Texas Election Security Assessment

Provided by Texas Secretary of State

The Security Assessment Designed for Election Leadership

Texas Secretary of State is providing advanced and comprehensive election security assessments for counties in Texas

The Texas Election Security Assessment provides:

- Onsite visit by Elections Security Experts to collect all necessary information
- All systems and processes related to elections will be evaluated and tested for security issues or compliance concerns
- Review of darknet and Internet for active threats
- Review of election processes & procedures for security concerns
- Specific recommendations provided in non-technical language
- All results are delivered to the county confidentially and not shared with Texas SoS
- Access to additional services through Texas DIR Managed Security Services to address issues

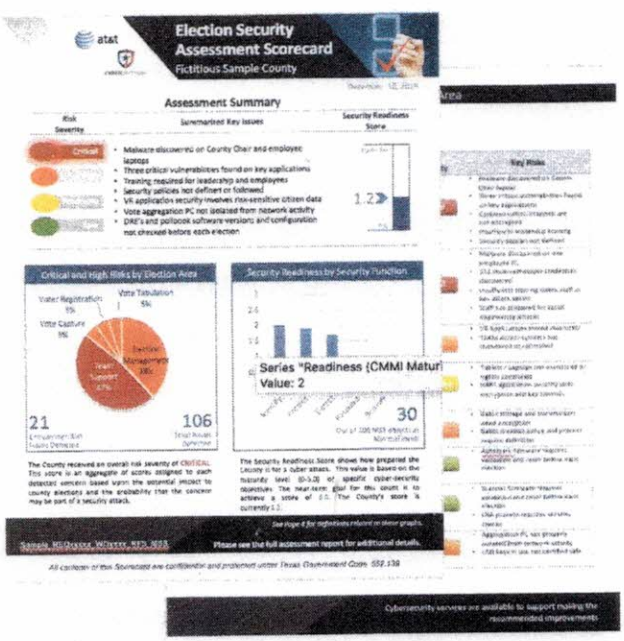
Participating counties receive:

Election Security Scorecard

- Comprehensive Risk Level
- Security Readiness Grade
- Key Risks and Recommendations
- Designed for Election Leadership

Detailed Technical Report

- Details of Risks and issues
- Detailed Recommendations
- Designed for IT Professionals



Contact DIRSharedServices@dir.texas.gov to sign up today.

Signing up for an Elections Assessment

To order your Advanced and Comprehensive Cybersecurity Assessment you must register as a DIR Managed Security Services client.

Register for DIR Shared Services Program

- Contact DIRSharedServices@dir.texas.gov to become customer
- Complete and submit a New Customer Form, the following happens in parallel:
  - Sign an Inter-Local Contract (ILC) and agree to the Managed Security Services terms and conditions for the Shared Services
  - DIR will submit your initial request
  - Customers will get onboarded to the Shared Services portal

The following additional cybersecurity services are offered through DIR Shared Services

Security Monitoring and Device Management (SMDM)

SMDM manages and monitors security devices in your environment. SMDM services include:

- Endpoint Management System
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Host-Based Intrusion Detection System (HIDS) / Host-Based Intrusion Prevention System (HIPS)
- Malware Detection Systems / Malware Prevention Systems
- Managed Firewall Services
- Managed Web Application Firewall (WAF) Services
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC) Services
- Threat Research

Incident Response

Incident Response assists you in the event of a security incident in your IT environment. Incident Response services include:

- Security Incident Management
- Digital Forensics
- Incident Response Preparedness

Risk and Compliance

Risk and Compliance assists you in identifying, remediating, monitoring, and managing enterprise risks. Risk and Compliance services include:

- Penetration Testing
- Risk Assessment
- Cloud Compliance Assessment
- Vulnerability Scanning
- Web Application Scanning

Cybersecurity services are available to support you in making the recommended improvements.

AT&T CYBERDEFENSES

Election Security Assessment Scorecard

Fictitious Sample County – July 12, 2018 Revision 1.0

Election Security Assessment

Risk Severity	Key Concerns	Security Readiness Score
Critical High Moderate Low	• Malware discovered on County Chair and employee laptops • Three critical vulnerabilities found on key applications • Indicators of activist attack targeting region found on darknet • Training required for leadership and employees • Security policies not defined or followed • VR application security involves risk-sensitive citizen data • Vote aggregation PC not isolated from network activity	2.6 Maturity Level

Critical & High Risks by Elections Area

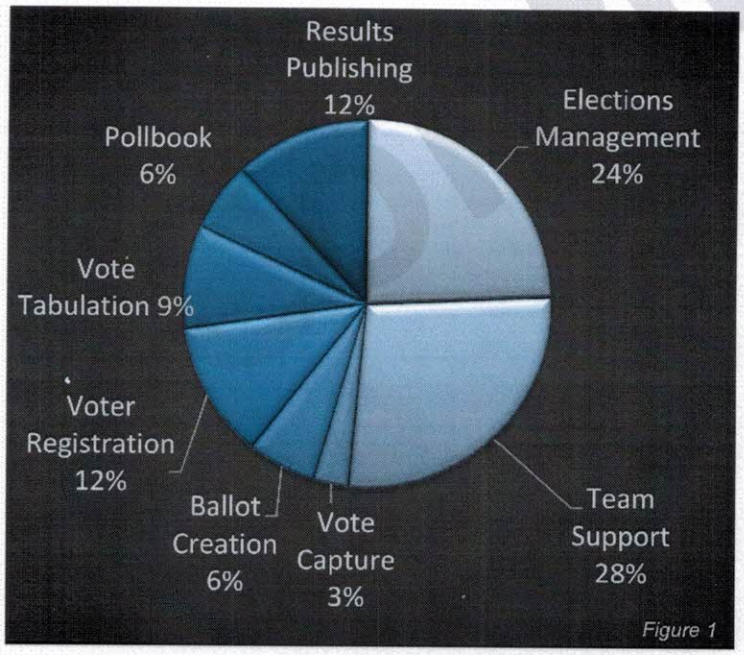


Figure 1

Critical/ High Risks Discovered: 33
Total Risks: 112

Cyber Security Objective Maturity Levels

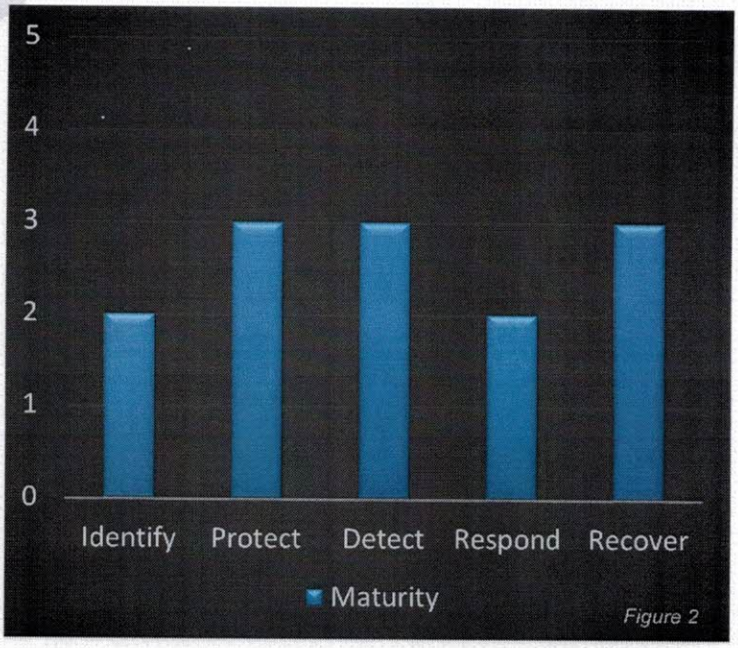


Figure 2

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

AT&T CYBERDEFENSES

Scorecard Per Elections Area

Fictitious Sample County, Texas

Elections Area	Description	Risk Severity	Key Risks
Election Management	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.	Critical	• Malware discovered on County Chair laptop • Three critical vulnerabilities found on key applications • Communication channels are not encrypted • Insufficient leadership training • Security policies not defined
Election Team Support	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.	Critical	• Malware discovered on one employee PC • 312 stolen employee credentials discovered • Insufficient training opens staff as key attack vector • Staff not prepared for social engineering attacks
Voter Registration	The County supports voter registration through the online use of TEAM. Applications are stored on a single Windows File Server.	High	• VR Applications stored insecurely • TEAM Access systems not monitored or controlled
Pollbook / Voter Check-in	ePollbook support and voter check-in managed via HART application using user county provided tablets and laptops. Voter information in ePollbook is not sensitive.	Moderate	• Tablets / Laptops not monitored or tightly controlled • HART application security lacks encryption and key controls
Ballot Creation & Distribution	Ballot design process performed in scanner vendor tools. Ballot distribution handled via email.	High	• Ballot storage and transmission need encryption • Ballot creation policy and process require definition
Vote Capture	Vote Capture is performed via paper ballot marking and in some precincts supported by Automark Ballot Markers	Low	• Automark firmware requires validation and reset before each election
Vote Tabulation	Vote tabulation supported by M100 and M650 scanners	Low	• Scanner firmware requires validation and reset before each election • LNA process requires security checks
Election Results Publishing	Elections results taken from scanner and aggregated on single air-gapped PC. Results transferred to SoS and County website via USB.	High	• Aggregation PC not properly isolated from network activity • USB keys in use not certified safe

Cybersecurity services are available to support making the recommended improvements

AT&T CYBERDEFENSES

Key Recommendation Summary

Fictitious Sample County, Texas

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

AT&T CYBERDEFENSES

Methodology and Definitions

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
Critical	High	High
High	Moderate High	High Moderate
Moderate	Moderate	Moderate
Low	Moderate Low Low	Low Moderate 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

Texas Election Security Assessment

Provided by Texas Secretary of State

The Security Assessment Designed for Election Leadership

Texas Secretary of State is providing advanced and comprehensive election security assessments for counties in Texas

The Texas Election Security Assessment provides:

- Onsite visit by Elections Security Experts to collect all necessary information
- All systems and processes related to elections will be evaluated and tested for security issues or compliance concerns
- Review of darknet and Internet for active threats
- Review of election processes & procedures for security concerns
- Specific recommendations provided in non-technical language
- All results are delivered to the county confidentially and not shared with Texas SoS
- Access to additional services through Texas DIR Managed Security Services to address issues

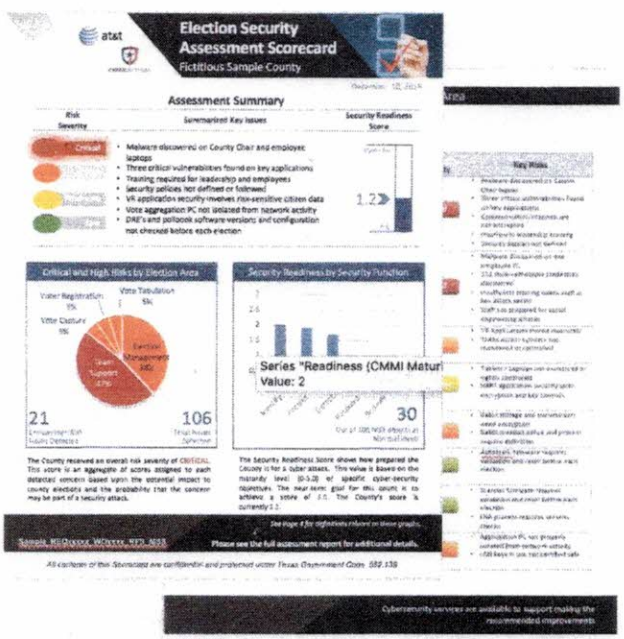
Participating counties receive:

Election Security Scorecard

- Comprehensive Risk Level
- Security Readiness Grade
- Key Risks and Recommendations
- Designed for Election Leadership

Detailed Technical Report

- Details of Risks and issues
- Detailed Recommendations
- Designed for IT Professionals



Contact DIRSharedServices@dir.texas.gov to sign up today.

Signing up for an Elections Assessment

To order your Advanced and Comprehensive Cybersecurity Assessment you must register as a DIR Managed Security Services client.

Register for DIR Shared Services Program

- Contact DIRSharedServices@dir.texas.gov to become customer
- Complete and submit a New Customer Form, the following happens in parallel:
  - Sign an Inter-Local Contract (ILC) and agree to the Managed Security Services terms and conditions for the Shared Services
  - DIR will submit your initial request
  - Customers will get onboarded to the Shared Services portal

The following additional cybersecurity services are offered through DIR Shared Services

Security Monitoring and Device Management (SMDM)

SMDM manages and monitors security devices in your environment. SMDM services include:

- Endpoint Management System
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Host-Based Intrusion Detection System (HIDS) / Host-Based Intrusion Prevention System (HIPS)
- Malware Detection Systems / Malware Prevention Systems
- Managed Firewall Services
- Managed Web Application Firewall (WAF) Services
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC) Services
- Threat Research

Incident Response

Incident Response assists you in the event of a security incident in your IT environment. Incident Response services include:

- Security Incident Management
- Digital Forensics
- Incident Response Preparedness

Risk and Compliance

Risk and Compliance assists you in identifying, remediating, monitoring, and managing enterprise risks. Risk and Compliance services include:

- Penetration Testing
- Risk Assessment
- Cloud Compliance Assessment
- Vulnerability Scanning
- Web Application Scanning

Cybersecurity services are available to support you in making the recommended improvements.