Texas Department of Information Resources

DIR Mission
To serve Texas government by:
• Leading the state's technology strategy,
• Protecting state technology infrastructure, and
• Offering innovative and cost-effective solutions for all levels of government.

DIR Vision
Transforming How Texas Government Serves Texans
87th Session State Affairs Committee Technology and Cybersecurity Bills

HB 1118 (Capriglione/Paxton)
SB 475 (Nelson/Capriglione)
HB 1118 (Capriglione/Paxton)

Relating to state agency and local government compliance with cybersecurity training requirements.

• Requires cybersecurity training for elected and appointed officials who have access to the computer system or database and use a computer for at least 25 percent of their required duties.

• Requires local governments to submit written certification of cybersecurity training completion when applying for Governor’s Division of Criminal Justice grants.

• Requires non-compliant local governments to pay back Criminal Justice Division grants and makes them ineligible for additional Criminal Justice Division grants for two years.

• Requires agencies to include completion of training certification in their strategic plan.

DIR implementation:

• Updated training requirements on DIR website.

• Added grant and strategic plan requirement language to training confirmation email sent to state agencies.

• Developed system for OOG to verify cybersecurity training completion.
SB 475 (Nelson/Capriglione)

Relating to state agency and local government information security, including establishment of the state risk and authorization management program and the Texas volunteer incident response team.

A comprehensive data security, data management and cybersecurity bill that strengthens the state’s standards on agencies’ data management practices, storage, and Texas’ ability to respond to cybersecurity incidents that creates:

- Texas Risk Authorization and Management Program
- State Agency Data Management Advisory Board and Data Management Officers
- Texas Volunteer Incident Response Teams
- Regional Cybersecurity Working Groups
- Regional Security Operation Center
- SB 475 also directs state agencies to consider using robotic process automation and prohibits state agencies from collecting biometric identifiers without consent.
SB 475: DIR Implementation of Cyber Initiatives

**Texas Risk Authorization and Management Program (TX-RAMP)**
- DIR board adopted rules (TAC 202.27 and 202.770) and program manual to establish program in December 2021.
- Certified 754 products as of April 25.

**Texas Volunteer Incident Response Teams (VIRT)**
- VIRT program manual and application published on DIR’s website in December 2021.
- Started recruiting volunteers with three cyber experts now on-board.

**Regional Cybersecurity Working Groups**
- Mutual aid agreement framework published on DIR’s website in December 2021.

**Regional Security Operation Center**
- Released Expression of Interest Document to public universities on January 7. Six responses received by February 28.
- Angelo State University selected as pilot partner.
Cybersecurity Overview
State of Texas – Information Technology (IT)

Texas’ Federated Model

- Agencies are responsible for their own IT and the security of their systems, applications, and the data they hold.
- Agencies have requirements to report to DIR as promulgated in Texas Government Code Chapter 2054 and Texas Administrative Code 202.
- DIR has responsibility for the state network as promulgated in Texas Government Code Chapter 2059.
## A Few of DIR’s Security Offerings

<table>
<thead>
<tr>
<th>Offerings</th>
<th>Local Government</th>
<th>State Government</th>
<th>Higher Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy &amp; Security Controls Catalog</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>InfoSec Academy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>End-User Security Awareness Training</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Multifactor Authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Information Security Forum</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vulnerability Scans &amp; Penetration Tests</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Assessments</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Statewide Data Center and Technology Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network Security Operations Center (NSOC)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Detection and Response</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
DIR Information Security

Office of the Chief Information Security Officer (OCISO)
- Information security leadership, policy, direction, education, awareness, reporting, and statewide initiatives

Cybersecurity Coordination
- Texas Cybersecurity Council

Cybersecurity Operations (CyOps)
- Network security monitoring, intrusion prevention services, alerting, incident response guidance, and threat analysis for state agency customers
### What OCISO Does

#### Governance, Risk, and Compliance
- TAC 202 and Security Controls Catalog
- Texas Cybersecurity Framework
- TX-RAMP
- Security Planning and Reporting
- SPECTRIM

#### Security Operations
- Volunteer Incident Response Team (VIRT)
- Cybersecurity Incident Response Team (CIRT)
- Regional Security Operations Center (RSOC)
- Statewide Incident Response Coordination

#### Security Services
- Security Training
- Assessments and Pen Tests
- Information Security Forum
- Shared Technology Services Security
- Multi-Factor Authentication

#### Cybersecurity Coordination
- Texas ISAO and Threat Reporting
- Public and Private Sector Collaboration
- Statewide Security Awareness Training
- Cybersecurity Council
Network Security Operations Center – Cyber Operations

Texas Government Code §2059

- Created the Network and Security Operations Center (NSOC) at DIR to provide state agencies network security and incident response for network security incidents.

Cyber Operations at the NSOC

- Block malicious traffic.
- Alert agencies to suspicious outbound traffic.
- Detect and mitigate Distributed Denial of Service (DDoS) attacks.
- Support agency incident investigations and incident response efforts.
- Analyze reported suspicious emails and attachments for malware / phishing.
- Provide oversight of Shared Technology Services (STS) security operations.
- Intelligence gathering and sharing.
# Overview of 2021 Global Cyber Activity

<table>
<thead>
<tr>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>December</td>
<td>January</td>
</tr>
<tr>
<td>SolarWinds:</td>
<td>Database: Data breach</td>
</tr>
<tr>
<td>Supply Chain</td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Governor Greg Abbott’s Letter

February 25, 2022

Governor Greg Abbott directs DIR and DPS to use every available resource to safeguard the state’s critical infrastructure and to assist local governments and school districts with their needs.

- Enhance Texas’ cyber security using best industry practices and other key measures.
- Ensure Texas can quickly detect a potential cyber intrusion using software services, such as antivirus and endpoint detection and response technologies.
- Prepare for an intrusion by utilizing a cyber incident response team.
- Maximize the state’s resilience to a destructive cyber incident.

Geopolitical Tensions

Cyber Operations Countermeasures Enacted:

- Active bi-directional intelligence sharing with federal, state, and industry partners.
- Increased aggressive blocking.
- Lowering of standard thresholds for threat notification and investigation of suspicious activity.
- On-going advanced threat hunting operations in the state's data centers and Network Security Operations Center (NSOC).
- Communication channels established with response teams and intelligence partners.
## Ransomware Trends

### Ransomware Attacks since 2019 by Government Type

<table>
<thead>
<tr>
<th>Organization Type</th>
<th>Number of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cities</td>
<td>35</td>
</tr>
<tr>
<td>Counties</td>
<td>17</td>
</tr>
<tr>
<td>School Districts</td>
<td>43</td>
</tr>
<tr>
<td>Other Local Entities</td>
<td>11</td>
</tr>
<tr>
<td>State Agencies</td>
<td>5</td>
</tr>
<tr>
<td>Institutions of Higher Education</td>
<td>8</td>
</tr>
</tbody>
</table>
Nationwide Cybersecurity Review

Overview

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of state, local, tribal and territorial (SLTT) governments’ cybersecurity programs.

The NCSR is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF provides a common language for understanding, managing, and expressing cybersecurity risk. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and align policy, business, and technological approaches to managing risk. Learn more at https://www.nist.gov/cyberframework/framework.
# Nationwide Cybersecurity Review

<table>
<thead>
<tr>
<th>SCORE</th>
<th>MATURITY LEVEL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Optimized</td>
<td>Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.</td>
</tr>
<tr>
<td>6</td>
<td>Tested and Verified</td>
<td>Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.</td>
</tr>
<tr>
<td>5</td>
<td>Implementation in Process</td>
<td>Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.</td>
</tr>
<tr>
<td>4</td>
<td>Partially Documented Standards and/or Procedures</td>
<td>Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.</td>
</tr>
<tr>
<td>3</td>
<td>Documented Policy</td>
<td>Your organization has a formal policy in place that has been approved by senior management.</td>
</tr>
<tr>
<td>2</td>
<td>Informally Done</td>
<td>Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.</td>
</tr>
<tr>
<td>1</td>
<td>Not Performed</td>
<td>Activities, processes, and technologies are not in place to achieve the referenced objective.</td>
</tr>
</tbody>
</table>
Nationwide Cybersecurity Review – 2021 Results

Peer Profile NCSR Results

NIST CSF Function

State of Texas

NCSR Maturity Level - Average Score

5.46  6.09

NIST CSF Function

State Peer Profile

NCSR Maturity Level - Average Score
# Measuring Maturity Through the Texas Cybersecurity Framework

### Identify
- Forty-Two Security Objectives
  - Privacy and Confidentiality
  - Data Classification
  - Critical Information Asset Inventory
  - Enterprise Security Policy, Standards, and Guidelines
  - Control Oversight and Safeguard Assurance
  - Information Security Risk Management
  - Security Oversight and Governance
  - Security Compliance and Regulatory Requirements Management
  - Cloud Usage and Security
  - Security Assessment and Authorization / Technology Risk Assessments
  - External Vendors and Third-Party Providers

### Protect
- Enterprise Architecture, Roadmap, and Emerging Technology
- Secure System Services, Acquisition, and Development
- Security Awareness and Training
- Privacy Awareness and Training
- Cryptography
- Secure Configuration Management
- Change Management
- Contingency Planning
- Media
- Physical Environmental Protection
- Personnel Security
- Third-Party Personnel Security
- System Configuration Hardening and Patch Management
- Access Control
- Account Management
- Security Systems Management
- Network Access and Perimeter Controls
- Internet Content Filtering
- Data Loss Prevention
- Identification and Authentication
- Spam Filtering
- Portable and Remote Computing
- System Communications Protection
- Information System Currency

### Detect
- Malware Protection
- Vulnerability Assessment
- Security Monitoring and Event Analysis
- Audit Logging and Accountability

### Respond
- Cybersecurity Incident Response
- Privacy Incident Response

### Recover
- Disaster Recovery Procedures
# Security Maturity Levels

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>DIR Description</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>There is no evidence of the organization meeting the objective.</td>
<td>None, Nonexistent</td>
</tr>
<tr>
<td>1</td>
<td>The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.</td>
<td>Ad-hoc, Initial</td>
</tr>
<tr>
<td>2</td>
<td>The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.</td>
<td>Managed, Consistent, Repeatable</td>
</tr>
<tr>
<td>3</td>
<td>The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.</td>
<td>Compliant, Defined</td>
</tr>
<tr>
<td>4</td>
<td>The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.</td>
<td>Risk-Based, Managed</td>
</tr>
<tr>
<td>5</td>
<td>The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.</td>
<td>Efficient, Optimized, Economized</td>
</tr>
</tbody>
</table>
State-wide Maturity Average by Functional Area

- DIR has been measuring maturity since 2014.
- There has been improvement each biennium.
- The general cybersecurity maturity level for state government is Level Three “Compliant.”
- Education Service Centers and Public Junior Colleges recently began participating in the assessments.
- As entities have focused on the framework security objectives, maturity has improved.
Functional Area and Overall Maturity 2014 - 2020 (State Agencies/Higher Education)
Local Entity Maturity Rating

**Elections Maturity**
- DIR worked with the Secretary of State to perform maturity assessments with county election officials.
- Average maturity for all counties is low.

**Local Maturity**
- Local entities not required to report to DIR.
- Discussions with local entities reflects that size and budget influence maturity, and the elections ratings are a fair assessment.
# Texas Cybersecurity Regulatory Coverage

<table>
<thead>
<tr>
<th></th>
<th>State Agencies</th>
<th>IHEs</th>
<th>Junior Colleges</th>
<th>Cities</th>
<th>Counties</th>
<th>K-12</th>
<th>Private Sector</th>
<th>Critical Infra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Laws &amp;</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Texas Law</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>DIR/State CISO</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Texas Admin Code 202</td>
<td>✅</td>
<td>✅</td>
<td></td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Tools &amp;</td>
<td>✅</td>
<td>✅</td>
<td></td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Required Reporting of Cyber Incidents

<table>
<thead>
<tr>
<th>Applies to</th>
<th>What</th>
<th>Reports to</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>State agencies and Institutions of Higher Education</td>
<td>Breach of system security that involves sensitive personal information</td>
<td>Department of Information Resources • Secretary of State if it involves election data • Office of Attorney General if it involves more than 250 people</td>
<td>Government Code Section 2054.1125 (See also Texas Administrative Code 202.23 and 202.73)</td>
</tr>
<tr>
<td>Businesses that own, license, or maintain computerized data that includes sensitive personal information</td>
<td>Breach of system security that involves sensitive personal information</td>
<td>Office of Attorney General if it involves more than 250 people</td>
<td>Business and Commerce Code Section 521.053</td>
</tr>
<tr>
<td>School districts</td>
<td>A cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security</td>
<td>Texas Education Agency</td>
<td>Education Code Section 11.175</td>
</tr>
<tr>
<td>County election officer</td>
<td>A breach of cybersecurity that impacts election data</td>
<td>Secretary of State *(must notify House and Senate Elections Committees)</td>
<td>Election Code CH 279</td>
</tr>
</tbody>
</table>
Local Government Needs

- **Additional Training**
- **Qualified Personnel**
  - Can’t afford and/or recruit qualified staff
- **Resources**
  - “Who do I ask for help if I can’t afford background checks?” – County official
Thank You

dir.texas.gov
#DIRisIT
@TexasDIR