CYBERSECURITY RESOURCES

Center for Internet Security

Cybersecurity & Infrastructure Security Agency (CISA)

Information Security Plan - The Information Security Plan is a report that state agencies, public universities, and junior colleges are required to complete every even-numbered year. These reports are completed through the SPECTRIM portal.

Information Technology Disaster Resource Center (ITDRC) - The Information Technology Disaster Resource Center (ITDRC) was founded in 2008 to provide communities with the technical resources necessary to continue operations and begin recovery after a disaster.

Multi-state Information Sharing & Analysis Center - The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

National Response Framework - The National Response Framework (NRF) provides foundational emergency management doctrine for how the Nation responds to all types of incidents. The NRF is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System (NIMS) to align key roles and responsibilities across the Nation.

Nationwide Cybersecurity Review (NCSR) - The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments.

Prioritization of Cybersecurity and Legacy Systems Projects (PCLS) - PCLS Project Questionnaire provides agencies with the opportunity to demonstrate the risks and potential impacts of not funding cybersecurity or legacy systems modernization projects.

SPECTRIM Portal - The SPECTRIM portal provides tools for managing and reporting security incidents, conducting risk assessments, storing and managing organizational policies, performing assessment and authorization (A&A) on information systems, templates for agency security planning activities, and more.

Technology Legislation - DIR tracks technology-related legislation, including bills with directives specific to DIR and bills that impact the state in general. Complete information about each bill is available at

the Texas Legislature Online.

Texas Administrative Code 202 - Texas Administrative Code Chapter 202 (TAC §202) outlines the minimum information security and cybersecurity responsibilities and roles at state agencies and institutions of higher education.

Texas Cybersecurity Council - The Texas Cybersecurity Council was created by DIR to develop enduring partnerships between private industry and public sector organizations to ensure that critical infrastructure and sensitive information are protected, to develop a 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.

Texas Cybersecurity Framework - DIR developed the Texas Cybersecurity Framework (TCF) in collaboration with other government entities and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies.

Texas Department of Information Resources (DIR) - The mission of the Texas Department of Information Resources (DIR) is 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.

Texas DIR Shared Services - DIR's Shared Technology Services Program is to supply access to managed IT as a Shared Service, allowing Customers to focus on supporting their mission and business functions rather than directly managing IT services.

Texas DIR YouTube Channel

Texas Division of Emergency Management (TDEM) - The Texas Division of Emergency Management (TDEM) serves the State of Texas by managing the all-hazards emergency management plan for the state. TDEM works closely with local jurisdictions, state agencies, and federal partners in ensuring Texas becomes more resilient for future disasters. TDEM staff are stationed statewide and serve six different regions. Whether natural or man-made, TDEM is prepared and ready to respond to all future disasters.

Texas Information Sharing and Analysis Organization (TxISAO) – The goal of the TxISAO is to provide a forum for entities in Texas, including state agencies, local governments, public and private institutions of higher education, and the private sector, to share information regarding cybersecurity threats, best practices, and remediation strategies.