

# THE TEXAS STATE-LEVEL ISAO

**PROMOTING PRIVATE-SECTOR CYBERSECURITY CAPABILITIES THROUGH STATE-LEVEL CYBER THREAT INFORMATION SHARING AND ANALYSIS**

ERNESTO BALLESTEROS, JD, MS, CISSP, CISA, SECURITY+  
STATE CYBERSECURITY COORDINATOR OF TEXAS



Office of the  
CHIEF INFORMATION  
SECURITY OFFICER  
State of Texas



Texas Department of Information Resources

- **Section 1: Introduction and Background Information**
- **Section 2: Advancing Public Sector Cyber Capabilities**
- **Section 3: Advancing Private Sector Cyber Capabilities**
- **Section 4: Looking Forward**

# SEC. 1: INTRODUCTION

## EXPERIENCE

- **State Cybersecurity Coordinator**, Texas Department of Information Resources (Austin, Texas)
- **Information Security Auditor**, CPS Energy (San Antonio, Texas)
- **Director**, The Center for Information Assurance Management and Leadership (a nationally recognized NSA/DHS Center for Academic Excellence in Cyber Defense Education)
- **Assistant Professor of Computer Information Systems and Security**, Our Lady of the Lake University \*NSA/DHS CAE-CDE (San Antonio, Texas)
- **Information Security Officer**, Jefferson Bank (San Antonio, Texas)
- **Information Security Consultant**, Omnikron Systems, Inc. (Los Angeles, California)

## EDUCATION

- **Law School**: Doctor of Jurisprudence (IT, Intellectual Property, and Privacy Law)
- **Graduate School**: Master of Science, Computer Information Systems and Security
- **Undergraduate**: Bachelor of Science, Computer Information Systems and Security

## PROFESSIONAL CERTIFICATIONS/LICENSES

- **Computer Information Systems Security Professional** (CISSP ID: 307695)
- **Certified Information Systems Auditor** (CISA ID: 17136337)
- **Security+** (ID: COMP001005265111)



## The Problem: Hardening Private Sector Security

### Increasingly Sophisticated Cyber Threats

- “Cybersecurity threats continue to evolve and are outpacing Texas organizations’ ability to protect the state’s cyber environment, compromising the **physical safety**, **financial security**, and **privacy** of Texas citizens.” (“**Building a More Secure and Prosperous Texas**,” 2012, p. 1)

#### HACKTIVISTS

Conduct attacks in furtherance of political interests.



#### CRIMINALS

Conduct attacks in furtherance of financial interests.



#### INSIDERS

Conduct attacks in furtherance of personal interests.



#### STATE ACTORS

Destruction, disruption, and espionage in furtherance of national interests.



#### STATE INTERESTS

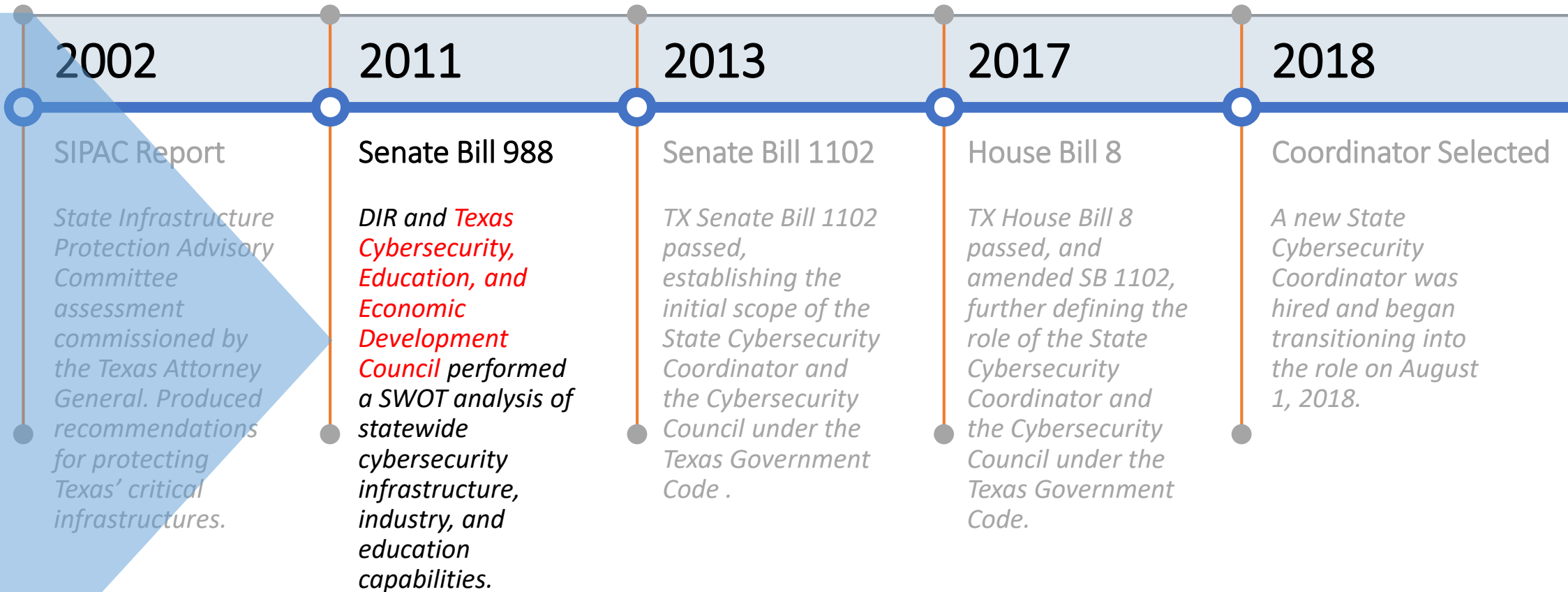
SAFETY

SECURITY

LIBERTIES

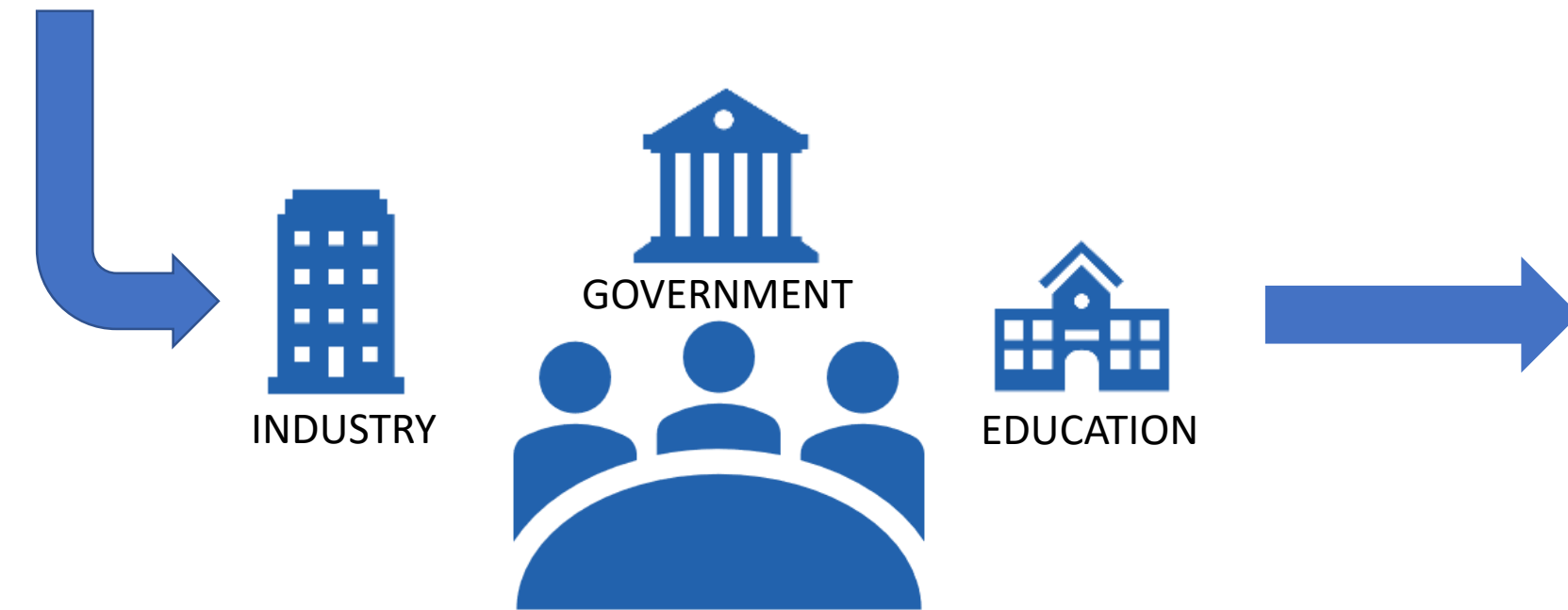
# SEC. 1: INTRODUCTION

## EVENTS LEADING TO THE TX ISAO



# SEC. 1: INTRODUCTION

The Response: “The 82<sup>nd</sup> Texas Legislature leveraged **public/private partnerships** to examine the infrastructure of the **state’s cybersecurity operations [and cyber environment]**.” (“Building a More Secure and Prosperous Texas,” 2012, p. 3)



**TEXAS CYBERSECURITY, EDUCATION, AND ECONOMIC DEVELOPMENT COUNCIL (TCEEDC)**

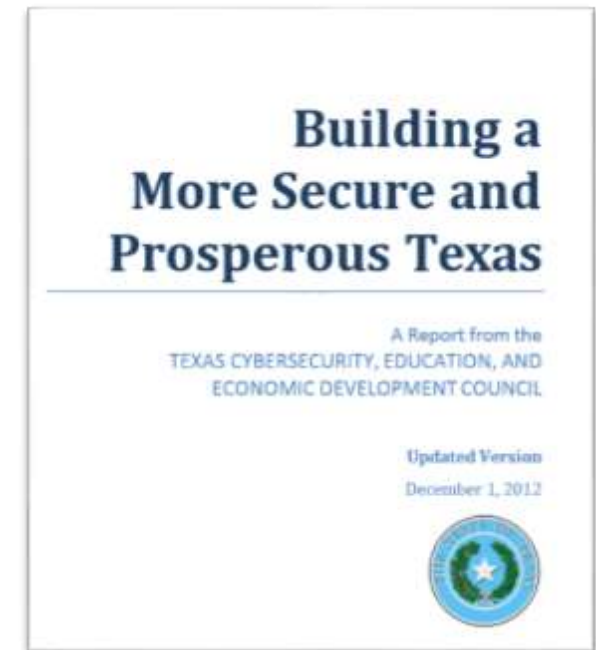


Figure 1: *Building a More Secure and Prosperous Texas* ([TCEEDC, 2012](#))



## CHALLENGES IDENTIFIED:

### 1. Private Sector Cybersecurity Coordination of Policy and Response:

- “Public, non-profit, and commercial entities within the state are challenged to **collaboratively identify and mitigate large-scale cyber events** by national and international entities with intent and ability to cause critical outages, steal private information, or harm Texas government and business in other ways.” (“**Building a More Secure and Prosperous Texas**,” 2012, p. 1)

### 2. Texas Cyber Workforce Shortage:

- “There is an insufficient number of qualified, trained cybersecurity personnel to meet industry demand.” (“**Building a More Secure and Prosperous Texas**,” 2012, p. 5)

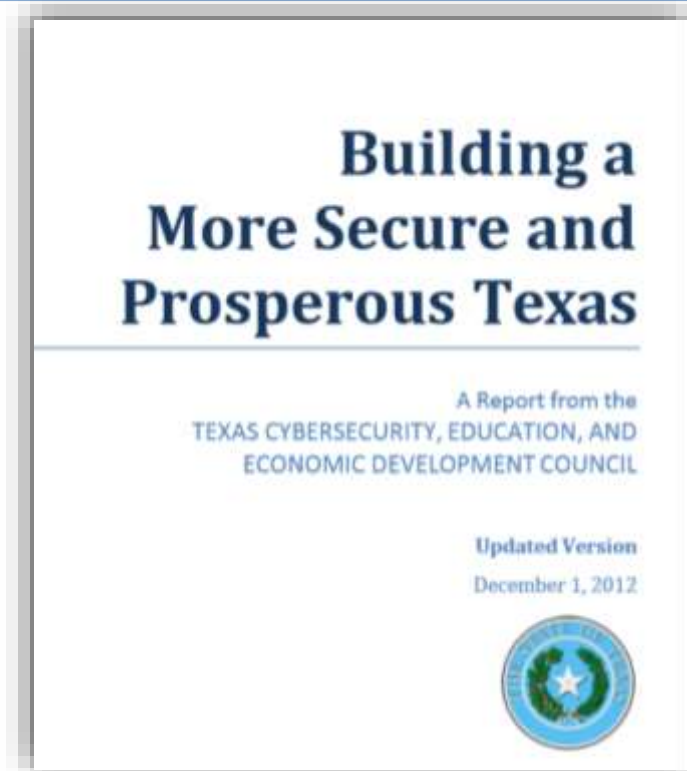


Figure 2: *Building a More Secure and Prosperous Texas* (TCEEDC, 2012)

**There is not enough cybersecurity collaboration, innovation, and entrepreneurship within the state.**

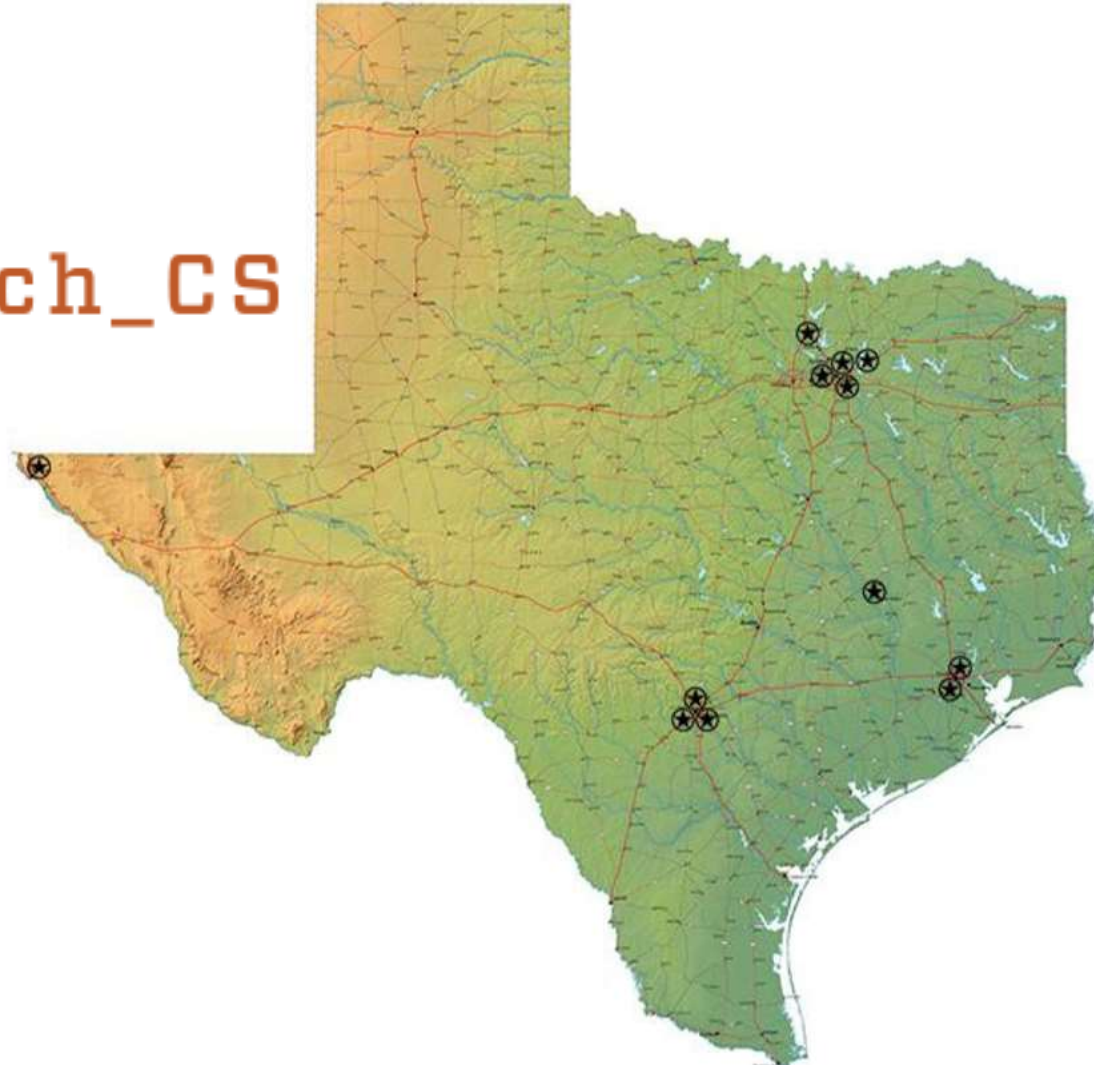
Figure 3: *Building a More Secure and Prosperous Texas* (TCEEDC, 2012)

# SEC. 1: INTRODUCTION

## TEXAS CYBERSECURITY EDUCATION PIPELINE



WeTeach\_CS



### NSA/DHS Centers of Academic Excellence in Information Assurance

#### College Station

Texas A&M University

#### Dallas

Richland College of the  
Dallas County Community College District  
Southern Methodist University

#### Denton

University of North Texas

#### El Paso

The University of Texas at El Paso

#### Houston

Rice University  
University of Houston

#### Irving

University of Dallas

#### Richardson

The University of Texas at Dallas

#### San Antonio

Our Lady of the Lake University  
Texas A & M University-San Antonio  
The University of Texas at San Antonio

Figure 3: Building a More Secure and Prosperous Texas ([TCEEDC, 2012](#))



# SEC. 1: INTRODUCTION



## 2018 TEXAS CYBERSECURITY WORKFORCE DATA

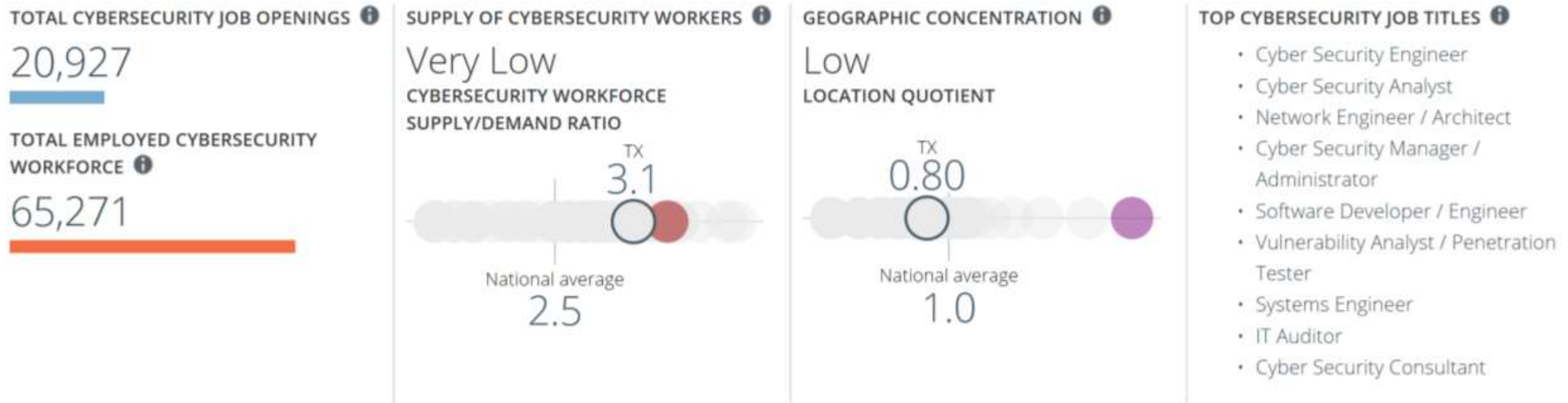


Figure 4: A collection of data regarding the cybersecurity workforce in the state of Texas, as of March 2018 ([NIST's Cyberseek Heatmap](#))

**Texas needs to invest in cybersecurity education programs across the K–12, community college, and university levels in order to obtain the number of trained cybersecurity professionals it needs across the employment continuum.**

Figure 5: *Building a More Secure and Prosperous Texas* ([TCEEDC, 2012](#))

## *Building a More Secure and Prosperous Texas*

- **Assessment Scope:** Assessment of statewide cybersecurity infrastructure, industry, and education capabilities.

### RECOMMENDATIONS:

1. How to improve the infrastructure of the state's cybersecurity operations with existing resources... and **through partnerships between government, business, and institutions of higher education;**
2. How to improve **cybersecurity coordination among non-state entities;** and
3. Specific actions to **accelerate growth of cybersecurity as an industry** in the state.

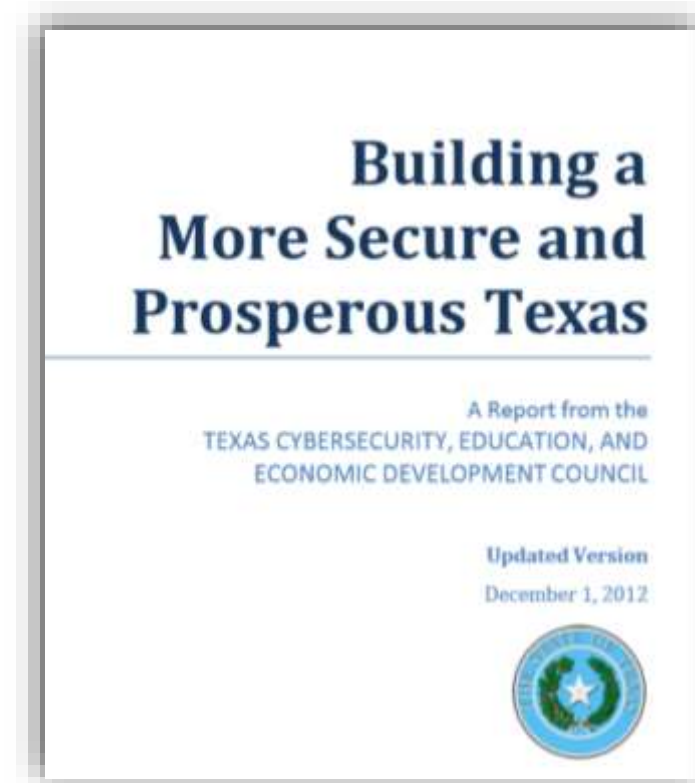


Figure 6: *Building a More Secure and Prosperous Texas* ([TCEEDC, 2012](#))

# SEC. 1: INTRODUCTION

## *Building a More Secure and Prosperous Texas*

- Assessment of statewide cybersecurity infrastructure, industry, and education capabilities

### CALL FOR ACTION:

- Establish a **statewide focus for the Texas cyber environment**;
- “Include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens... and to spur innovation in the cyber environment” (p. 6)

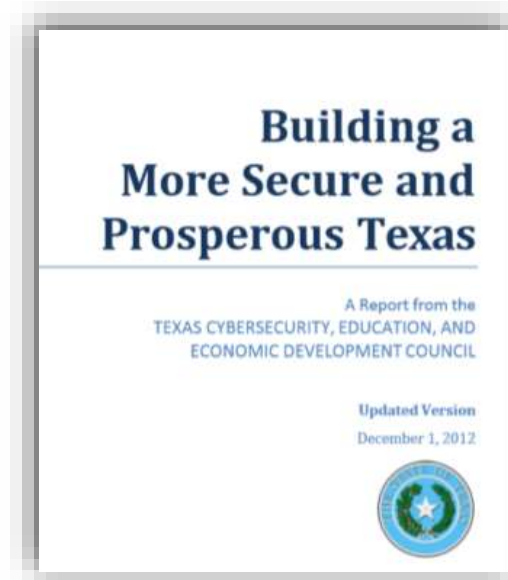


Figure 7: *Building a More Secure and Prosperous Texas* ([TCEEDC, 2012](#))

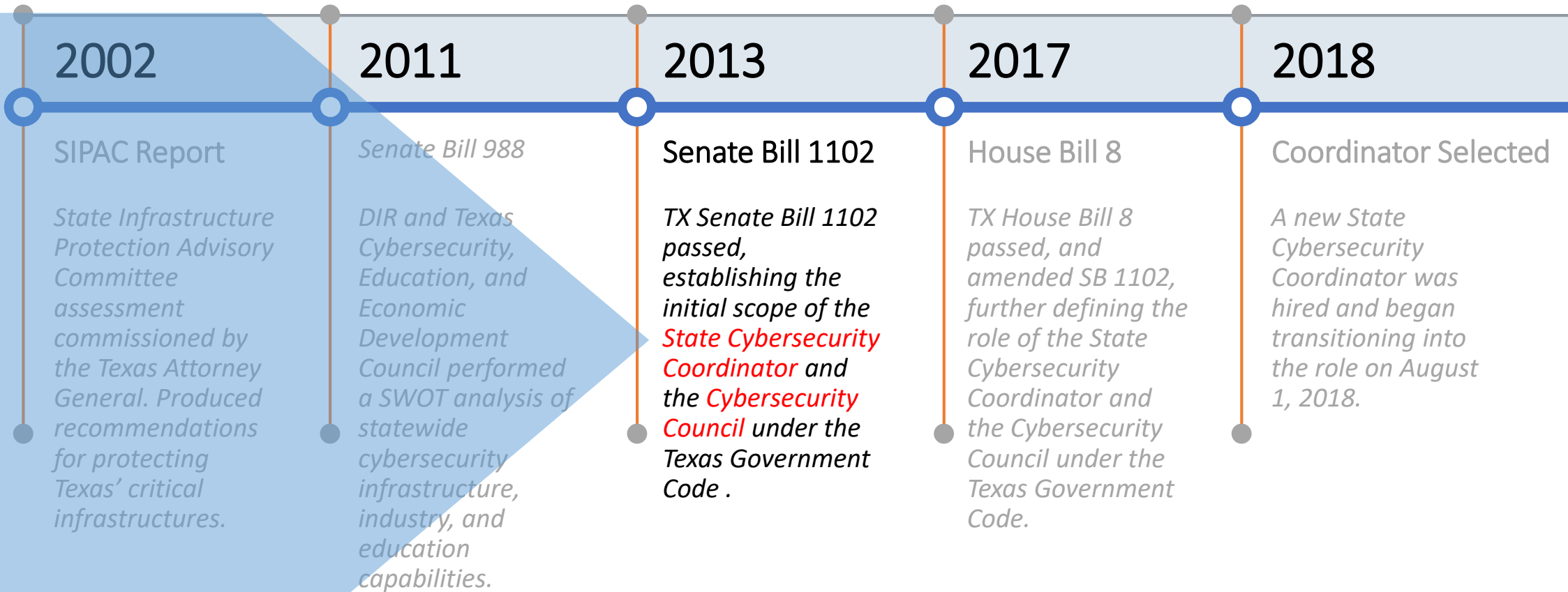
### **Establish a Texas Coordinator of Cybersecurity within the Office of the Governor.**

Improving cybersecurity for a state the size and complexity of Texas requires a heightened synergy of effort as well as different leadership expectations to address the question of “who’s in charge” when it comes to cybersecurity.

Figure 8: *Building a More Secure and Prosperous Texas* ([TCEEDC, 2012](#))

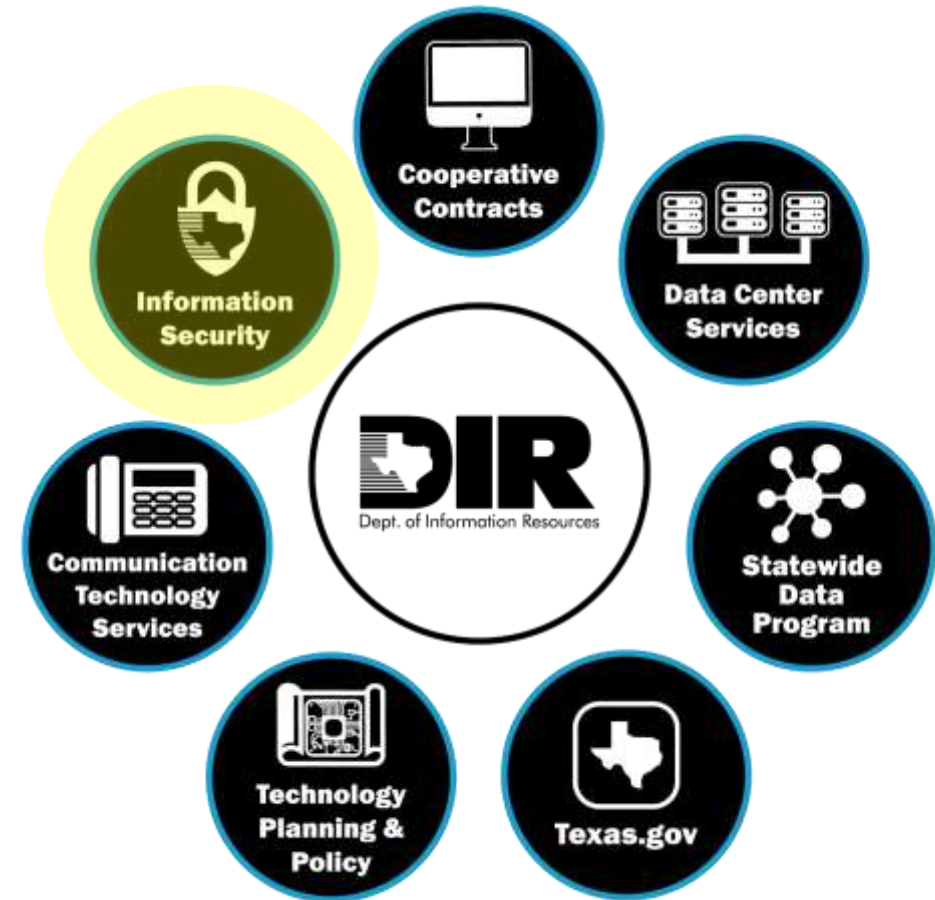
# SEC. 1: INTRODUCTION

## EVENTS LEADING TO THE TX ISAO





Office of the  
**CHIEF INFORMATION  
SECURITY OFFICER**  
State of Texas



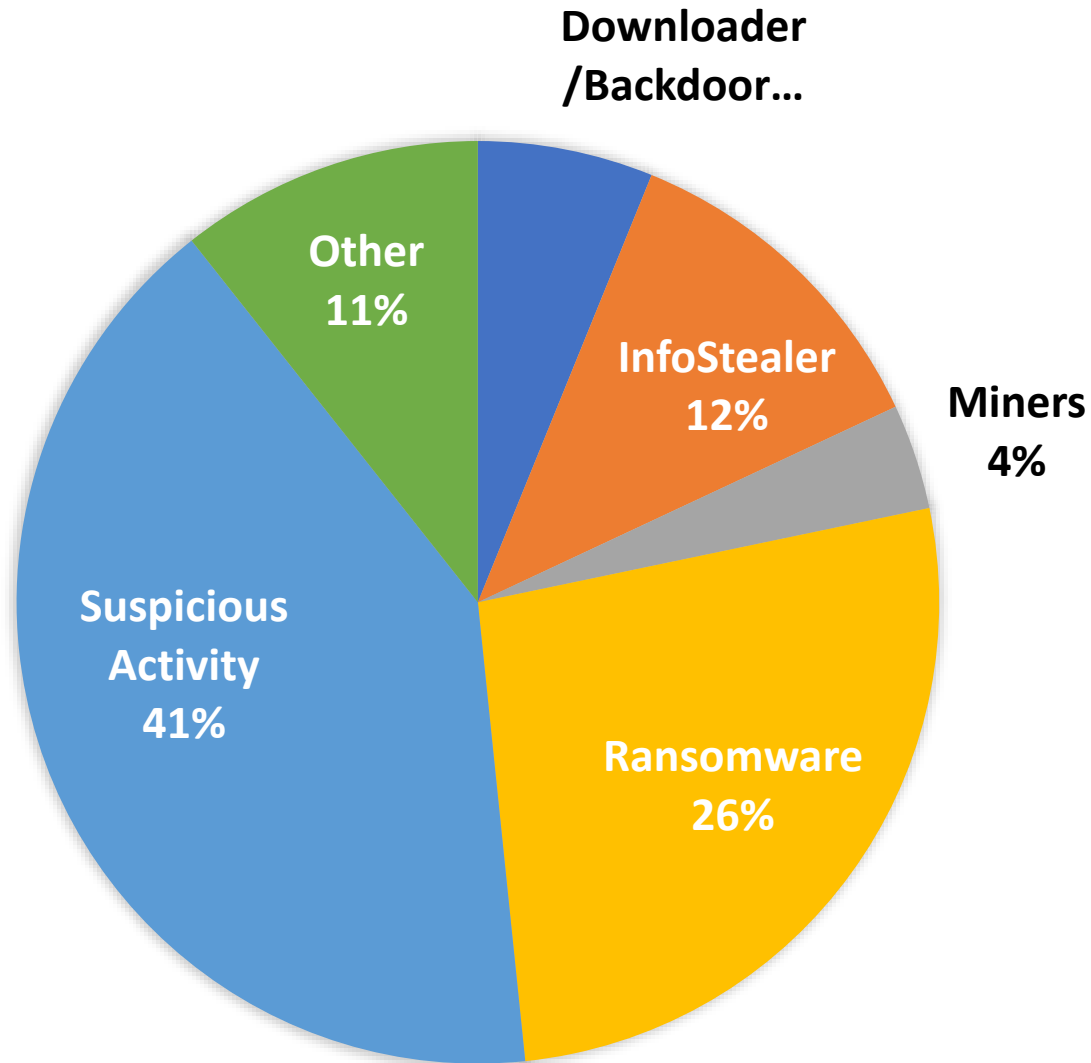


# DIR SERVICE HIGHLIGHTS

LOCAL GOV	STATE GOV	HIGHER EDUC	
	✓	✓	Policy/Security Controls Catalog
	✓	✓	InfoSec Academy
	✓	✓	End-User Security Awareness Training
✓	✓	✓	Information Security Forum (ISF)
✓	✓	✓	Vulnerability Scans/ Penetration Tests
✓	✓	✓	Security Assessments
✓	✓	✓	Managed Security Services

LOCAL GOV	STATE GOV	HIGHER EDUC	
*	✓	✓	Statewide Portal for Enterprise Cybersecurity Threat, Risk, & Incident Management (SPECTRIM)
	✓	✓	Decision Support Services
✓	✓		Network Security Operations Center (NSOC)
✓	✓	✓	Statewide Data Center and Technology Services (DCS)
	✓		Legacy Modernization
✓	✓	✓	Texas Cybersecurity Council

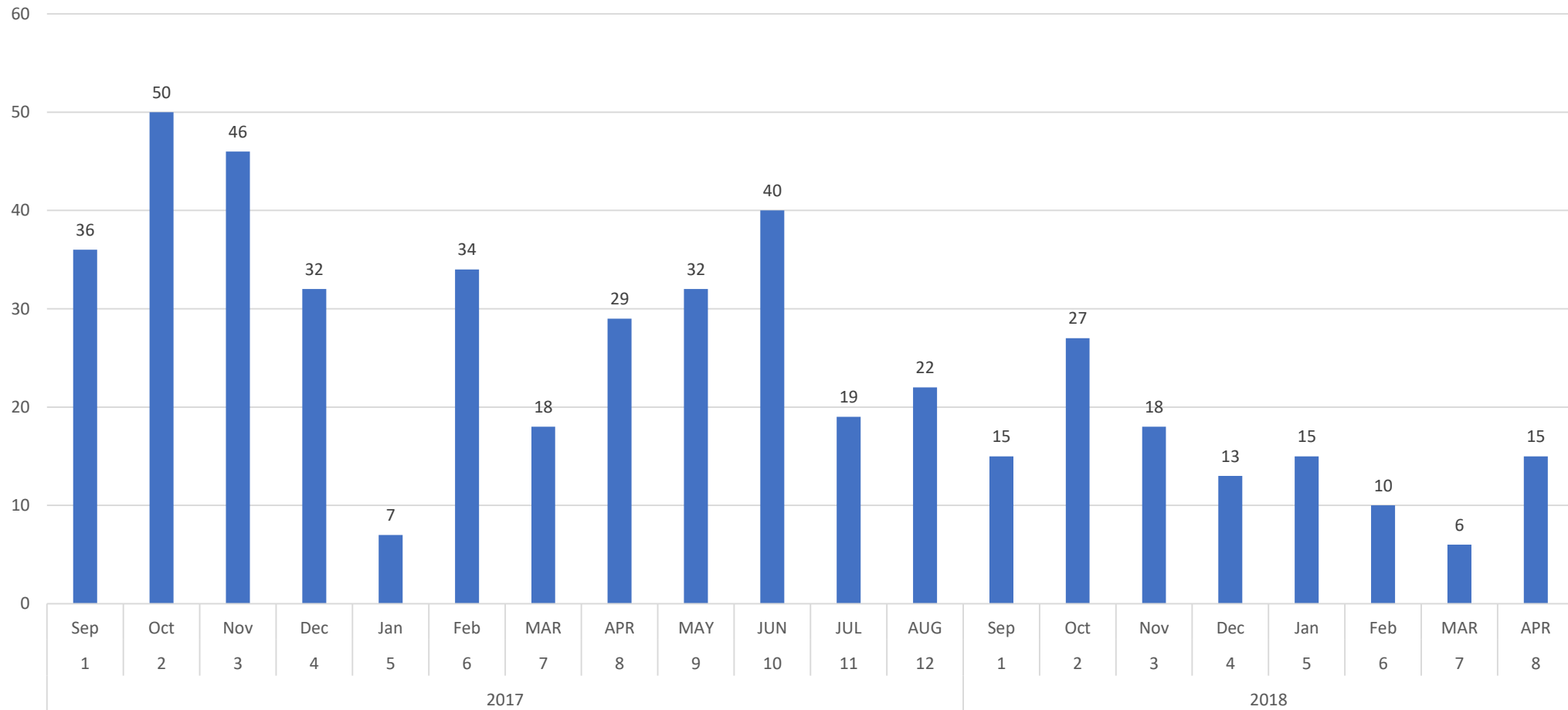
\* Planned



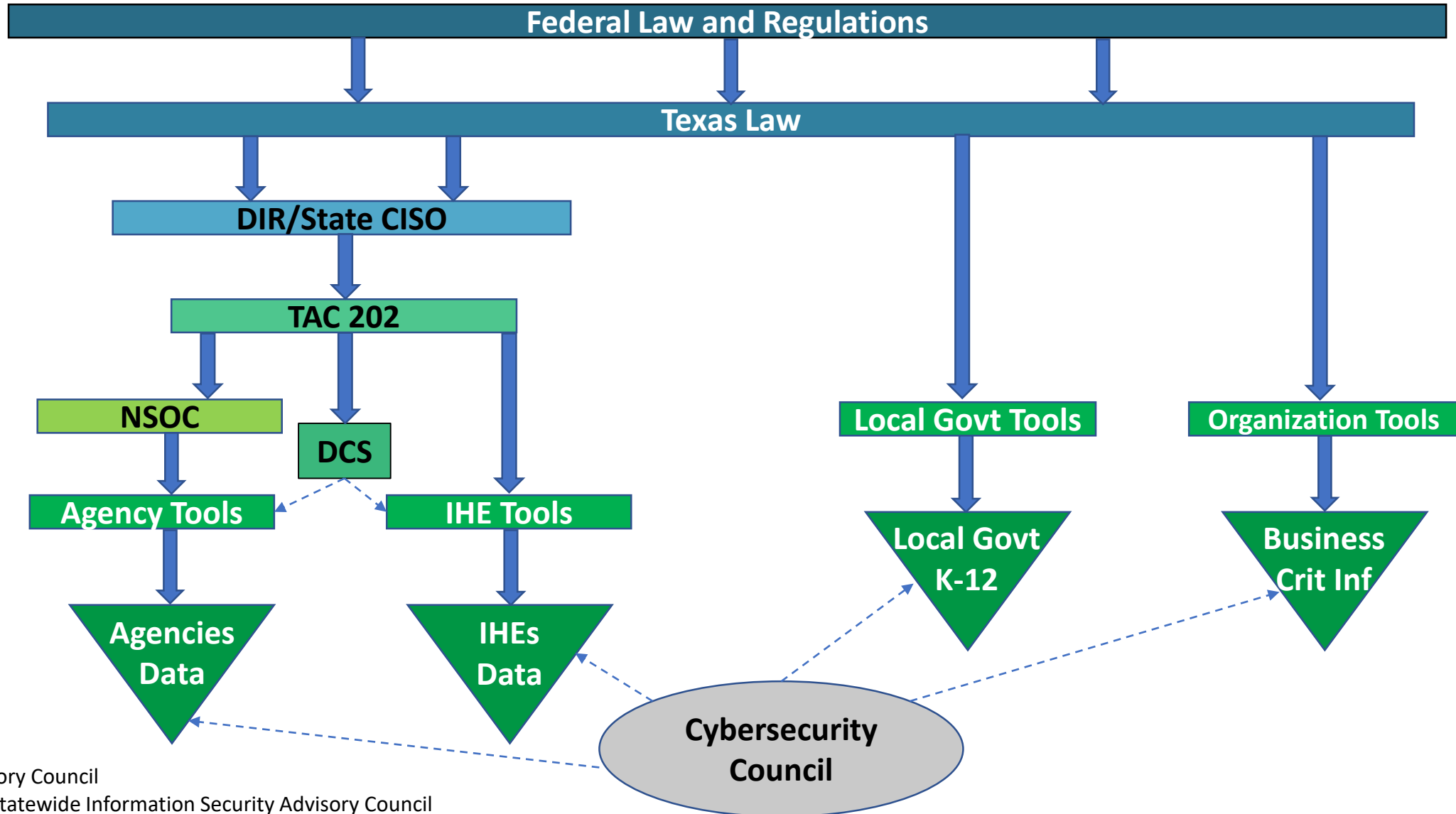
## ACTIVE THREATS

- Fraud/Organized Crime – High Threat: Phishing
- Nation/State – High Threat: APT (Advanced Persistent Threat)
- Hacktivists – Low Threat

# NSOC ALERTS- AGENCY NOTIFICATIONS



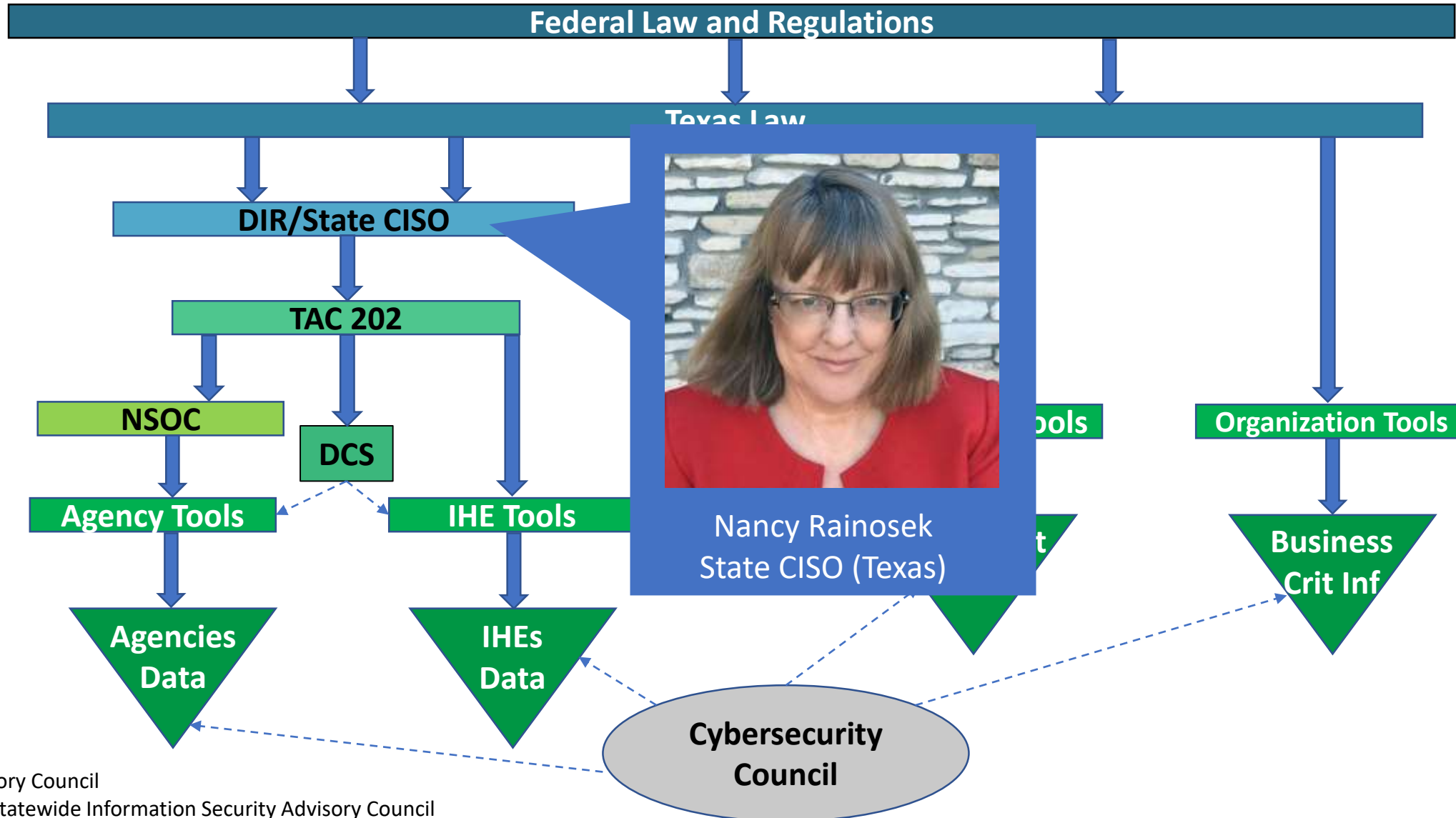
# TEXAS CYBERSECURITY PROGRAM



Advisory Council

- Statewide Information Security Advisory Council

# TEXAS CYBERSECURITY PROGRAM











Advisory Council

- Statewide Information Security Advisory Council

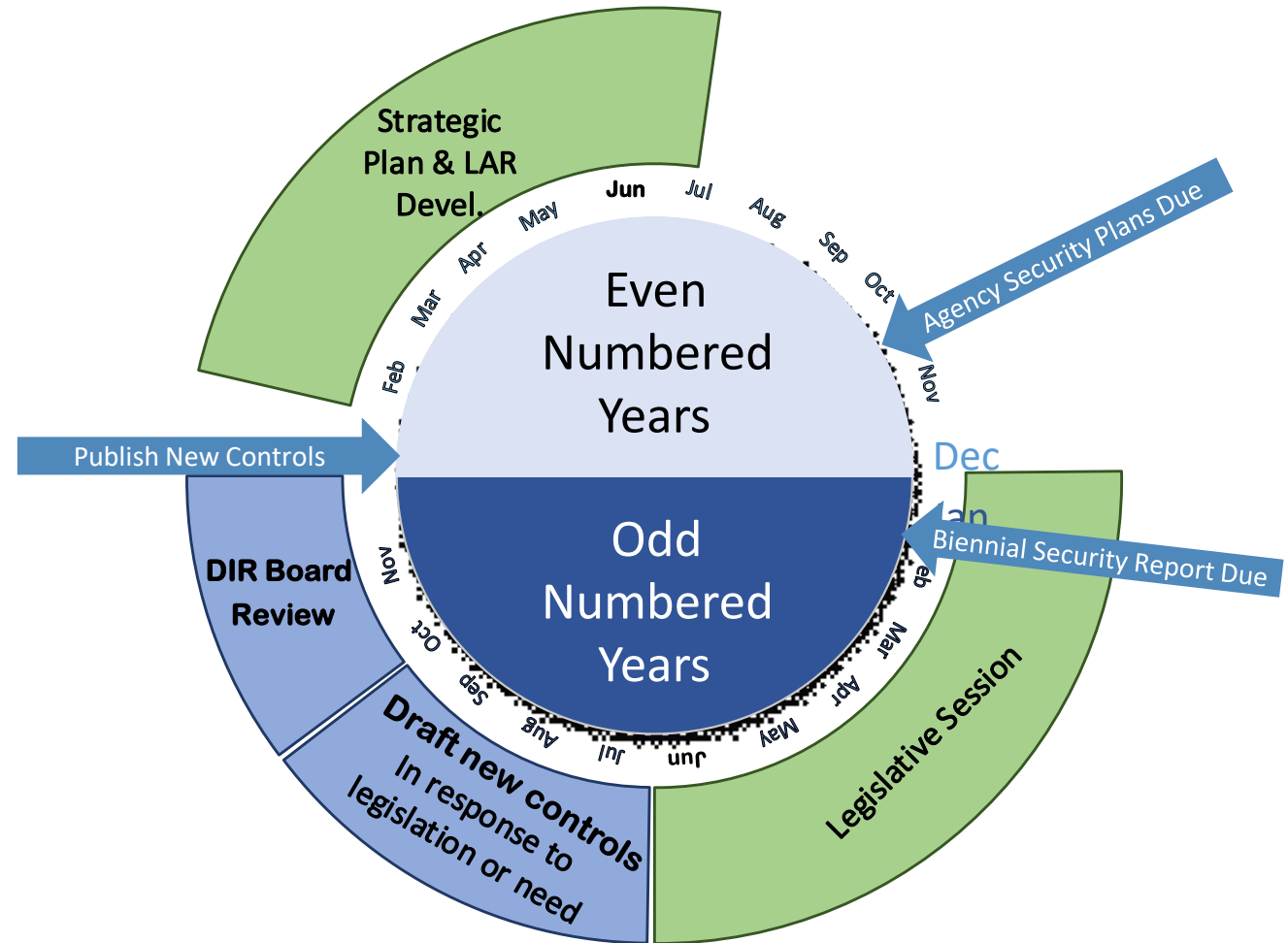


# TEXAS CYBERSECURITY REGULATORY COVERAGE

	State Agencies 	IHEs 	Local Govts 	K-12 	Junior Colleges 	Business 	Industry 	Critical Infra 
Federal Laws & Regulations	✓	✓	✓	✓	✓	✓	✓	✓
Texas Law	✓	✓	✓	✓	✓	✓	✓	✓
DIR/State CISO	✓	✓						
Texas Admin Code 202	✓	✓						
Organizational Tools & Policy	✓	✓						

# STATE OF TEXAS GOVERNANCE TIMELINE

- Updates to State security standards can be based on:
  - Legislation
  - Identified need
  - Changes in technology
- Changes published in time to be included in Strategic Plan and LAR decisions



# MEASURING MATURITY THROUGH THE TEXAS CYBERSECURITY FRAMEWORK



- Forty Security Objectives

- Identify Challenges

- Develop Roadmap

Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> <li>– Privacy and Confidentiality</li> <li>– Data Classification</li> <li>– Critical Information Asset Inventory</li> <li>– Enterprise Security Policy, Standards and Guidelines</li> <li>– Control Oversight and Safeguard Assurance</li> <li>– Information Security Risk Management</li> <li>– Security Oversight and Governance</li> <li>– Security Compliance and Regulatory Requirements Management</li> <li>– Cloud Usage and Security</li> <li>– Security Assessment and Authorization / Technology Risk Assessments</li> <li>– External Vendors and Third Party Providers</li> </ul>	<ul style="list-style-type: none"> <li>– Enterprise Architecture, Roadmap &amp; Emerging Technology</li> <li>– Secure System Services, Acquisition and Development</li> <li>– Security Awareness and Training</li> <li>– Privacy Awareness and Training</li> <li>– Cryptography</li> <li>– Secure Configuration Management</li> <li>– Change Management</li> <li>– Contingency Planning</li> <li>– Media</li> <li>– Physical Environmental Protection</li> <li>– Personnel Security</li> <li>– Third-Party Personnel Security</li> <li>– System Configuration Hardening &amp; Patch Management</li> <li>– Access Control</li> <li>– Account Management</li> <li>– Security Systems Management</li> <li>– Network Access and Perimeter Controls</li> <li>– Internet Content Filtering</li> <li>– Data Loss Prevention</li> <li>– Identification &amp; Authentication</li> <li>– Spam Filtering</li> <li>– Portable &amp; Remote Computing</li> <li>– System Communications Protection</li> </ul>	<ul style="list-style-type: none"> <li>– Malware Protection</li> <li>– Vulnerability Assessment</li> <li>– Security Monitoring and Event Analysis</li> </ul>	<ul style="list-style-type: none"> <li>– Cyber-Security Incident Response</li> <li>– Privacy Incident Response</li> </ul>	<ul style="list-style-type: none"> <li>– Disaster Recovery Procedures</li> </ul>

# SECURITY MATURITY LEVELS

MATURITY LEVEL	DIR DESCRIPTION	KEYWORDS
0	There is no evidence of the organization meeting the objective.	None, Nonexistent
1	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	Ad-hoc, Initial
2	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.	Managed, Consistent, Repeatable
3	The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	Compliant, Defined
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	Risk-Based, Managed
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.	Efficient, Optimized, Economized



Office of the  
**CHIEF INFORMATION  
SECURITY OFFICER**  
State of Texas

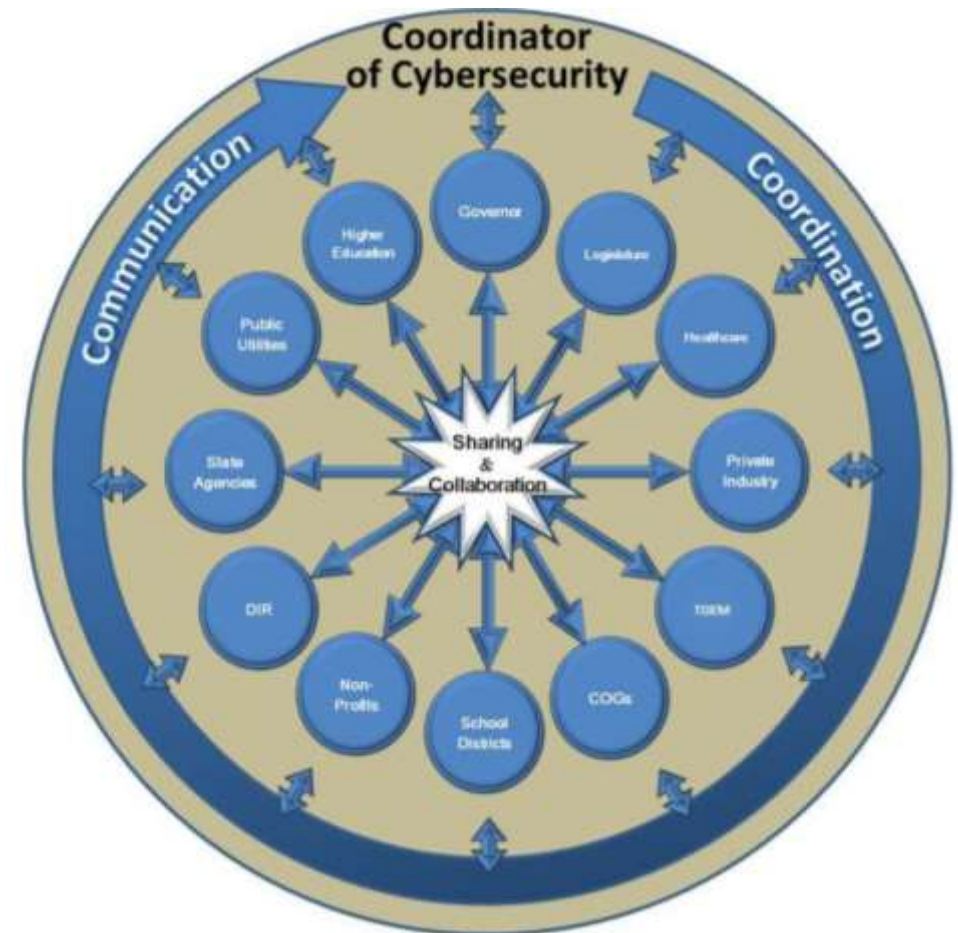
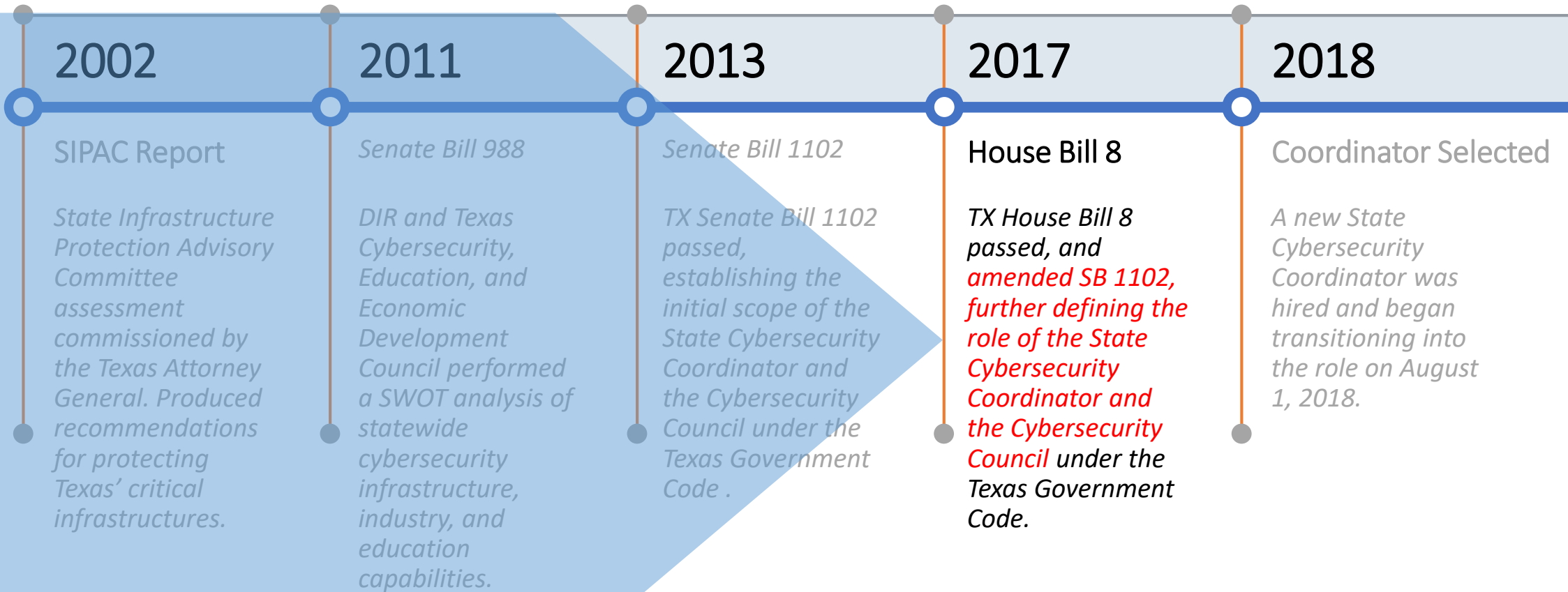


Figure 8: *Building a More Secure and Prosperous Texas*  
([TCEEDC, 2012](#))



# EVENTS LEADING TO THE TX ISAO



## What are the responsibilities of the State Cybersecurity Coordinator?

Sec. 2054.511 of the Texas Government Code, the State Cybersecurity Coordinator shall "oversee cybersecurity matters for th[e] state."

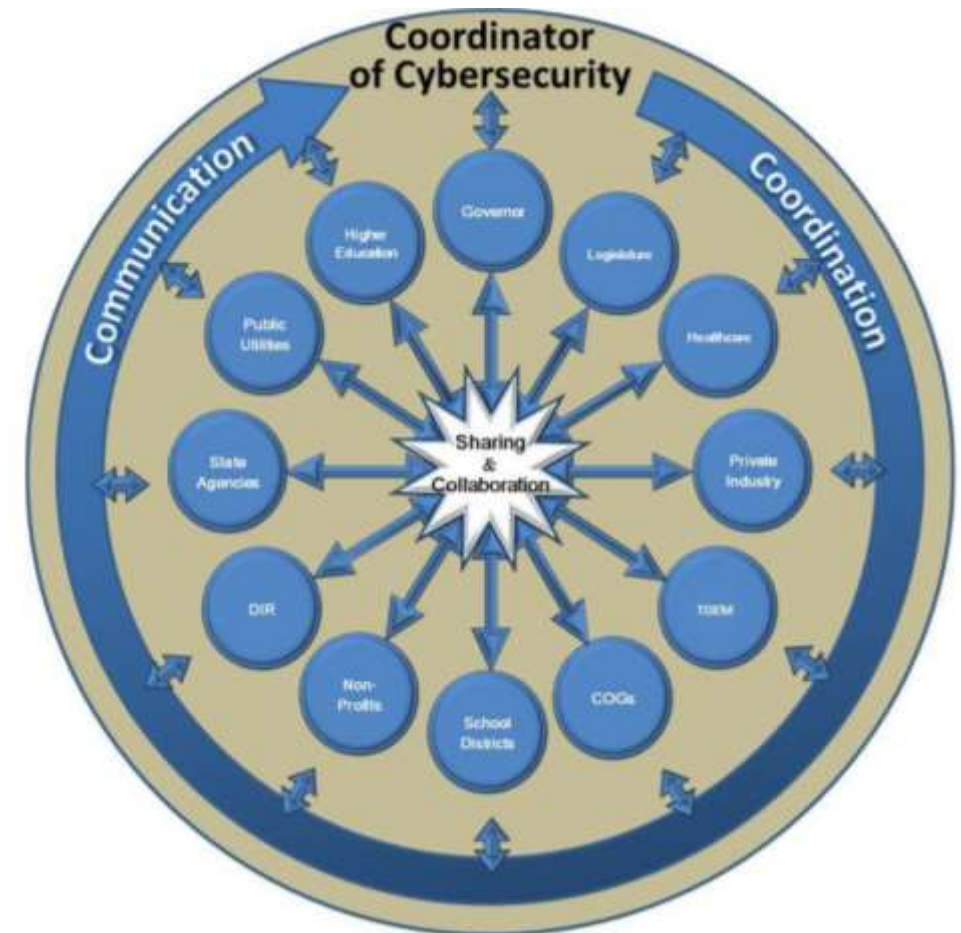
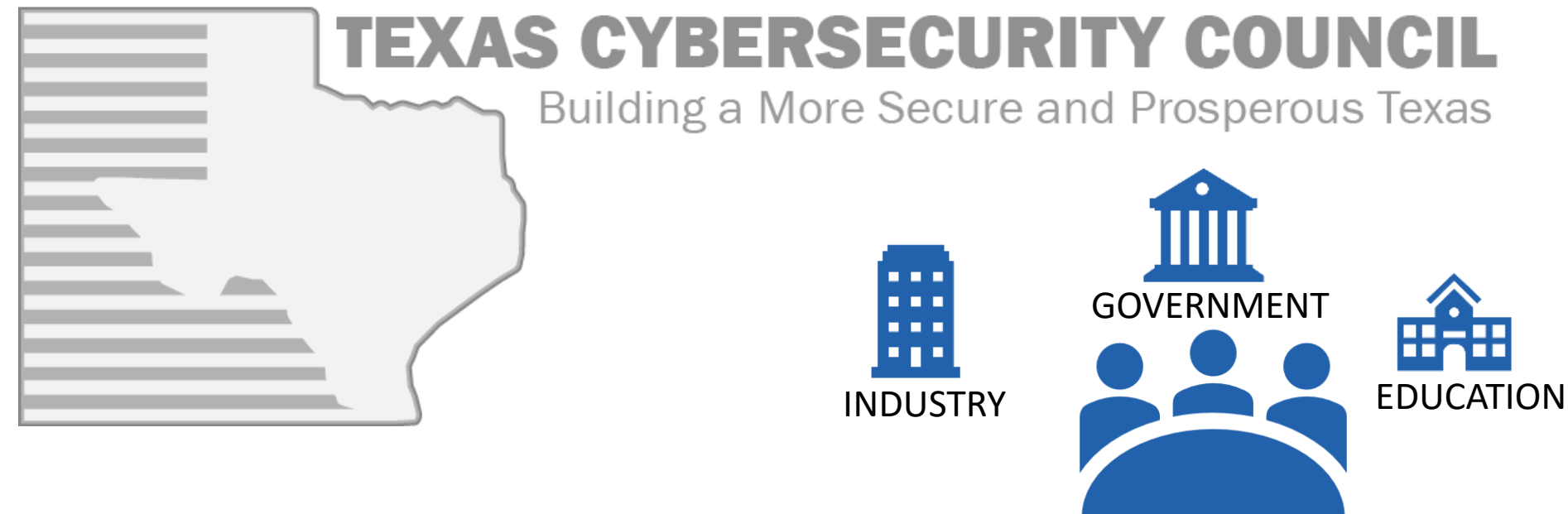


Figure 9: *Building a More Secure and Prosperous Texas* (TCEEDC, 2012)

## What are the responsibilities of the State Cybersecurity Coordinator?

**Sec. 2054.512 of the Texas Government Code**, the State Cybersecurity Coordinator "shall establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning the state."



## TEXAS CYBERSECURITY COUNCIL

Building a More Secure and Prosperous Texas



### PURPOSE

“The Texas Cybersecurity Council was created by the Department of Information Resources to develop enduring partnerships between private industry and public sector organizations to ensure that critical infrastructure and sensitive information are protected, to develop an exemplary cybersecurity workforce to protect technology resources from increasing threats, and develop strategies and solutions that ensure that Texas continues to lead in areas of cybersecurity at a national level.”

(Source: <https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=133> )

## TEXAS CYBERSECURITY COUNCIL

Building a More Secure and Prosperous Texas



### OBJECTIVES

The objectives of the Texas Cybersecurity Council include:

1. Establishing a council that includes a diverse makeup of public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning the State of Texas.
2. Develop strategies and solutions to increase the number and quality of cybersecurity practitioners in Texas.
3. Promote collaboration, innovation, and entrepreneurship in cybersecurity to further develop the cybersecurity industry in Texas.
4. Evaluate program requirements that establish exemplary cybersecurity practices and consider adoption within private and public entities.
5. Provide a consistent voice for industry regarding cybersecurity policies at a local, state, and federal level.
6. Promote awareness and education of cybersecurity throughout the state.

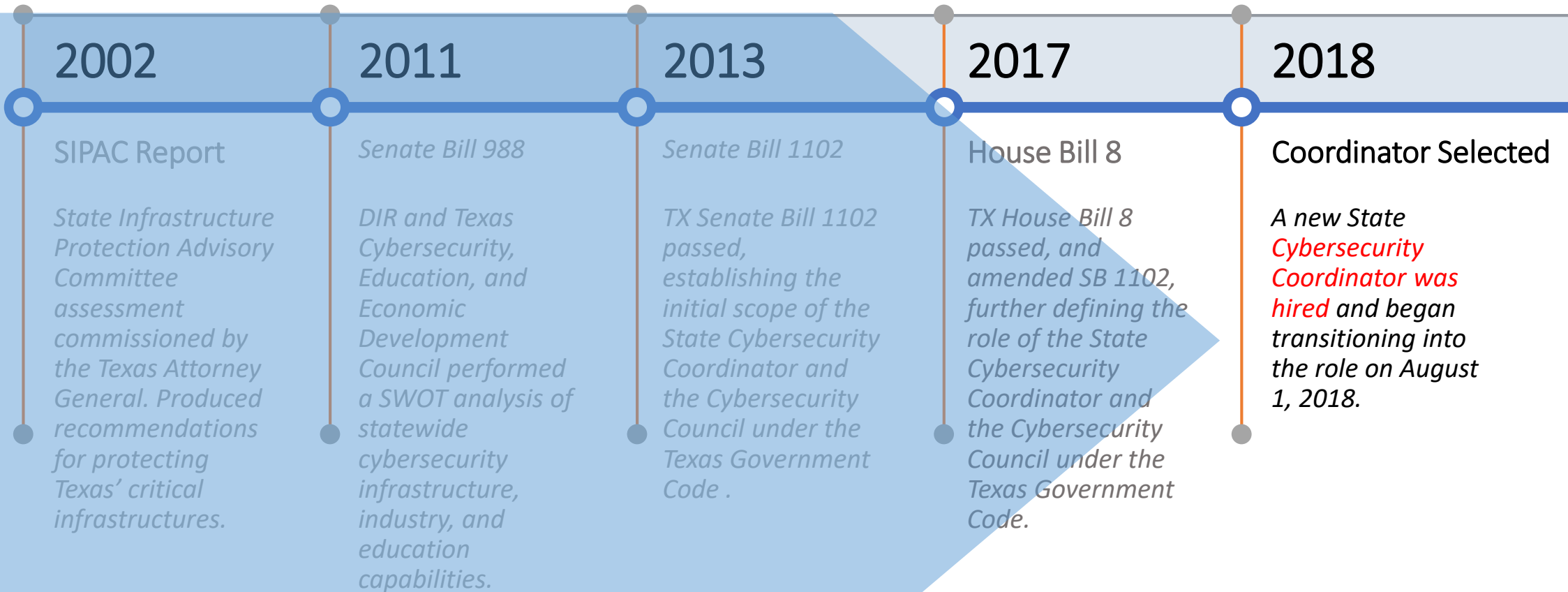


## What are the responsibilities of the State Cybersecurity Coordinator?

**Sec. 2054.0594 of the Texas Government Code**, the department "shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies."

```
Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) The department shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.
(b) The department shall appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.
(c) The department, using funds other than funds appropriated to the department in a general appropriations act, shall provide administrative support to the information sharing and analysis center.
Added by Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 5, eff. September 1, 2017.
```

# EVENTS LEADING TO THE TX ISAO



Our mission is to provide a forum for public and private entities based in Texas to share actionable and timely information regarding cybersecurity threats, best practices, and remediation strategies, in furtherance of advancing the cybersecurity capabilities and resiliency of the state.

Primary goals for the TX ISAO include the following:

1. To enhance the cybersecurity awareness, capabilities, and resiliency of both public and private sector computer networks based in Texas;
2. To mitigate the costs and risks associated with cyber threats;
3. To promote the sharing of information regarding cybersecurity threats, best practices, and remediation strategies between the public and private sector; and
4. To enhance the Texas cyber workforce through scholarship, public service, and public-private partnerships.

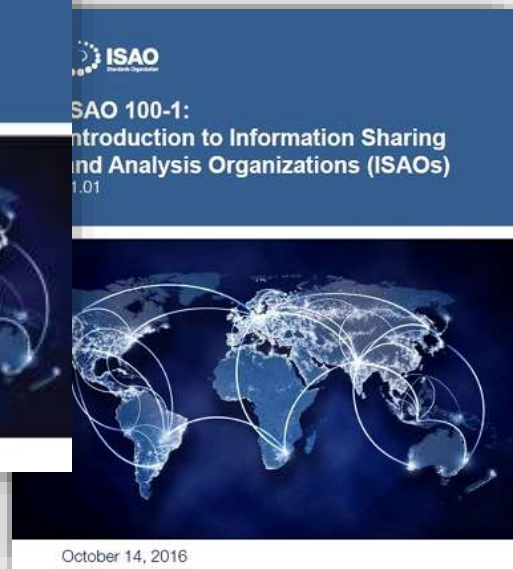
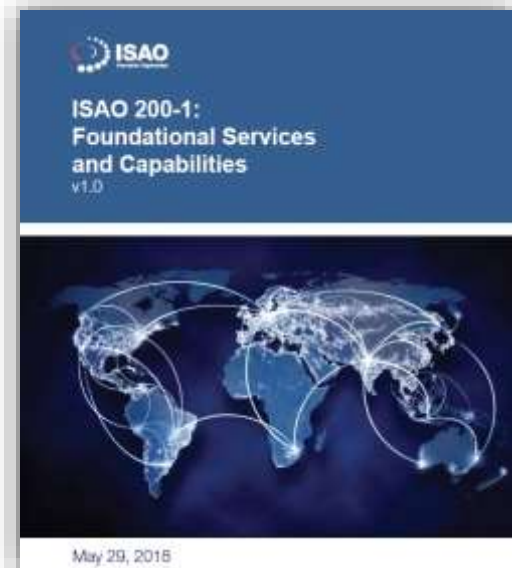
# TEXAS STATE-LEVEL ISAO

## GUIDING STANDARDS



# ISAO

Standards Organization



# TEXAS STATE-LEVEL ISAO STRUCTURE

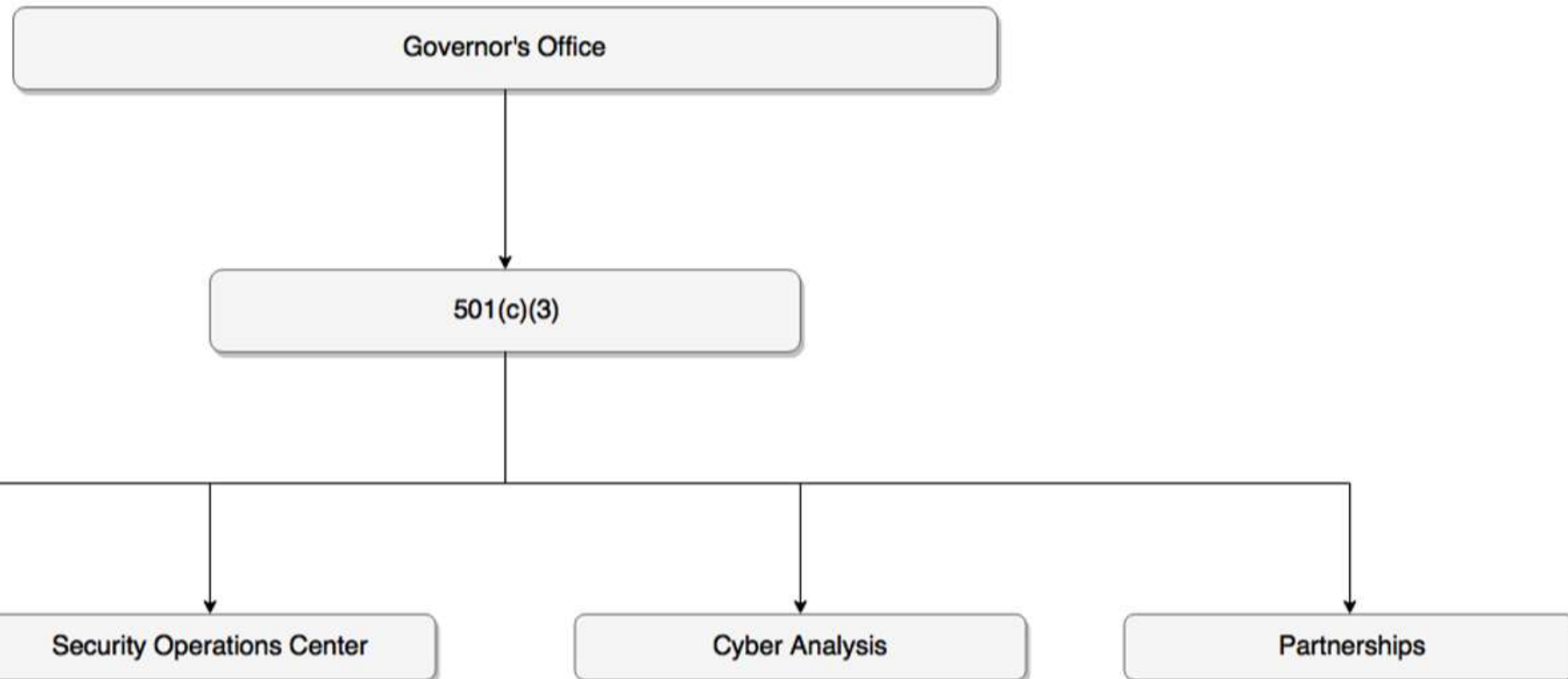


Figure 11: ISAO 600-1: A Framework for State-Level Information Sharing and Analysis Organizations v1.0 (ISAO Standards Organization, 2018)



## TX ISAO

- Leverage the resources of the “information sharing” community
- Identify initial services and capabilities
- Identify a governance structure
- Identify state-level partners (academe and private sector)



## TEXAS CYBERSECURITY EDUCATION AND WORKFORCE

- Assist and promote cybersecurity awareness, education, and training initiatives across the state (K-12 & Higher Education)



WeTeach\_CS



**CAE**  
**COMMUNITY**

## IICS 2018 LESSONS LEARNED

- **“COLLECTIVE SECURITY”**
  - We’re learning together... but must continue to mature as well
- **Leverage the Information Sharing Community**
  - ISAO SO publications
  - Advice, experience, and expertise of peer organizations
- **Engendering TRUST is Paramount**
  - “Trust” must be established between the ISAO, the public, and its private-sector members to succeed
    - Without “trust”, ISAO members will be reluctant to share cyber threat information with the ISAO and its members
  - Inform private-sector partners of the value proposition of ISAO membership



# CONTACT INFORMATION



Office of the  
**CHIEF INFORMATION  
SECURITY OFFICER**  
State of Texas

Ernesto C. Ballesteros, JD, MS, CISSP, CISA, Security+  
State Cybersecurity Coordinator for Texas  
Email: [ernesto.Ballesteros@dir.Texas.gov](mailto:ernesto.Ballesteros@dir.Texas.gov)