



Texas Cyber Risk

Texas is connected to the Internet so it is exposed to daily cyber-attacks by criminals and nation states—increasingly coming from a broader range of individuals and entities who understand cyber vulnerabilities and how to exploit them. The Department of Information Resources (DIR) has prevented as many as 110 million incidents in a given month and prevents an average of 75 million incidents monthly.

Privacy and Security Nexus

- **Privacy is Why** – Authoritative requirements: HIPAA, Hi-Tech, Texas Medical Privacy, others
- **Security is How** – Security controls to reduce risk of improper release of electronic health records

Texas Critical Infrastructure

Texas depends on a complex system of integrated, intertwined infrastructure—this critical infrastructure includes our energy grids and power plants, dams, water supplies, control systems, gas and oil production, transport, distribution systems, airports, harbors, railways and fuel supplies, **public health and police systems**, technology and telecommunication systems, and military installations.

Texas Critical Information

The State of Texas is investing significant resources to reduce cyber risks for the financial information, **personal data (including ePHI)**, and systems and networks it relies on to conduct critical functions on behalf of our citizens.

Statewide Cybersecurity

Most State of Texas organizations, including all state agencies and higher education institutions, have built information security programs **based on common regulatory requirements and individual business and compliance needs to support their risk-based decisions**.



Statewide Cybersecurity Collaboration

Texas Cybersecurity Council

In 2011, Senate Bill 988 (Senator Van de Putte; Representative Larson) authorized formation of the Texas Cybersecurity, Education, and Economic Development Council.

- Public/private partnership to improve the infrastructure of the state's cybersecurity operations, examine strategies to accelerate the growth of cybersecurity as an industry in Texas, and encourage the industry to call Texas "home"
- **Statewide public survey for baselining the state of cyber infrastructure and education in Texas**
- Review results and identify ways to mature security, scale best practices, and seek approaches to cybersecurity education (kindergarten to senior citizens)
- Assess federal and state government and industry best practices or new initiatives
- Identify strategies for enhancing the cybersecurity industry within Texas

Cyber Response Partnership

DIR partners with DPS and Texas Homeland Security for response planning and management for cybersecurity events that may impact the state's critical infrastructure. DIR also works with the U.S. Department of Homeland Security's Multi-State Information Analysis and Coordination Center to conduct cyber exercises and improve the state's cyber plans.

State Cyber Operations

DIR's statewide network, secure data center, and state portal offerings all have built-in security capabilities. DIR Network and Security Operation Center analyzes and reports cyber events and defends against cyber-attacks. DIR also provides third-party network, web, and host vulnerability testing to help state agency, higher education, and other customers identify and repair security weaknesses.

Statewide Information Security Advisory Committee (SISAC)

DIR chartered SISAC to provide guidance to protect government information assets and technology. SISAC is chaired by the State CISO and comprises the **State ISO** (DPS, GLO, CPA, TWC, TEA, UT-System, **HHSC**, SOS, OOG, OAG, BON), IT, Legal, City/County, and Industry Members.

Security Program Assessment Service

DIR sponsors **security program assessments for state agencies** to help measure agency cybersecurity capabilities and provide recommendations for improvement.

State of the State Information Security Report

DIR will publish a **State of the State Report** that presents trends identified in agency security program assessments and agency survey responses and describes the current state of cybersecurity in Texas.