SCPs; (2) if DIR Customer receives Federal tax returns or return information; and (3) if DIR Customer is subject to any other requirements specific to the provision of Services. If DIR Customer receives federal tax returns or return information, then DIR Customer must comply with the requirement of IRS Publication 1075 and Exhibit 7 to IRS Publication 1075. In the event a DIR customer is subject to additional requirement as mentioned in this section, DIR shall require SCPs to maintain the confidentiality of DIR Customer information in accordance with language included in Attachment B of this agreement. Such additional requirements as is included in Attachment B of this agreement shall be included in the relevant SMM.

## **7.4 Notification Information**

Contact information for purposes of notification for each Party is set forth below.

DIR Customer's Primary Contact

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Address: \_\_\_\_\_  
Telephone: \_\_\_\_\_  
Email: \_\_\_\_\_

DIR's Primary Contact

sharedservicescontractoffice@dir.texas.gov

The DIR Billing Contact is listed in the DIR Contacts section of the monthly Shared Services Payment Guidance letter, which is provided to the DIR Customer with the monthly Shared Services invoice.

**7.5 Binding Effect**

The Parties hereto bind themselves to the faithful performance of their respective obligations under this ILC.

**7.6 Amendments**

This ILC may not be amended except by written document signed by the Parties hereto or as specified within this ILC or the attachment being amended.

**7.7 Conflicts between Agreements**

If the terms of this Contract conflict with the terms of any other contract between the Parties, the most recent contract shall prevail. This Contract provides a general description of certain terms within the DIR Shared Services Contracts. If the terms of this Contract conflict with the terms of the DIR Shared Services Contracts, the DIR Shared Services Contracts' terms shall prevail. If the terms of this Contract conflict with the terms of an accepted proposal or solution from a Request for Services, this Contract shall prevail.

**7.8 Responsibilities of the Parties**

The Parties shall comply with all federal, state and local laws, statutes, ordinances, rules and regulations and with the orders and decrees of any courts or administrative bodies or tribunals in any manner affecting the performance of the ILC. The parties do not intend to create a joint venture. Each Party acknowledges it is not an agent, servant or employee of the other. Each Party is responsible for its own acts and deeds and for those of its agents, servants and employees. Notwithstanding the foregoing, DIR will cooperate with

DIR Customer in all reasonable respects to resolve any issues pertaining to federal funding in connection with this ILC or the DIR Shared Services Contracts.

DIR and DIR Customer agree that Services contemplated in this ILC shall be governed by provisions in the DIR Shared Services Contracts regarding individual responsibilities of the parties, including Services provided by the SCPs. DIR Customer shall comply with all policies, procedures, and processes in the relevant SMM (s) and as provided by DIR. In the event DIR Customer actions, failure to perform certain responsibilities, or Request for Services result in financial costs to DIR, including interest accrued, those costs shall be the responsibility of DIR Customer. DIR and DIR Customer shall coordinate and plan for situations where conflicts, failure to perform or meet timely deadlines, or competition for resources may occur during the term of this contract. Unless otherwise specifically addressed, the governance process, addressed above, for the DIR Shared Services Contracts shall be used for issue resolution between DIR Customers, DIR and DIR SCPs.

#### **7.9 Audit Rights of the State Auditor's Office**

In accordance with Section 2262.154, Texas Government Code and other applicable law, the Parties acknowledge and agree that: (1) the state auditor, the Parties' internal auditors, and if applicable, the Office of Inspector General of DIR Customer or their designees may conduct audits or investigations of any entity receiving funds from the state directly under the Contract or the DIR Shared Services Contracts, or indirectly through a subcontract under the DIR Shared Services Contracts; (2) that the acceptance of funds directly through this Contract or indirectly through a subcontractor under the Contract acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, the Parties' internal auditors, and if applicable, the Office of Inspector General of DIR Customer or their designees to conduct audits or investigations in connection with those funds; and (3) that the Parties shall provide such auditors or inspectors with access to any information considered relevant by such auditors or inspectors to their investigations or audits.

#### **7.10 General Terms**

Except as expressly provided herein, no provision of this ILC will constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies or immunities available to DIR Customer. The failure to enforce or any delay in the enforcement of any privileges, rights, defenses, remedies, or immunities available to DIR Customer by law will not constitute a waiver of said privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. Except as expressly provided herein, DIR Customer does not waive any privileges, rights, defenses, remedies or immunities available to DIR Customer.

This Customer Agreement will be construed and governed by the laws of the State of Texas. Venue for any action relating to this Customer Agreement is in Texas state courts in Austin, Travis County, Texas, or, with respect to any matter in which the federal courts have exclusive jurisdiction, the federal courts for Travis County, Texas.

If one or more provisions of this ILC, or the application of any provision to any Party or circumstance, is held invalid, unenforceable, or illegal in any respect, the remainder of this ILC and the application of the provision to other Parties or circumstances will remain valid and in full force and effect.

**Signatory Warranty**

Each signatory warrants requisite authority to execute the ILC on behalf of the entity represented.

**SECTION VIII  
CERTIFICATIONS**

The undersigned Parties hereby certify that: (1) the matters specified above are necessary and essential for activities that are properly within the statutory functions and programs of the affected agencies of State Government; (2) this ILC serves the interest of efficient and economical administration of State Government; and (3) the Services, supplies or materials in this ILC are not required by Section 21, Article 16 of the Constitution of Texas to be supplied under contract given to the lowest responsible bidder.

**IN WITNESS WHEREOF**, the Parties have signed this ILC effective on date of last signature below.

**RECEIVING ENTITY: XXXX**

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**PERFORMING AGENCY: DEPARTMENT OF INFORMATION RESOURCES**

By: \_\_\_\_\_

Printed Name: Sally Ward

Title: Director, Program Planning and Governance

Date: \_\_\_\_\_

Legal: \_\_\_\_\_

DIR Contract No. \_\_\_\_\_

**Attachments to ILC**

Attachment A Estimated Spend Form – (Customer may provide Attachment A to DIR if required by their processes.)

Attachment B Additional Confidentially Requirements – (As necessary and described in Section 7.3, Confidential Information)

**Attachment A**  
**Estimated Spend Form**

\*This form is to be used as needed by the DIR Customer to capture spend within the Shared Services Program. This amount may be based upon the DIR Customer's biennial budget(s).

Below are the estimated spend amounts for certain DIR Shared Services received through this ILC and may change based upon DIR Customer consumption. This amount is to be managed and monitored solely by the DIR Customer. Amounts may be transferred by the DIR Customer that change this amount. Such increases or decreases are strictly within the control of the DIR Customer.

DIR Customer is required to pay for any costs incurred in accordance with this ILC and the related DIR Shared Services Contracts regardless of the estimated spend amounts reflected herein.

Updates to this form may be executed through written notice by the DIR Customer to DIR.

Costs, such as incremental network expenses, which are billed directly to or paid by the DIR Customer, are not included in these amounts.

For the period MONTH DAY, YEAR through MONTH DAY, YEAR the estimated spend is \$XX,XXX as the spend applies to \_\_\_\_\_ Services.

DIR Customer acknowledges and agrees that the responsibility to manage, monitor, and change the amounts contained in this form are the sole responsibility of the DIR Customer. Further, each signatory warrants requisite authority to execute any changes to this Attachment A in accordance with the DIR Customer's applicable approval processes.

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

DIR Contract No. \_\_\_\_\_

**Attachment B**  
**Additional Confidentiality Requirements**

None

**AT&T Tracking Number**  
**WO Number:**

**S**

**Vendor:** AT&T  
**Customer:**  
**WO Number:**  
**Request Title:** Solution Design - MSS - MSSTEST  
**Request Number:**  
**AT&T Tracking Number:**  
**Date of Submission:** March 5, 2019

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement. Version 1.0*

*© 2017 AT&T Intellectual Property. All rights reserved.*



**AT&T Tracking Number**  
**WO Number:**

**Table of Contents**

1.	<b>Scope</b> .....	1
2.	<b>Service Descriptions</b> .....	2
3.	<b>Customer Responsibilities</b> .....	2
4.	<b>Assumptions</b> .....	3
5.	<b>Services Out of Scope</b> .....	4
6.	<b>Use of Personal Systems</b> .....	4
7.	<b>Communications Plan</b> .....	4
8.	<b>Escalation Process</b> .....	4
9.	<b>Initiation of Work</b> .....	5
10.	<b>Schedule and Expected Duration</b> .....	5
11.	<b>Confidentiality</b> .....	5
12.	<b>Acceptance Criteria</b> .....	6
13.	<b>Resource Management</b> .....	6
14.	<b>Risks</b> .....	6
15.	<b>Change Order Process</b> .....	7
16.	<b>Engagement Contacts</b> .....	7
17.	<b>Appendix A: Election Security Assessment Service Details</b> .....	8
18.	<b>Appendix B: Definitions</b> .....	15

**CONFIDENTIAL INFORMATION**

**AT&T Tracking Number**  
**WO Number:**

**1. Scope**

The scope of the service being offered is detailed in the table below:

Service	Scope
Election Security Assessment (ESA)	Thorough review of Elections Processes, Procedures, Technology and Staff to provide concerns and recommendations to improve the security of the elections process for a Customer (County). The ESA includes a site visit by one or more cybersecurity professionals to perform a holistic compliance, vulnerability and security assessment of the entire elections process.

**CONFIDENTIAL INFORMATION**

**AT&T Tracking Number**  
**WO Number:**

## **2. Service Descriptions**

### Election Security Assessment

The Election Security Assessment (ESA) provides a thorough assessment of the policies, process, technology and staff involved in the elections process at the County level. This assessment will provide an onsite assessment team to carefully review all practices of the Election team and provide analysis on areas of risk, as well as recommendations for specific improvements that should be made to improve the security and perception of security within the County. The ESA is performed by trained cybersecurity experts and is assessed versus the NIST Cyber Security Framework (CSF).

The following deliverables are provided as the output of the ESA Process to the County.

- Election Security Assessment (ESA) Scorecard
- Election Security Assessment (ESA) Report

The ESA Scorecard provides the County with a 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. 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.

The service is offered jointly by AT&T and its Election Security Assessment partner, CyberDefenses. Throughout this document, references to AT&T refer to the joint partnership between AT&T and CyberDefenses.

The ESA is targeted specifically for Counties that provide Elections to their local communities. Throughout this document, the term County and Customer are used interchangeably and refer to the Elections department within a County that would be assessed as a part of an ESA service.

Through acceptance of this document, the Customer acknowledges that a security assessment will be performed on County resources. While reasonable steps will be taken to minimize impact on the provided resources, it is possible that normal operation of technology may be impacted by through these activities. Throughout the assessment process, the ESA team will work closely with Customer staff to monitor and detect if assessment activities are affecting the normal, and take steps to help resolve any concerns. Whenever possible, such impacts will be minimized and/or coordinated with Customer staff.

## **3. Customer Responsibilities**

The Customer agrees to provide timely access to all personnel, resources, and requested information that is deemed necessary to fulfill its commitments stated herein. AT&T will make reasonable efforts to provide lead-time to the Customer.

The Customer also specifically agrees to:

- Provide Executive sponsorship within the County. This sponsorship will include notifying appropriate internal and external organizations of this engagement and requesting their full cooperation.
- Assign a Single Point of Contact (SPOC) to represent the County's election effort. The SPOC will have decision-making authority for most matters that may arise.
- Make the SPOC available to meet with AT&T for regular status meetings.
- Ensure that the individuals responsible for the managing Elections within the County are prepared to constructively engage with the assessment.
- If the County manages Voter Registration independently from the Elections, the County must ensure the leadership that manages Voter Registration is prepared to constructively engage in the ESA process.
- Provide support from IT professionals that manage the systems and networks related to elections.
- SPOC, and representation from Elections, Voter Registration and IT Support will participate in the ESA Kickoff meeting.
- Schedule and support a site visit, where cybersecurity experts will interview the team and access all related Elections systems.

### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

- During the site visit, the County will provide access to the Election organization's facilities, including storage and preparation facilities for any devices involved in the voting process.
- County will interface with vendors of software or hardware that are currently used by the Elections organization to encourage them to provide risk information to AT&T, if necessary.
- Provide input to and acceptance of service timelines and deliverables.
- Provide timely access to staff and personnel to answer questions.
- Inform AT&T of any developments in other projects that might impact this engagement.
- Provide AT&T with the necessary physical and/or system access complete job functions.
- Provide IP Addresses and/or web addresses (URLs) for devices and external applications/websites that will be assessed for vulnerabilities.
- Provide scheduled windows in which external election website & application may be scanned for vulnerabilities.
- Obtain authorization from any hosting, cloud or other third-party provider prior to AT&T testing any devices or services under their control.
- Include in Customer's emergency contact list staff capable of administering the Customer's computer systems and who are on 24-hour notification during the delivery of the Service.
- Customer IT will place AT&T's IP address ranges in the Customer's non-shun list (whitelist) within Customer's firewall or IDS/IPS prior to starting the vulnerability assessment.

If the Customer fails to perform any of the responsibilities set forth herein, the parties agree to resolve the situation via a mutually agreeable change order process. The receiving Party shall issue a written response within five (5) working days of the receipt of the request, indicating whether the receiving Party accepts or rejects the change(s). Notwithstanding the foregoing, neither of the parties is bound to use the Change Order Process in the event of a material breach by the other party.

**4. Assumptions**

The assumptions and dependencies below were used by AT&T to scope this engagement based on information provided to it by the Customer. If any of these items prove to be invalid, the parties agree to resolve the situation via the Change Order Process. Notwithstanding the foregoing, neither of the parties is bound to use the Change Order Process in the event of a material breach by the other party.

- The Customer will be responsible for ensuring that all necessary personnel are available to AT&T in a timely manner and ensure cooperation of vendors and partners as needed.
- The Customer will identify and provide stakeholders responsible for providing information and interfacing with the AT&T team.
- The Customer will need to confirm the availability of any key team members during service initiation.
- The Customer will provide AT&T with all relevant documentation and information relevant to efforts for services.
- AT&T assumes that there will not be any special conditions or restrictions that would affect a productive workday.
- The Customer's personnel will be cooperative and forthcoming with information.
- The Customer's other vendors and their personnel will be cooperative and forthcoming with information.
- All items listed in the Customer Responsibilities section of the SPP are met, delivered, or provided (as appropriate) in a timely manner.
- Documentation from AT&T will be furnished using MS Office products (Word, Excel, PowerPoint, Project, Visio) as appropriate.
- All devices that needed to be assessed (described within this document) will be provided by the customer.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

**5. Services Out of Scope**

The following activities are out of scope for this effort. AT&T will not provide as part of this effort:

- Remediation for security incidents
- Onsite support for helpdesk and other IT Infrastructure related support
- Forensic analysis for security incidents
- Monitoring for network related services
- Infrastructure management and support beyond those items identified *Section 1. Scope.*
- Project management or vendor management, other than AT&T vendors and personnel, outside the scope of services

Out of scope services can be added at any time by submitting a new Request for Service.

**6. Use of Personal Systems**

If the County currently allows the use of personal systems in the elections process, then it will also be required that those system will be considered in the ESA Process. If the personal system is determined to house sensitive information surrounding the election or to be a critical element of the elections process, the Assessor may request to evaluate and/or scan that system.

In order for that system to be evaluated, the owner of that system will be required to first sign a release, which will provide a legal structure in which the device may be reviewed. If the owner is unable to consent to the review of the device and provide appropriate access credentials, then the risk of the unmanaged and unsecured device will be included in the ESA deliverables.

**7. Communications Plan**

Reports

Reports will be delivered via a customer portal

Ad Hoc Communications

The SPOCs will define the situations where AT&T personnel will be able to contact Customer personnel without the need to document these conversations.

**8. Escalation Process**

Both parties agree to use the following escalation process when a situation arises that either party feels could jeopardize the overall success of the engagement. Either party may initiate the escalation process, by contacting the named individual at the top of the table. If the initiating party feels that the situation hasn't been adequately resolved; isn't being resolved quickly enough; or is of sufficient magnitude to cause significant damage to the overall relationship, they may proceed along the escalation path, as they deem appropriate. Initiation of this process is restricted to the individuals that are named in the escalation path for their party.

AT&T Escalation Path

Title	Name	Phone Number
ATT Program Manager	Daniel Weiske	(720) 481-7918
Program Manager	Maria Acosta (subcontractor)	(737) 205-7057
Account Manager	Ray Via	(571) 292-6499
Regional Services Manager	Mia Stovall Grove	(512) 750-7211

Customer Escalation Path

Title	Name	Phone Number

**CONFIDENTIAL INFORMATION**

This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.  
Version 1.0

**AT&T Tracking Number**  
**WO Number:**

Escalations of a more tactical nature will be handled between the AT&T Engagement Manager and the appropriate SPOC serving as an escalation point.

Security Incidents

If, in the course of the assessment, a critical cybersecurity incident is suspected, the Assessor and/or Engineer will immediately perform an initial review of the suspected incident and provide all relevant information and recommended next steps to County authorities immediately. AT&T will also be notified of the Incident and all relevant details to help support the Customer in forming an immediate action plan.

If the details of the security incident provide a potential threat or impact to an organization outside of the County, then any subcontractors and AT&T will be required to notify the Texas Secretary of State and potentially additional authorities, as described in the **Confidentiality** Section of this document.

**9. Initiation of Work**

AT&T's ability to provide resources will be based on:

- AT&T's acceptance of the customer request
- The customer's approval of the request
- The availability of resources at the time of request

AT&T requires up to four (4) business weeks after the approved SPP is received to provide resources to the Customer. The start of any specific resource under this SPP must be mutually agreed to by AT&T and the Customer.

**10. Schedule and Expected Duration**

Within one week of receipt of the Request for Solution (RFS), AT&T (or any subcontractors) will contact the Customer to confirm the scheduled timeline and the target dates for the Site Visit.

If the Customer can support it, the ESA Kick-off Meeting will be schedule within 10 working days of receipt of order.

The ESA Site Visit will occur at a time mutually agreed upon between AT&T and the Customer. Once the Site Visit has occurred and all relevant information collected by AT&T, the ESA Deliverables will be provided to the Customer within 30 working days.

**11. Confidentiality**

The artifacts collected and the deliverables of the Election Security Assessment (ESA) are considered confidential to the County, unless a specific incident is discovered that has a direct impact on organizations or individuals outside of the County.

AT&T will generate the ESA Scorecard and the ESA Report and they may be reviewed for quality or correctness by AT&T. The results of any specific County will not be delivered to the Texas Department of Information Resources (DIR) or the Texas Secretary of State (SoS). The ESA deliverables are excepted from Public Information Requests because these documents specifically include information regarding security vulnerabilities (Texas Government Code 552.139).

If a security incident is discovered during the assessment that has an impact on individuals or organizations outside of the County, then AT&T is required to notify the Secretary of State's office and/or other appropriate authorities, depending on the details of the incident.

If AT&T identifies child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110, in conducting the activities described in this SPP, AT&T shall report such to the Customer's Executive Director or highest-level executive and an appropriate law enforcement agency and shall provide the law enforcement agency with access to the offending material. If AT&T identifies information that it perceives as a serious threat to human life or safety in conducting the activities described in this SPP, AT&T shall report such threat to an appropriate law enforcement agency and the Customer's Executive Director or highest-level executive.

Aggregated results will be delivered to the SoS once a sufficient number of counties have been evaluated that will allow for a reasonable level of anonymity. Any information that might help to identify a specific County will be withheld to protect the anonymity of any specific County's results.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

## **12. Acceptance Criteria**

Upon receipt of the ESA Scorecard and the ESA Report and any other deliverable required under this SPP, the Customer will have ten working days to request clarification and/or updates. Where needed, updates or clarifications will be provided within ten business days or as quickly as possible. The Customer will be given ten working days from the receipt of each respective update or clarification to request additional updates or clarification until the Customer is satisfied that the deliverable complies with the standards in this SPP. If the Customer receives the deliverables and does not respond with either acceptance or requests for updates for a period of ten (10) working days, then the deliverables will be considered accepted by the Customer.

If the Customer and AT&T reach a point where AT&T cannot agree to provide additional updates or clarification, and the Customer is not satisfied that the deliverable complies with the standards in this SPP, the Customer shall utilize the Escalation Process contemplated in Section 8 of this SPP, and, if that does not result in a deliverable which the Customer believes is compliant with this SPP, the matter shall be referred by the Customer to DIR and resolved by DIR and AT&T pursuant to the dispute resolution procedures set forth in Article 19 of the Master Services Agreement between DIR and AT&T, DIR-MSS-SCP-001.

Each County choosing to participate in the ESA program will execute, among other things, a separate Inter-local contract ("ILC") with DIR; however, any provisions in each respective ILC (including, but not necessarily limited to, portions of Sections V, VI, and VII of each respective ILC) do not apply to the ESA Program to the extent they conflict with this SPP and the addendum to the Inter-agency Contract, DIR-SS-IAC0031, between SoS and DIR ("IAC") relating to the ESA Program. In addition, any provisions in the IAC (including, but not necessarily limited to, portions of Sections V, VI, and VII of the IAC) do not apply to the ESA Program to the extent they conflict with the addendum to the IAC and this SPP.

Once updates or clarifications are provided to the Customer's satisfaction or the deliverable is otherwise considered to be accepted following the aforementioned dispute resolution process, then the review process is considered completed and final. DIR and/or AT&T shall notify SoS that the review process is complete, and DIR may invoice SoS for the services provided to the Customer. No invoice shall be issued by DIR, and no payment shall be made by SoS, for a Customer, unless and until the current documentation workflow for that Customer, as referenced in Amendment 1 to the IAC, is substantively followed and the ESA Program services are considered to be accepted by that Customer in accordance with this section.

## **13. Resource Management**

AT&T reserves the right to assign resources based on AT&T's understanding of the technical requirements and AT&T resource availability. The Customer agrees that all AT&T contractors are acceptable for this project.

AT&T will follow the Customer's policies when working at the Customer's facilities so long as such policies do not violate applicable state or federal law. This includes but is not limited to issues such as dress code, workplace conduct and security.

## **14. Risks**

AT&T has identified the following potential risks in being able to complete this engagement. If any of these risks are in danger of occurring, AT&T shall invoke the Escalation Process. If any of these risks do occur, the parties agree to resolve the situation via the Change Order Process. Notwithstanding the foregoing, neither of the parties is bound to use the Change Order Process in the event of a material breach by the other party.

- Uncooperative Customer personnel or other entities (e.g. they won't provide information, provide incorrect or incomplete information, hinder progress of AT&T resources, etc.).
- Inability to travel due to government action (such as grounding of airlines).
- Delays in accessing network devices, systems, locations, documentation and people who are vital during the engagement.
- Delays in receiving Customer IP address ranges and/or URLs that are vital during the information collection phase of this project.
- The receipt of inaccurate information regarding the design and configuration as provided by the Customer or its third-party resources.
- Prolonged network outages that limit the access to in-scope devices.
- The active shunning of AT&T's security testing IP addresses by the Customer or its third-party resources.

### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

Should any of these risks occur and cannot be resolved within the duration window of the ESA, then the relevant sections of the ESA deliverables will reflect that some information was not available and the associated Risk Level, Concerns and Recommendations will reflect that not all information was provided.

**15. Change Order Process**

The parties agree that this SPP may be amended by a Change Order Form prepared by AT&T and signed by both parties for one or more of the following reasons:

- The occurrence of any of the Risks.
- The invalidation of any of the Assumptions.
- Failure of the Customer to meet its Customer Responsibilities.
- Failure of AT&T or any subcontractors to complete the ESA.
- Changes in the Description of Work or Deliverables requested by the Customer and agreed to by AT&T.
- The occurrence of any other event or the discovery of any other information that affects AT&T's ability to perform the engagement as specified herein.
- Any other mutually agreeable reason.

The remedy to any of the above may include changes to: the composition of the engagement team and/or duration. If the remedy to any of the above includes changes to the pricing, AT&T must obtain approval for changes to the pricing from DIR and SOS.

AT&T will obtain the necessary approvals, signatures and, if required, a purchase order from DIR and Customer for any additional costs. AT&T will return the form signed by DIR to Customer, who will countersign the form, distribute it to the appropriate parties.

Whenever there is a conflict between the terms of a fully executed Change Order Form and those in this SPP, or a previous fully executed Change Order Form, the terms of the most recent fully executed Change Order Form shall prevail.

**16. Engagement Contacts**

AT&T Consulting

Election Security Assessment Services Manager  
NAME: Daniel Weiske  
PHONE: (720) 481-7918  
EMAIL: daniel.weiske@att.com

**CONFIDENTIAL INFORMATION**



**AT&T Tracking Number**  
**WO Number:**

**17. Appendix A: Election Security Assessment Service Details**

The following sections outline the specific activities that will be included within the Election Security Assessment service.

The Customer workflow process is designed to facilitate the collection of **Artifacts**. An artifact is any piece of information that helps the Assessor to determine the current state of the organization. An artifact can be information that is obtained from a Customer through observation, verbally or through provided documents. An artifact can also be the result of technical scans that reveal information about specific systems or technology. For the purposes of categorization, AT&T will be working to obtain the following types of Artifacts throughout the ESA.

- **Provided Artifacts:** These artifacts represent information that is stored and needs to be collected from the Customer. Common examples are written policies & procedures, org charts, lists of product vendors, email addresses, domains and IP address ranges. Where possible, if the Customer can collect and deliver the Provided Artifacts, then the Site Visit can be shortened. If it is not reasonable, then the Assessor will work with the Customer staff to collect the Provided Artifacts during the site visit.
- **Interview Artifacts:** These artifacts represent information that is not collected in documents and needs to be verbally gathered by the Assessor. Interview Artifacts will typically be gathered in-person, though could be performed via conference call, if necessary. Interview Artifacts will typically be gathered in the form of notes taken by the interviewer. In some cases, Interview Artifacts are gathered by having the Engineer or Assessor review the activities of an individual that is executing specific policies.
- **Scanned Artifacts:** Scanned Artifacts will be collected through the use of technology, such as vulnerability or malware scanning tools, and the inspection of systems or networks.
- **Intelligence Artifacts:** Intelligence Artifacts are gathered through investigation of the internet, darknet and/or individuals that are outside the elections organization. Examples of intelligence artifacts might be information that is being sold on the darknet that relates to the Customer, such as stolen usernames/passwords.

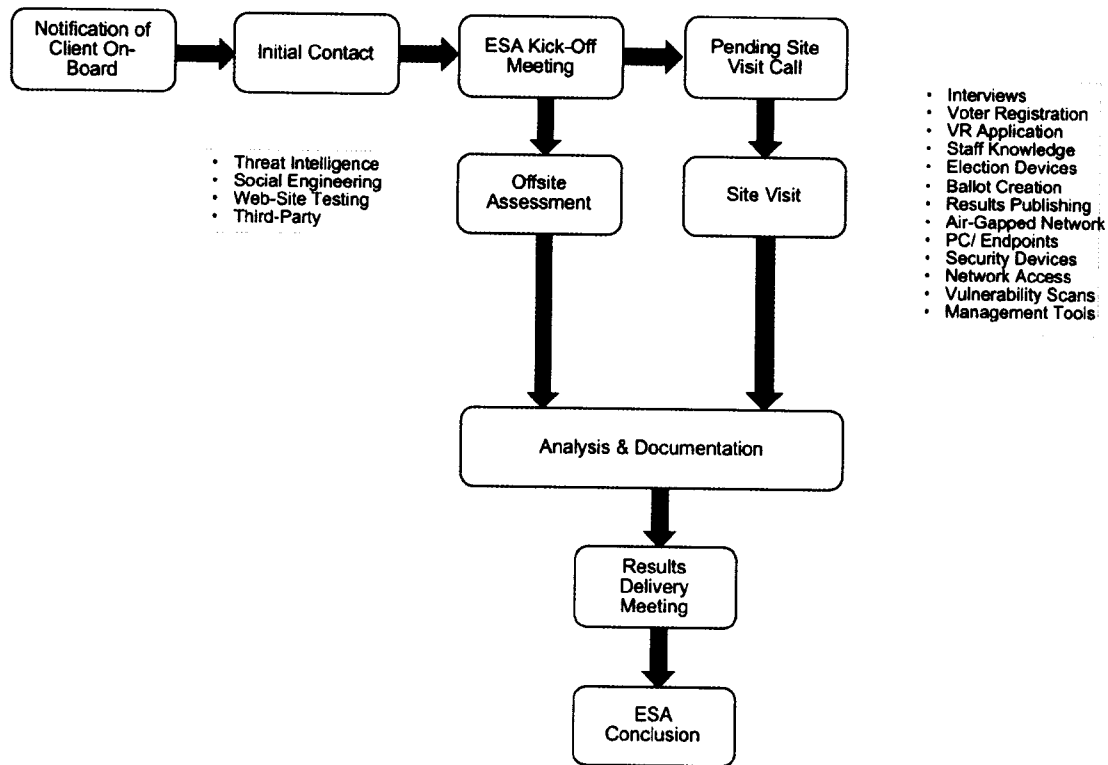
All of the following steps in this workflow will facilitate Artifact collection. The Artifacts are then reviewed and analyzed to provide the resulting reports.

The figure below describes the expected Customer interaction workflow for the ESA. Each stage in the workflow is described in more detail in the following sections.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

AT&T Tracking Number  
WO Number:



ESA Workflow

### Initial Contact

Within three working days, the Program Manager will make Initial Contact with the Primary point of contact by phone, if possible, and provide them with the necessary steps to set up the Election Security Assessment Kick-Off Meeting to accomplish the following objectives:

- Confirm the key roles that will participate in the entire ESA process and Kick-Off meeting
- Identify the time of the Election Security Assessment Kick-off meeting to occur within two weeks, unless the Customer requests a later date and time
- Describe a very high-level outline of the site visit activities, contributions needed from the Customer and expectations to help prepare the Customer for the assessment
- Begin the process to identify a tentative date for the ESA Site Visit.

### Election Security Assessment Kick-off Meeting

The Election Security Assessment Kick-off meeting is a critical event in the ESA process and requires that one representative from each important role be present. The meeting will be delayed until a time when all critical roles can participate, assuming that they exist within the Customer's organization. The three critical roles are:

- Administrator of Election
- Administrator of Voter Registration
- IT staff (County or Election)

The following roles will participate from the assessment team. Additional team members from DIR and AT&T may also contribute, dependent upon the Customer's specific requirements.

- Program Manager
- Lead Assessor

### **CONFIDENTIAL INFORMATION**

This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.

**AT&T Tracking Number**  
**WO Number:**

The following activities will occur on the ESA Kick-off meeting. The ESA Kick-Off will typically be held as a conference call, though could be scheduled as an onsite meeting if requested by the Customer.

- Introduction of all team members
- Short overview of the ESA Process and expectations of participants
- Review of the Site Visit planned activities and confirmation of the following details:
  - AT&T will require access to:
    - All required systems, even if they are in storage.
    - The required samples of devices (such as DREs, Pollbooks, scanners, etc) and to the workspace where devices are prepared.
    - Networks and Domains to perform required tasks
    - Air-gapped networks
  - Customer team will be present and available for interviews, including
    - Administrator of Election
    - Administrator of Voter Registration
    - County and Elections IT Staff
    - Staff members that are familiar with the use of:
      - Election Management System
      - Electronic poll book or paper poll book generation
      - Ballot creation system
      - Vote capture devices
      - Vote tabulation
      - Results Publication
      - Current security practices

The Customer will be notified that social engineering efforts will begin immediately and may continue until the final report is delivered. The Customer will be requested to identify any calendar time-blocks where such efforts would be inappropriate or may slow or impact the elections process.

A contact will be identified to coordinate scheduling of vulnerability testing efforts of external websites.

Discussion of required Provided Artifacts and whether the Customer is able to provide any in advance. If the Customer is able to support the collection of the Provided Artifacts in advance, then access to the ESA secure portal will be granted.

Pending Site Visit Call

As the ESA Site Visit date approaches, the Program Manager will schedule a call to occur approximately two weeks before the visit. This call will include at least the Primary Point of contact but may also include the other organizational leaders. In this call, the Program Manager will review the plan for the site visit and re-confirm the dates and availability of required resources.

Site Visit

Every ESA will include a Site Visit that will involve one to four cybersecurity experts visiting the County and all relevant sites, depending on the size of the elections operation. Once on-site the following activities will be performed by the Assessor(s) and/or Engineer.

The visiting ESA team will utilize a digital camera to collect relevant photographic evidence of the facility and any visually identified artifacts.

*Interview Process*

The purpose of the Interview Process is to explore the Customer's elections processes and cybersecurity operations. Interviews with Elections and Voter Registration leadership are used to establish the governance, oversight, and management of risk as it relates to elections cybersecurity. Interviews with County Information Technology personnel are used to explore the IT functions provided to the elections department and how County technology services relate to cybersecurity capabilities. Interviews will also include security personnel in counties that have staff dedicated to the areas of cybersecurity.

**CONFIDENTIAL INFORMATION**

**AT&T Tracking Number**  
**WO Number:**

*Voter Registration System*

In Texas, voter registration is managed with a centralized application, TEAM. TEAM supports two common models of Voter Registration (VR), Online and Offline. For each of the models, users of the Customer's VR system will be asked to demonstrate common activities.

*VR Application Storage*

Texas law requires that each Customer store the original registration application submitted by a voter, according to specific retention requirements. The ESA Assessor will review the storage process and confirm that proper access controls and encryption levels are used throughout the transmission and storage of the application. If applications are stored in paper format, the practices for collecting and processing applications from digital sources will be inspected.

*Staff Security Knowledge*

The ESA team will hold short interviews with one to three staff members to assess general knowledge of security principals and to understand the level of security knowledge of the elections staff. Staff will also be asked to describe the staff and volunteer training process, specifically as it relates to the security of the election.

*Election Devices*

A sample of every device that is used as a part of the election process will be evaluated for proper security controls. Prior to arrival, the ESA team will request access to at least two of each type of the following devices that might be used at the Customer:

- Digital-Recording Equipment (DRE)
- Scanners (both Precinct and Central)
- Ballot Marker
- Computers that are specifically used at polling locations, commonly pollbook software
- Computers that are specifically used on a non-internet connected networks
- Tablets or Phones that are specifically used at polling locations

*Ballot Creation Process & Tools*

The Elections leadership (and/or staff members) will be requested to walk the ESA Assessor through the procedures and practices involved in the creation, verification, distribution and usage of Ballots. This will include the management and programming of the ballots throughout the early voting process and election day. Every point where the ballot is digitally stored or transmitted will be considered for security and verified by the Engineer, if possible.

For cases where external software programs or contract vendors are used for ballot programming, the external company will be requested to respond to a third-party risk assessment.

*Results Publication Process & Tools*

The Elections leadership (or a delegate) will be requested to walk the ESA Assessor through the procedures and practices involved in collecting the result of an election from the tabulation system and posting the results to the Secretary of State or to any of the Customer's publication mechanisms (such as websites).

*Non-Connected Network & System*

The ESA team will perform a limited penetration test on any air-gapped network that is used within the elections process. This effort will confirm that the air-gapped network is configured correctly and that network access is completely disabled. A monitoring device will be deployed on the air-gapped network to confirm that no external traffic is probing the controlled network. Systems on the air-gapped network will be manually inspected to insure proper configuration and security measures are in place.

*General Computer / Endpoints*

Every computer that is involved in the elections process and generally available during the Site Visit will be accessed and tools will be executed to determine the following:

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

- Is endpoint security software present and configured properly?
- Is malware or suspicious software present?

Remotely executed tools will be used to evaluate security of the devices, executed remotely whenever possible (using Admin access over a domain). If remote access is not available, the Engineer will briefly access each computer to run the required scans and perform the appropriate manual inspection. This process creates Scanned Artifacts that contribute to the overall analysis effort.

*Security Devices*

The Assessment Engineer will work with the County or Election IT staff to identify all security devices (firewalls, URL filters, behavioral detection, etc) and review their configuration and logs to understand the full network protection provided to the elections network. In some cases, the devices will be employed only at the Customer network access points and they will still be evaluated for proper protection configuration and usage.

*Internet Connected Election Network*

The Engineer will work closely with the IT Staff (County or Elections) to determine the optimal placement for network analysis tools within the environment. These tools will optimally be placed at a network ingress/egress point. If network access point cannot be monitored, the tools can be placed in front of key servers.

The Engineer will provide the necessary monitoring appliance and required network tap(s) to allow visibility without interrupting network traffic. The appliance will deploy IDS and Behavioral detection technologies for a period of at least 24 hours and record the results.

*Network Access*

The ESA team will work with the County IT staff to identify each area where devices may be added to the network. These ingress/egress points are often defined as links to the internet, as network access ports or the wi-fi network. The Engineer will evaluate each of those points for proper physical and network access controls, dependent upon the technologies used.

The networking plan in use for polls and early voting will also be analyzed and evaluated, if possible.

*Vulnerability Detection*

The ESA team will deploy a network appliance that will be used to perform a vulnerability scan of each computer or supporting information technology devices that are associated with the election and/or voter registration process and are network accessible.

*Management Tools*

Products (devices or applications) that are used to support the general management of the election process will be identified and visually inspected to determine the security capability and current usage of those devices. In most cases, these products will include the County or elections organization's email system, file servers and any collaboration and/or distributed program management tools.

*Maintenance and Remote Support*

The ESA team will evaluate any vendor maintenance capabilities and remote support mechanisms for information technology devices and elections functions to ensure that access is appropriately limited to authorized personnel, properly protected to ensure that unauthorized access is prohibited, and established with audit trails and attribution to identify remote access and associated maintenance activities.

The ESA team will look for records that establish authorized vendors and corresponding personnel as well as inspect the methods used for equipment maintenance and remote support. Maintenance and remote access interfaces will have a limited test conducted to verify protections are effective.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

Off-Site Assessment Activity

Off-site Assessment activity refers to Artifact collection that does not require the assessment team to be at the Customer site. The activities will occur at a time that is convenient for the assessment team, but before the final analysis is complete and delivered to the Customer. Whenever direct interactions are required with the Customer (or Customer systems), the Program Manager will schedule the activity with the Customer.

*Threat Intelligence*

As soon as the Customer is able to provide confirmation of their IP Address ranges and internet domains (Provided Artifacts), AT&T will schedule the Intelligence Sub-Assessment. This effort will engage expert cybersecurity analysts in the effort of scanning the internet and darknet (criminal elements of the internet) for any of the following:

- Hacker communication that may impact the County or election
- Activity on the darknet that may indicate that information has been stolen from the Customer or a Customer's partner
- Collection of all Intelligence Artifacts on the darknet that can be associated with the Customer. For example, stolen accounts (from other companies/orgs) that may provide clues on how to access the Customer resources
- Attacker activity that may focus on the Customer's specific region

The Threat Intelligence Assessment does not require any interaction from the Customer and will not directly impact their ongoing activities. If a critical security incident is discovered, the Customer will be notified immediately. All discovered Intelligence Artifacts will be considered in the generation of the final ESA Scorecard and ESA Report.

*Social Engineering*

The ESA Team will undergo efforts to use social engineering in attempts to determine whether the staff uses common security principals when responding to requests for sensitive voter or elections information. Social Engineering attempts will include (but is not limited to) sending of phishing email and phone calls from individuals pretending to request protected information. Social Engineering phone calls to the Customer's staff will be recorded.

The results of the Social Engineering efforts are cataloged and treated as Scanned Artifacts.

Through the acceptance of this document, the Customer is acknowledging that the AT&T staff will contact the elections staff, pretending to be individuals that they are not, and attempt to retrieve information that should not be provided by Customer staff. Any information that is collected through these efforts will be treated confidentially.

*External Web-site Vulnerability Testing*

Each external website used by the Customer for any specific elections purpose will be evaluated to determine if it is currently compromised, if there are any indicators of past compromises and whether current application vulnerabilities make it susceptible to attack.

Web application vulnerability scans and analysis will be used. Limited efforts to penetrate existing security controls will be used to ensure that basic security constructs are in place. This test does not intend to provide a full cybersecurity penetration test of the application, though the Customer's processes will be evaluated to ensure that annual security assessments of all external interfaces are included.

*Third-party Risk Assessments*

Each outsourced and third-party vendor provided product that a Customer uses as a critical element of the elections infrastructure will be identified and the ESA Team will engage with the vendor to perform a risk assessment of that application. In some cases the ESA Team may require assistance from the Customer to obtain responses to the assessment request. The Risk Assessment will present the vendor with a focused questionnaire that will assess the vendor's adherence to NIST CSF principals and industry best practices. Whenever possible, the risk assessment will be performed prior to the site visit so that any specific configuration practices might be evaluated.

Analysis and Documentation

Following the collection of the Artifacts, the AT&T team will be able to perform analysis and generate the findings and deliverables. The analysis effort happens continuously throughout the collection process but is primarily focused on the period of time following the Site Visit until the final deliverables are presented.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

*Cybersecurity Capability*

The ESA will evaluate the Customer's ability to perform activities within the NIST CSF functions and the level of maturity for ongoing cybersecurity operations. Using Provided Artifacts that include reports, procedure documents, and other outputs that are related to each of the associated activities, assessors will use the information to focus interview questions for sessions with key personnel during the on-site visit. Assessors will measure the maturity of capabilities using a capability/maturity scale. Capabilities are also validated using the Scanned Artifacts produced during the technical testing where possible.

The analysis is then compiled and scored using the ESA methodology to provide the capability scorecard summary and key recommendations for high risk areas where maturity is lacking or performing at low levels.

*Findings and Recommendations*

Through the analysis argument, each Artifact will be reviewed by ESA Analysts and a set of findings (concerns) will be documented. Each finding will be assigned a recommendation to address the concern with an appropriate level of maturity, given the current security level of the Customer.

Findings will be presented in the ESA Scorecard and ESA Report across the entire organization and also broken down across each of the eight areas of elections focus:

- Elections Management
- Election Team Support
- Voter Registration
- Pollbook / Voter Check-in
- Ballot Creation & Distribution
- Vote Capture (Paper or DRE)
- Vote Tabulation (Manual and/or Automated)
- Election Results Publishing (locally and to SoS)

*Risk Assessment*

ESA Analysts will process all findings and assign each a value to determine the impact that issue may have on the Customer and the overall probability that the issue may happen. Based upon these values each concern is assigned a risk level:

- Critical
- High
- Medium
- Low

Each area of the election (described above) is provided a Risk Level and the entire organization is assigned an overall Risk Level. These results are reported in both the ESA Scorecard and Report.

Delivery of Results

As the analysis effort is nearing completion, the Program Manager will contact the Primary Point of Contact for the Customer and schedule the Delivery of Results meeting. This meeting will typically be held as a conference call to review the ESA Scorecard and some of the key findings. This meeting will represent the first time the Customer has seen the results.

In this meeting, the ESA Lead Assessor will review the structure of the results and each of the key findings and discuss recommendations for improvements. The Customer will be provided with access to a secure portal to download the delivered reports and will be advised on mechanisms to protect the contents of the deliverables. A member of the sales team will also be available to discuss next steps, should the Customer wish to engage in resolving the concerns with the same team.

The Customer will be advised that they have five working days to review the results and request clarification and/or updates.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

**AT&T Tracking Number**  
**WO Number:**

## 18. Appendix B: Definitions

### Customer Roles:

**Administrator of Elections** - A general term that refers to a County employ that has the responsibility of managing the elections process.

**Administrator of Voter Registration** - A general term that refers to a County employ that has the responsibility of managing the voter registration efforts for the County.

**County IT Staff** - Many counties provide IT services for the election organization. The County IT Staff provides host, network and/or applications support across a large number of County departments, often including Elections.

**Election IT Staff** - Many elections organizations retain IT staff to directly support the technology requirements of the election infrastructure.

### Assessment Roles

**Assessor** – A cybersecurity risk assessment expert that has the role of collecting Provided Artifacts and Interview Artifacts.

**Engineer** – A technical cybersecurity expert that has the role of working with the Customer's technology to collect Scanned Artifacts and the ESA.

**Lead Assessor** – The lead of the ESA Team who will serve as the primary liaison throughout the Site Visit and through the ESA process. In most cases, there is only a single Assessor, who also serves as the Lead Assessor.

**Program Manager** – Manages the schedule and the process of delivering the ESA to the Customer. The Program Manager serves as a point of contact for the Customer and coordinates all aspect of providing the service.

**Sales** – Members of the AT&T Sales team members will a serve top help inform each Customer about the assessment and facilitating the sign-up process

### Terminology

**Artifact** - Piece of data or indicator of activity that contributes information to the ESA process and is used to help assess the risk and security preparedness of each Customer.

**County** - This term refers to the government responsible for managing the business of a specific County.

**Customer** - This general term is used to refer to the organization that is undergoing the assessment. In the case of the Election Security Assessment, the Customer is typically the County's election organization(s).

**Cyber Security Framework (CSF)** – A CSF consists of standards, guidelines, and best practices to manage cybersecurity-related risk.

**Darknet** – The darknet represents a small portion of the internet that is not accessible via normal internet search and access methods. Adversaries use this hidden area of the internet to communicate and coordinate activity that might be considered criminal and often to sell or trade information that is gathered through criminal activities

**Intelligence Artifact** – Piece of data or literature that was generated through research that was performed outside of the Customer's staff or systems.

**Inter-Local Contract (ILC)** – The ILC is a legal document that must be executed between the County and the Texas Department of Information Resources (DIR) that provides the legal framework in which the ESA will be provided.

**Interview Artifact** – Piece of data or literature that was generated through discussion or communication with an individual within the Customer.

**NIST CSF** – The NIST Cyber Security Framework is a CSF that is authored by the National Institute of Standards and Technology that provides a basic framework managed cybersecurity-related risk.

**Vulnerability Testing** – The technical effort of evaluating a specific system or network to identify known issues with the software or hardware that may allow an adversary to access that system.

**Phish** – To request confidential information under false pretenses, usually done via the Internet (email), phone or social media.

**Provided Artifact** – Piece of data or indicator (artifact) provided by the customer.

**Scanned Artifact** – Data found via scanning with assessment tools or through manual inspection of technology.

**Scan** - A test of capabilities, usually aimed to find areas of vulnerability or to define capability.

### **CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*



**AT&T Tracking Number**  
**WO Number:**

**Security Incident** – The determination by a security analyst that an investigated Security Alert meets the criteria of the defined Security Incident classification policy and which generates notification to the Customer.

**Social Engineering** - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

**Vulnerability** - A weakness that can be exploited by an adversary that wishes to access systems or technology that they would otherwise not have access to.

**CONFIDENTIAL INFORMATION**

*This SPP, its INFORMATION, and its use are subject to the terms and condition of the Master Services Agreement.*

Version 1.0

Page 16

© 2018 AT&T Intellectual Property. All rights reserved.



# DIR Shared Services New Customer Form

- Please fill out the below information to establish your DIR Shared Services account.
- E-mail completed form (with W-9 if you are not a state agency) to [DIRSharedServices@dir.texas.gov](mailto:DIRSharedServices@dir.texas.gov)
- Upon receipt of your information, a DIR representative will contact you to set up your Interagency Contract (IAC) and gather any additional required information.

You may tab from one field to the next.

## General Information and Eligibility

The DIR Shared Services Program is available to all state agencies and other governmental entities. If not a state agency, please attach W-9 with this form to confirm your eligibility.

Agency or Organization Name: Johnson County

Agency or Organization Acronym: \_\_\_\_\_

Comptroller Taxpayer ID Number: 75-6001030

Type of Government Entity: County

Six Digit Agency Code (if Applicable): N/A

## Customer Contacts

### IAC Contact

The IAC contact will be responsible for reviewing and signing the IAC between your organization and DIR.

Name: Roger Harmon

Title: County Judge

Address: #2 N Main St.

Cleburne, TX. 76033  
(City),(State) (Zip)

Telephone Number: (817) 556-6360 Ext: \_\_\_\_\_

E-mail: countyjudge@johnsoncountytexas.org

### Secondary IAC Contact (EA)

Name: Patty Bourgeois

Title: Elections Administrator

Address: 103 S Walnut St.

Cleburne, TX. 76033  
(City),(State) (Zip)

Telephone Number: (817) 556-6197 Ext: \_\_\_\_\_

E-mail: pattyb@johnsoncountytexas.org

### Tertiary IAC Contact (VR)

Name: N/A

Title: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Telephone Number: \_\_\_\_\_

E-mail: \_\_\_\_\_



# DIR Shared Services New Customer Form

## IT Operations Contact

The IT Operations Contact will be responsible for providing technical information to set up your services and will act as the day to day Customer Representative, including requesting/approving services through the online Portal, after services are established.)

Same as Main Contact

Name: Dan Milam,  
 Title: IT Director  
 Address: 2 N Mill St.  
Cleburne, TX 76033  
(City),(State) (Zip)  
 Telephone Number: (817) 556-6366 Ext: \_\_\_\_\_  
 E-mail: dmilam@johnsoncountytexas.org

## Primary Finance Contact

The Primary Finance contact will be responsible for reviewing invoices, including accessing the online billing system, and ensuring payment is submitted timely.

Same as Main Contact

Name: N/A  
 Title: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 \_\_\_\_\_  
 Telephone Number: \_\_\_\_\_  
 E-mail: \_\_\_\_\_

## DIR Shared Services

Select the DIR Shared Services you are currently interested in:

- |                                                                           |                                                                 |
|---------------------------------------------------------------------------|-----------------------------------------------------------------|
| <input type="checkbox"/> Email (Microsoft Office 365)                     | <input type="checkbox"/> Disaster Recovery as a Service (DRaaS) |
| <input type="checkbox"/> Microsoft Custom Support Agreement               | <input type="checkbox"/> Print/Mail                             |
| <input type="checkbox"/> Managed Services – Server and Storage            | <input type="checkbox"/> Backup as a Service (BUaaS)            |
| <input type="checkbox"/> Managed Services – Application Development/Maint | <input type="checkbox"/> Managed Services - Security            |

Indicate any additional DCS services you may be interested in:

- |                                                                |                                                                 |
|----------------------------------------------------------------|-----------------------------------------------------------------|
| <input type="checkbox"/> Email (Microsoft Office 365)          | <input type="checkbox"/> Google Imagery                         |
| <input type="checkbox"/> Managed Services – Server and Storage | <input type="checkbox"/> Backup as a Service (BUaaS)            |
| <input type="checkbox"/> Managed Services – Mainframe          | <input type="checkbox"/> Disaster Recovery as a Service (DRaaS) |
| <input type="checkbox"/> Print/Mail                            | <input type="checkbox"/> Etc.                                   |

Thank you for your interest in the Texas Shared Services Program. Please email this form to [DIRSharedServices@dir.texas.gov](mailto:DIRSharedServices@dir.texas.gov) and we will contact you to set up your IAC, gather information about your environment, and discuss the steps to initiate service.

