TXCC

TEXAS CYBER COMMAND

Partnering for Progress

www.txcc.texas.gov

Joe Poole

Director – Cyber Incident Response Unit (CIRU)

- 14 years experience at DIR NSOC
- Director of Cybersecurity Operations – managed the state networks security as well as the state's datacenters and public cloud cybersecurity
- Responsible for incident response for state agencies during that time working all kinds of events
- 6.5 years experience as a digital investigator at the Office of the Attorney General

Todays Agenda for 911 Coordinators

1. DIR transition to TXCC - Done
2. 911 Incident Reporting Requirements
3. Current Cyber Threats for 911.
4. Incident Response Support

DIR to TXCC Transition

During the 89th Legislative Session, the Texas Legislature passed **House Bill 150**, which established the **Texas Cyber Command (TXCC)** and officially transferred statewide cybersecurity powers, duties, and rulemaking authority from the **Department of Information Resources (DIR)** to the new Command under **Texas Government Code Chapter 2063**.

- **Texas Government Code 2054 > Texas Government Code 2063**
- **Texas Government Code 2059 > Texas Government Code 2063**
- **Texas Administrative Code 202 > Texas Administrative Code 477**

DIR Staff to TXCC Staff

All the DIR staff assigned to statewide cybersecurity were transferred to the Cyber Command on March 1, 2026

The transition is done

TXCC Responsibilities

TXCC
TEXAS CYBER COMMAND

Tex. Gov. Code Sec. 2063.004 (A)

PREVENTION & STANDARDS

- Promote public awareness of cybersecurity risks
- Establish cybersecurity best practices and minimum standards
- Provide cybersecurity training and awareness programs
- Establish policies to protect systems and sensitive data
- Coordinate with DIR to ensure technology meets cybersecurity standards

INTELLIGENCE & OPERATIONS

- Operate the Cybersecurity Threat Intelligence Center (CTIC)
- Serve as a cybersecurity information clearinghouse and intelligence hub
- Operate the Digital Forensics Laboratory (DFL)
- Manage the statewide cybersecurity portal and 24/7 cyber hotline

INCIDENT RESPONSE SUPPORT

- Support agencies during cybersecurity incidents and respond to reports
- Provide cybersecurity tools, services, and resources to agencies and covered entities

PARTNERSHIPS & COORDINATION

- Partner with law enforcement on incident response, training, and support
- Collaborate with federal agencies on prevention, response, and recovery

Texas Cyber Command

An Integrated Strategy

- **Information Sharing Analysis Organization** (ISAO) serves TXCC's outward -facing engagement and communications.
- **Unified Cyber Task Force** (UCTF) executes synchronized cyber campaigns, defends state agencies, responds to incidents
- **Cyber Threat Intelligence Center** (CTIC) gathers and shares intelligence to improve readiness, resilience, and situational awareness statewide.

Operational Terrains

TXCC executes its mission to prevent and respond to cyber incidents across six operational cyberspace terrains:

1. **Texas state government entities**
2. Institutions of Higher Education
3. Law Enforcement and Judiciary
4. Covered Entities
5. Critical Infrastructure
6. Texas data

Five Pillars

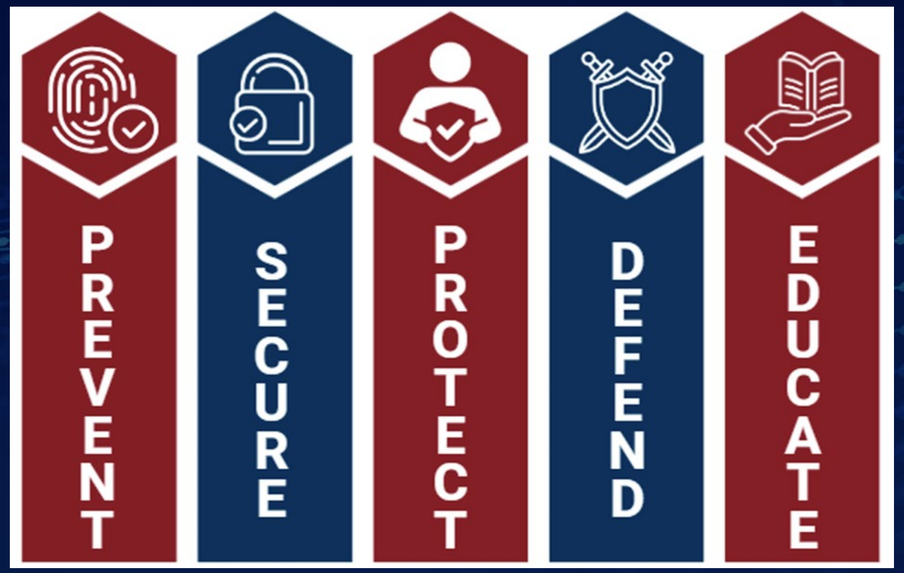
PREVENT – Proactive measures to stop cyber threats and attacks before they can harm systems, networks, or data, acting as the first line of defense.

SECURE – Establish and maintain a foundational, resilient posture across systems, networks, and data.

PROTECT – Implement specific safeguards and countermeasures to limit or contain the impact of a potential cyber incident.

DEFEND – Detect, respond to, and recover from active threats or attacks when protective measures have been bypassed.

EDUCATE – Outcomes focused on training and certifying people on relevant cybersecurity methods and technologies.



TXCC
TEXAS CYBER COMMAND

911 Systems Incident Reporting

911 Systems operated by a local government entity are subject to 48 -hour mandatory cybersecurity incident reporting requirements.

Under **Texas Government Code K 2063.302** , a 911 system operated by a local government must report a cybersecurity incident **within 48 hours of discovery** if the event meets any of the following criteria:

1. **System Compromise** – unauthorized incident that compromises info systems, applications, or access
2. **Network Propagation** – it has potential to propagate to other entities
3. **Confidential Data Breach** – unauthorized disclosure or modification of confidential or sensitive personal information
4. **Criminal Violation** - It results in criminal violations that must be reported to law enforcement.

Note – Always seek the guidance of General Counsel

www.txcc.texas.gov/report-an-incident

Big 3 Cyber Threats to Texas 911 Systems

1

Ransomware

The worst-case scenario

2

Data Exfiltration

Stealing PII from call records

3

Denial of Service

Flood your PSAPs with fake calls or internet traffic

TXCC
TEXAS CYBER COMMAND

TXCC
TEXAS CYBER COMMAND

Proactive Cyber Defense

5 Protective Measures

- Endpoint Detection and Response (EDR)
- **Multifactor Authentication (MFA)**
- Vulnerability Management - Up to date Patching
- 24/7 monitoring
- Log retention and analysis

TXCC
TEXAS CYBER COMMAND

Cyber Incident Response Unit

1. Hotline Number: 877 -347-2476
2. Incident Response Management and/or Support
3. Digital Forensics
4. Assistance Acquiring Resources

TXCC
TEXAS CYBER COMMAND

Securing the Digital Freedom of Texas

- Bringing **focus** where there is **fragmentation**.
- Building **capacity** where there are **gaps**.
- Activating **dedicated capability** to **defend** critical systems.

Joe Poole

THANK YOU

Joe Poole | Director – CIRU
Joe.poole@txcc.Texas.gov
512.289.7834

TXCC
TEXAS CYBER COMMAND