



Texas Department of Information Resources
Transforming How Texas Government Serves Texans



Office of the
**Chief Information
Security Officer**
State of Texas

Security Services Guide

April 2023

Version 1.2

Contents

[Introduction](#)

- [Message from the OCISO](#)
- [Finding Your Way Around](#)
- [DIR Security Services Eligibility](#)
- [DIR Security Services Overview](#)

[Statewide Incident Response](#)

- [Incident Response Support, Guidance, and Resources](#)
- [Reporting Guidance – Data Breach, and Phishing Emails](#)
- [All Other Incident Reporting](#)

[Texas Volunteer Incident Response Team \(VIRT\)](#)

[DIR Cybersecurity Operations at the NSOC](#)

[Governance, Risk, and Compliance \(GRC\)](#)

- [Incident Response Report Guidance and Resources](#)
- [Texas Administrative Code 202 \(TAC 202\)](#)
- [Texas Policy and Assurance Course](#)
- [Statewide Portal for Enterprise Cybersecurity, Threat, Risk, and Incident Management \(SPECTRIM\)](#)
- [Texas Risk and Authorization Management Platform \(TX-RAMP\)](#)
- [Policy and Planning](#)

[Education and Training](#)

- [Texas InfoSec Academy](#)
- [Information Security Forum \(ISF\)](#)
- [Statewide Cybersecurity Awareness Training](#)

[Outreach and Growth](#)

- [Connecting Public and Private Sectors](#)
- [Texas Cyberstar Certificate Program](#)
- [Monthly Meetings and Webinars](#)
- [Texas Information Sharing and Analysis Organization \(TX-ISAO\)](#)
- [Communications and Mailing Lists](#)

[Technology Services](#)

- [Multi-Factor Authentication Program \(MFA\)](#)
- [Endpoint Detection and Response \(EDR\)](#)
- [Managed Security Services \(MSS\)](#)
- [Texas Cybersecurity Framework \(TCF\) Assessment](#)
- [Penetration Testing](#)

[Purchasing IT Services Through DIR Cooperative Contracts](#)

[The DIR Resource Library](#)

[Other Resources and Partner Organizations](#)

- [Resources for Information Security Officers \(ISOs\)](#)
- [Other Reporting and Complaint Resources](#)
- [Sign Up for Security News, Bulletins, and Updates](#)
- [Other General Security Resources](#)
- [Request a Gartner Professional License](#)
- [Other Cybersecurity Community Resources](#)

[Reporting Dates to Remember](#)

- [School Districts and Local Government](#)
- [State Agencies, Institutions of Higher Education, and Public Junior Colleges](#)

Message from the Office of the Chief Information Security Officer

Protecting Texas from cyber threats requires more than just protecting state level government. It requires assisting and working with local governments, educational organizations, critical infrastructure, and the private sector. The OCISO team works to set state information security policies and standards, publish guidance on best practices, improve incident response preparedness, monitor and analyze incidents, coordinate security services, and promote information sharing throughout the public sector cybersecurity community.

The DIR's security services guide was developed to provide a single source of all DIR's security-related services as well as how, when, and where to get assistance and support from the OCISO team.

Nancy Rainosek
Chief Information Security Officer
Texas Department of Information Resources

Finding Your Way Around

- Browse topics using the links in the Contents.
- Resource document titles are almost always shown as links.
- Use the Page Up/Page Down keys or arrow keys to switch pages.
- Most sections contain "Go to:" links which, when clicked, will display more information about that topic or service. Other links may display listings or other information broken down by various methods.
- Click on a document title to open the document in a new browser window.
- Several sections contain references to "eligible customers". Click on the eligible customer link to be taken to the OCISO Security Services Eligibility table on page 2 of this guide.
- Click on the [Back to Contents](#) at the bottom of each page to return to the Contents.



DIR Security Services Eligibility

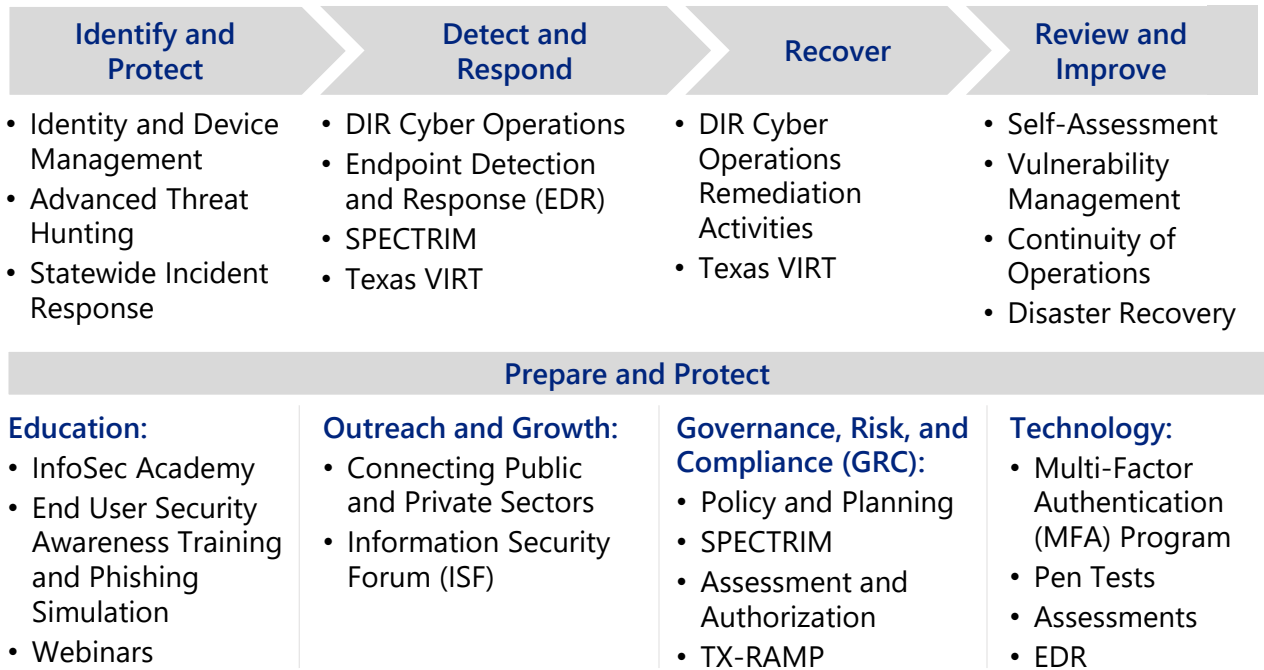
OCISO Services	State Agency	Institution of Higher Education	Public/Junior College	Local Gov't	Independent School District
Information Security Forum	✓	✓	✓	✓	✓
Webinars (Topical/Educational)	✓	✓	✓	✓	✓
Website Resources and Templates	✓	✓	✓	✓	✓
Texas Information Sharing and Analysis Organization	✓	✓	✓	✓	✓
Network Penetration Tests	✓	✓	✓	\$	\$
Web or Mobile Application Penetration Tests	✓	✓	✓	\$	\$
TCF Security Assessments	✓	✓	✓	\$	\$
InfoSec Academy Security Cert Prep Courses	✓	✓	✓	\$	\$
InfoSec Academy Secure Developer Training	✓	✓	✓	\$	\$
End User Awareness Training and Phishing Simulation	✓	✓	✓		
Endpoint Detection and Response (EDR)	✓	\$	\$	\$	\$
Multi-Factor Authentication (Internal Only)	✓	✓	✓		
Multi-Factor Authentication (For Org Constituents)	*	*	*		
Research and Advisory Services	✓	✓	✓		
SPECTRIM Access	✓	✓	✓		
Incident Response Assistance from OCISO	*	*	*	*	*
Mandatory Cybersecurity Training Program					
Training Program Certification	✓	✓	✓	✓	✓
Published List of Certified Programs	*	*	*	*	*

Key

✓	Service available at no cost
\$	Service available at \$
*	Service may be available; possible \$
	Service not available

Note: This table is intended to provide a broad understanding of governmental entities' eligibility for network security services provided by DIR or its contracted vendor. This table does not constitute a binding statement that your governmental entity is eligible for these services; whether an interested entity may be a particular type of governmental entity found in this chart could be subject to DIR legal analysis in many cases.

DIR Security Services Overview



Statewide Incident Response

DIR provides statewide incident response services to assist organizations impacted by a cybersecurity incident. This includes support, guidance, and resources *before, during, and after* a cybersecurity incident.



Use the Incident Response Hotline **during** cybersecurity incidents.

Incident Response Hotline

For state and local government organizations.

(877) DIR-CISO | (877) 347-2476

For all other security related inquiries (including *before and after* a cybersecurity event), please email DIRsecurity@dir.texas.gov.

Incident Response Support, Guidance, and Resources

- [Cybersecurity Strategic Plan](#)
- [Incident Response Template](#)
- [State of Texas Guide to Cybersecurity Incident Response](#)
- [State of Texas Guide to Cybersecurity Resources](#)
- [CISA MS-ISAC Ransomware Guide S508C](#)
- [Ransomware Tips and Information](#)

Go to: [Cybersecurity Incident Management and Reporting](#)

Reporting Guidance – Data Breach and Phishing Emails

Certain types of breaches trigger legal notification responsibilities.

- Actual or suspected breaches must be reported to the OCISO Incident Response Hotline within 48 hours of discovery.
- The Secretary of State. Must be notified of any election data breach.
- Certain businesses and state agencies that experience a breach of system security affecting 250 or more Texans must contact the Office of the Texas Attorney General.



Report Phishing Emails to DIR by forwarding the message as an attachment to security-alerts@dir.texas.gov

All Other Incident Reporting

Guidance for all other types of incident reporting can be found in the Governance, Risk, and Compliance section of this guide. Go to: Governance, Risk, and Compliance Incident Reporting

Texas Volunteer Incident Response Team (VIRT)



The Texas VIRT team is comprised of experienced volunteers that support Texas agencies, institutions of higher education, and local governments in responding to significant cybersecurity events and restoring impacted services quickly. Go to: Texas VIRT

Have VIRT Questions?

Send and email to:

TexasVIRT@dir.texas.gov

- Texas VIRT Program Handbook
- VIRT Volunteer Application Form

DIR Cyberoperations at the NSOC

DIR Cyber Operations is located at the DIR Network Security Operations Center (NSOC) and supports state agencies, customers of the state data center, and eligible partners in obtaining internet access through DIR.

DIR Cyber Operations is 24x7 and provides:

- IP and domain name blocking
- Monitoring and alerting of suspicious activity
- Incident response guidance and support
- Intelligence gathering and sharing
- Oversight of DCS Security Operations
- Distributed Denial of Service (DDoS) attack detection and mitigation

DIR Cyber Operations NSOC After Hours

On Call Analyst:

(512) 701-7152 or

(512) 965-8320

Incident Response Report Guidance and Resources

Urgent Incident Reporting to DIR through [SPECTRIM](#)

State agencies and institutions of higher education are required to timely report any incident that may:

- Propagate to other state systems (emergency reporting) OR
- Result in criminal violations that shall be reported to law enforcement OR
- Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information.

Local Government Incident Reporting

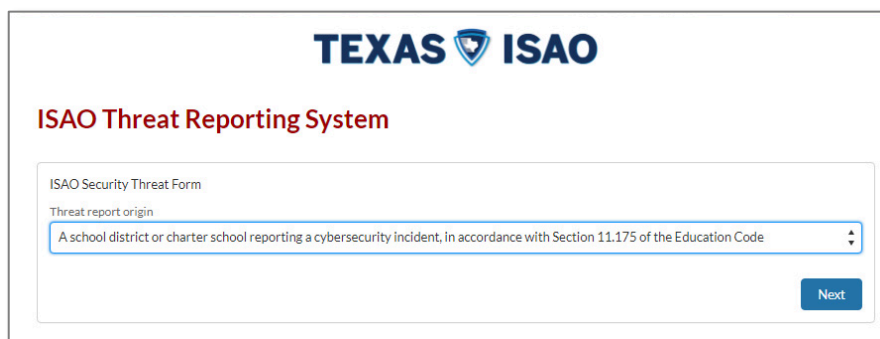
Report cyber threats to TX-ISAO who may research and disseminate. [Submit a Threat Report](#) and select "Other".



The screenshot shows the 'ISAO Threat Reporting System' interface. At the top, the 'TEXAS ISAO' logo is displayed. Below the logo, the title 'ISAO Threat Reporting System' is shown in red. The form contains a section titled 'ISAO Security Threat Form' with a dropdown menu for 'Threat report origin'. The dropdown menu is open, and 'Other' is selected. A blue 'Next' button is located at the bottom right of the form.

School Districts and Charter Schools Incident Reporting

School districts and charter schools must report cyber threats or cybersecurity incidents that constitutes a "breach of security" to TX-ISAO. [Submit a Threat Report](#) using the dropdown to select "a school district or charter school..."



The screenshot shows the 'ISAO Threat Reporting System' interface. At the top, the 'TEXAS ISAO' logo is displayed. Below the logo, the title 'ISAO Threat Reporting System' is shown in red. The form contains a section titled 'ISAO Security Threat Form' with a dropdown menu for 'Threat report origin'. The dropdown menu is open, and 'A school district or charter school reporting a cybersecurity incident, in accordance with Section 11.175 of the Education Code' is selected. A blue 'Next' button is located at the bottom right of the form.

Texas Administrative Code Chapter 202 (TAC §202)

- Describes the information security standards that state agencies and institutions of higher education are required to follow.
- Outlines the minimum information security and cybersecurity responsibilities and roles at state agencies and institutes of higher education.
- Requires agencies and institutions of higher education to adhere to the TAC §202 Security Controls Standards Catalog.



Go to: [TAC 202 at dir.texas.gov](#) for more information.

Texas Government Code 2054: Information Resources Management Act provides DIR with the ability to create rules and establishes the specific rules DIR must create, such as rules on information security, accessibility, and digital signatures.

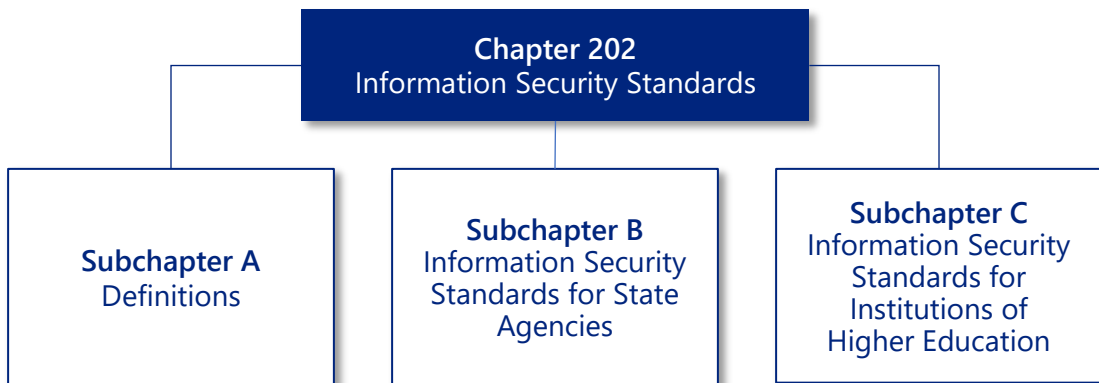
TAC 202 Security Controls Standards

Review the minimum list of security controls for state data and systems in the [Security Controls Standards Catalog](#).

Download the [Control Crosswalk Reference](#) to see how the catalog maps to various regulatory controls.

Security Controls Standards will be implemented using baseline levels to determine:

- which controls to implement,
- relate to the impact of a system, and
- include three (3) impact levels: low, moderate, and high.



- ✓ Mandatory security controls shall be defined by the department in a Control Standards document published on the department's website.
- ✓ The controls shall include information security requirements for all State information and information systems.
- ✓ The controls shall include standards to be used by all agencies to provide levels of information security according to risk level.
- ✓ Review of the agency's information security program for compliance with these standards will be performed at least biennially by individual(s) independent of the information security program.

Texas Policy and Assurance Course

DIR created the “Texas Security Policy & Assurance” course to assist security staff in applying state rules regarding information security within state agencies or institutions of higher education.

The course includes a module dedicated to articulating the responsibilities of state agencies and institutions of higher education under TAC 202. The course is available through the [InfoSec Academy](#) and provided at no cost to [eligible customers](#).

Statewide Portal for Enterprise Cybersecurity, Threat, Risk, and Incident Management (SPECTRIM)

- Manage and report security incidents.
- Conduct risk assessments.
- Store and manage organizational policies.
- Perform Assessment and Authorization (A&A).

Unlimited access to the SPECTRIM portal is free to [eligible organizations](#). Accounts must be requested by the organization’s ISO through a support request in the portal.

- [SPECTRIM](#)
- [Policy Management End User Training](#)

IT Security Vulnerability Management in SPECTRIM

SPECTRIM integrates RiskRecon scans of internet-facing assets to determine vulnerability priority based on asset value and issue severity. Through the portal, organizations can manage scan results, create vulnerability tickets, and make informed risk decisions associated with identified vulnerabilities.

- [Request access to a recording of the RiskRecon & IT Security Vulnerability Management Overview Webinar](#)

Need Help With Monthly Incident Reporting, Password Reset, or Have Other Questions?

Send an email to:

GRC@dir.texas.gov



Texas Risk and Authorization Management Platform (TX-RAMP)



As required by Government Code 2054.0593, TX-RAMP is a framework established by DIR for collecting and assessing information about cloud services security postures for compliance with required controls and documentation.

Go to: [TX-RAMP](#)

- [TX-RAMP Program Manual](#)
- [TX-RAMP Certified Cloud Products](#)
- [TX-RAMP Security Control Baselines](#)
- [TX-RAMP Overview for State Agencies](#)

Policy and Planning

OCISO provides resources to assist organizations with the establishment of structured security programs. Go to: [Security Policy and Planning](#)

- [Learn or review the cybersecurity rules for state agencies in Texas](#)
- [Find resources on the security framework Texas state agencies have adopted](#)

DIR established the below chartered committees and councils focus on specific topics and inform Texas' cybersecurity strategy.

- [Statewide Information Security Advisory Council \(SISAC\)](#)
- [Texas Cybersecurity Council](#)

Biennial Information Security Plan

State law requires state agencies, public universities, and junior colleges to complete an Information Security Plan every even-numbered year. These reports are due June 1 and must be submitted via the SPECTRIM portal.

Go to: [Information Security Plan](#) to access resources to assist you in meeting this statutory requirement.

- [2022 Information Security Plan Instructions \(DOCX\)](#)
- [2022 Information Security Plan Template \(XLSX\)](#)
- [Executive Sign Off Acknowledgement Form \(DOCX\)](#)
- [Vulnerability Report Questionnaire \(PDF\)](#)
- [2022 Information Security Plan Overview Webinar \(on demand\)](#)

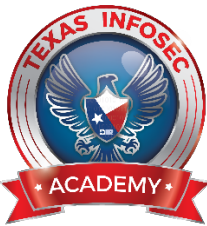
**Have Questions About
the Contents of Your Plan
or Related Legislation?**

Send an email to:

DIRSecurity@dir.texas.gov

Education and Training

Texas InfoSec Academy



The Texas InfoSec Academy provides cybersecurity certification and application developer courses, as well as exam certification vouchers for information technology staff at state agencies and public institutions of higher learning. Go to: [InfoSec Academy FAQ](#)

[Access the InfoSec Academy Portal](#)

Individuals not employed by an eligible customer can find competitively priced security trainings through the [DIR Cooperative Contracts program](#).

Information Security Forum (ISF)



The ISF is an annual educational conference bringing together security and IT professionals from public sector organizations across the state of Texas.

This premier conference focuses on cybersecurity trends and current issues. State and local government employees are eligible to attend at no cost. Go to: [ISF](#)

**Have ISF
Questions?**

Send an email to:

ISF@dir.texas.gov

Statewide Cybersecurity Awareness Training

Texas Government Code 2054.519 requires DIR to certify cybersecurity training programs for state and local government employees. Section 2054.5191 requires state and local government employees to complete a certified training program. Prepare your training program submission in advance by reviewing the application guide. [FY 22-23 Application Guide](#) (PDF 292.75KB)

Go to: [Statewide Security Awareness Training](#) to find:

- [List of certified programs](#),
- Annual timeline for certification of trainings,
- [Training program certification standards](#),
- [Submit a Training Program Recertification Application](#), and
- Training and reporting requirements for state agencies, local governments, and contractors.

End-User Security Awareness Training

DIR offers [eligible customers](#) end-user awareness training that meets the mandatory security training requirements through Proofpoint's Security Awareness Training platform (PSAT).

- [Information for Texans](#)
- [Securing Your Organization](#)
- [Mandatory Security Training Program and FAQ](#)

Phishing Simulation

The PSAT platform allows agencies to develop and deliver targeted and tailored education and training to promote awareness, change user behavior, and help your organization manage risk.

Choose available templates or customize your own campaigns to target your organization's specific needs.

Identify
Risk

Change User
Behavior

Reduce
Exposure

Need End-User Security Awareness Training?

Submit your request here:

[User License Request](#)

Other Security Awareness Resources

Guidance for access additional security awareness resources can be found in the Outreach and Growth Section of this catalog. Go to: [Outreach and Growth](#)

Outreach and Growth

Connecting Public and Private Sectors

DIR hosts and participates in events throughout the year to provide guidance to organizations and highlight the importance of cybersecurity.

Program initiatives include:

- Operating the Texas Information Sharing and Analysis Organization (TX-ISAO),
- Cybersecurity Awareness Month,
- MS-ISAC Kids Contest,
- Texas High School Public Service Announcement Contest,
- [Cyberstart America](#),
- [CyberPatriot](#), and
- Other competitions and contents for Texas youth.

Go to: [Cybersecurity Outreach](#) to learn more about these and other initiatives and follow us on social media.



Learn More:
[DIR Cybersecurity Outreach](#)

Cybersecurity Best Practices for All

- [Tips for Online Safety](#)
- [DIR OCISO Cybersecurity Tips Guide](#)
- [Securing Your Organization](#)

Go to: [Cybersecurity Information for Texans](#)



Texans can find cybersecurity news, tips, and resources to protect their information from a cyberattack on the [Texas.gov Cyber Safety Corner](#).

Texas Cyberstar Certificate Program



The Texas Cyberstar Certificate is recognition of an organization's commitment to cybersecurity best practices and to being a good organizational cybercitizen in the Texas cybercommunity. It does not validate an organization's overall cybersecurity program.

- [Cyberstar Information and Requirements](#)
- [Cyberstar Certificate Program Manual](#)
- [Cyberstar Certificate Request](#)



The TX-ISAO is the primary method OCISO uses to send communications, including the invitation to the OCISO month security meeting, and InfoSec Academy courses. The TX-ISAO is open to any entity in Texas and by joining, you will also have access to the TX-ISAO portal which is built onto the SPECTRIM platform.

The TX-ISAO Portal provides an efficient and secure method to share Indicators of compromise (IOCs) and other actionable intelligence, threat bulletins, and educational opportunities. You can also use the portal to engage with the Texas cybercommunity.

[Submit a request to join the TX-ISAO.](#)

Note: We recommend you request access to the State or Public Higher Education sector and any other applicable sectors.

Monthly Meetings and Webinars

DIR holds two separate monthly meetings to disseminate news, legislative and program updates, and security operations activity.

- **The OCISO Monthly Security Meeting**, held the second Thursday of each month, focuses on news pertinent specifically to state agency, university, and public junior college security employees.

[Click here to join the meeting.](#)

- **The TX-ISAO Monthly Meeting**, held the third Tuesday of each month, is designed for local governments and private organizations, although state agencies are welcome to attend. The agenda includes an educational briefing from the University of Texas at San Antonio Center for Infrastructure Assurance and Security and a technical briefing with updated threat information from Texas A&M University.

[Click here to add this meeting to your calendar.](#)

DIR sends notifications through the TX-ISAO portal for the following webinars and educational events.

The Gartner Series Webinar focuses on current cybersecurity trends and topics.

When: The third Wednesday of every month at 11:00 am (CST).

Who can attend? All interested public sector employees.

OCISO Educational Webinars focus on new trends, cybersecurity technologies, and lessons learned from the vendor community.

When: The fourth Wednesday of every even-numbered month at 11:00 am (CST)

Who can attend? All interested public sector employees.



Communications and Mailing Lists

DIR disseminates regular communications about events, meetings, programs updates, and other information through the following mailing lists.

- Security-officer@lists.state.tx.us – Email discussion list *for designated ISOs* used for official communications and networking among ISOs. All ISOs are automatically subscribed to this list.
- DIRTech@lists.state.tx.us – Dedicated to general technology conversations. Seek advice from other government IT staff, post training opportunities, discuss technical issues, request referrals or opinions about IT products and services, and share resources and expertise.
- DIRTrain@lists.state.tx.us – A list pertaining to training. Seek advice and referrals from other government staff, post training opportunities or needs. discuss issues involving training, request referrals or opinions about products and services, share resources and expertise, and announce meetings and events.

Technology Services

Multi-Factor Authentication (MFA)

The Texas Digital Identity Solution streamlines identify proofing and verification, risk-based multi-factor authentication, and single-sign on (SSO) access so Texas government employees can easily and securely access authorized agency systems with a global unique identifier (GUID). Go to: [Digital Identity Solutions](#).

Solution Components	
Access Management	Identity Management
User Dashboard	Logging and Reporting
Integrated User Repository	Privileged Identity and Access Management*

* Components are available for purchase on a separate license by the consuming agency.

[Best Practices for Multi-Factor Authentication](#)

Endpoint Detection and Response (EDR)

The EDR solution provides 24x7 management of network access points, protecting from risky activity and attacks. The service covers mobile devices, workstations, laptops, and physical or virtual servers. Interested in this service? [Complete this form](#) to be contacted about service options.

Managed Security Services (MSS)

AT&T security products under the MSS contract are available to state agencies, institutions of higher education, cities and counties, special districts, and school districts. Go to: [Managed Security Services](#). Available MSS services include:

- Security Monitoring and Device Management
- Incident Response
- Risk and Compliance

[Learn More:
Managed Security Services
MSS Contracts Overview](#)

Texas Cybersecurity Framework (TCF) Assessments

The Texas Cybersecurity Framework (TCF) uses common language and control objectives in alignment with the National Institute of Standards and Technology (NIST) to help organizations identify, assess, and manage cybersecurity risks in their environment based on business needs. Go to: [TCF](#)

Eligible Customers
may request a TCF
assessment funded by DIR.

TCF Control Objectives and Definitions

The TCF is structured to determine maturity of each security control objective and gauge the maturity of an organization based on a defined model.

Maturity Level	Keywords	Description
0	None, Non-existent	There is no evidence of the organization meeting the objective.
1	Ad-hoc, Initial	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the objective
2	Consistent, Repeatable	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.
3	Compliant, Defined	The organization has documented, detailed approach to meeting the objective, and regularly measure its compliance.
4	Risk-based, Managed	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
5	Efficient, Optimizes	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

- Existing customers can request this service using the STS Service Catalog item, [MSS Texas Cyber Security Framework](#).
- New eligible customers interested in this service can [complete this form to Request a TCF Assessment](#) and a representative will contact you.

Penetration Testing

The MSS program offers penetration testing which can determine how vulnerable the organization's critical systems and sensitive information are to a compromise or attack.

- Existing customers can request this service using the STS Service Catalog item, [MSS Penetration Testing](#).
- New customers interested in this service can [complete this form](#) to be contacted about options to meet your business needs.

MSS offers a [remediation verification service](#) through a separate request following a pen test. This request may only be submitted within 60 days of approval of the Project Acceptance Letter (PAL) from the original external network penetration test. Requests past 60 days require a new RFS request for penetration testing and incur an additional cost.

Purchasing IT Services Through DIR Cooperative Contracts

Through the [Cooperative Contract Program](#), DIR leverages the purchasing power of the State to negotiate contracts and procure a wide variety of IT products and services. DIR is continuously expanding these offerings to meet customer needs.

[Learn More:
Cooperative
Customer Eligibility](#)

Training courses offered through Cooperative Contracts include:

- Data Analytics,
- Networking and Wireless Training,
- Project Management, and
- Application and Web Programming.



Go to: [Cooperative Contracts](#)



In some instances, other states may purchase services through [DIR Cooperative Contracts](#).

The DIR Resource Library

DIR's website contains over 1,000 technology-related reports, policies, standards, guidelines, procedures, and presentations. Go to: [Resource Library](#)

Search Documents, Videos and More:

Enter keywords here... [Search](#)

Topic: Type: Resources for:

Topic:	Type:	Resources for:
Select All	Select All	Select All
<input type="checkbox"/> Administration	<input type="checkbox"/> Audit	<input type="checkbox"/> EIR Accessibility Coordinators
<input type="checkbox"/> General	<input type="checkbox"/> Form	<input type="checkbox"/> Multiple Public Sector
<input type="checkbox"/> Audit	<input type="checkbox"/> Guidelines	<input type="checkbox"/> General
<input type="checkbox"/> Board	<input type="checkbox"/> News/Events	<input type="checkbox"/> Information Resources Managers (IRMs)
<input type="checkbox"/> Collaboration	<input checked="" type="checkbox"/> Policy	<input checked="" type="checkbox"/> Information Security Officers (ISOs)
<input type="checkbox"/> Event Materials	<input type="checkbox"/> Report/Presentation	<input type="checkbox"/> Other (auditors, agencies, public)
<input type="checkbox"/> Multiple Public Sector	<input type="checkbox"/> Standard Operating Procedure	<input type="checkbox"/> Procurement Professionals
<input type="checkbox"/> Procurement	<input type="checkbox"/> Tool/Template	<input type="checkbox"/> Vendors
<input checked="" type="checkbox"/> Security	<input type="checkbox"/> Training	
<input type="checkbox"/> State Agencies	<input type="checkbox"/> User Guide	
<input type="checkbox"/> Telecom		

At the bottom of the [Resource Library Page](#) landing page, you will find links to resources by organization type.



[State Agencies](#)



[Higher Education](#)



[Local Government](#)



[School Districts](#)

Other Resources and Partner Organizations

Resources for Information Security Officers (ISOs)

The ISO will be DIR's main contact for cybersecurity-related issues.

Go to: [Information Security Officers](#). If you are ready to designate an ISO for your organization or change your current designation, [use this form](#).

- [The State of Texas Guide to Cybersecurity Incident Response](#)
- [The State of Texas Guide to Cybersecurity Resources](#)
- [Insights from the Cybersecurity and Infrastructure Security Agency](#)
- [OCISO Cybersecurity Tips Guide](#)
- [Federal Ransomware Tip Sheet](#)
- [DHS Government Tip Card](#)



Other Reporting and Complaint Resources

- [Federal Trade Commission](#)
- [US-Computer Emergency Response Team \(US-CERT\)](#)
- [FBI Internet Crime Complaint Center \(IC3\)](#)
- [Texas DPS Computer Information Technology Electronic Crime Unit](#)
- [Texas Division of Emergency Management \(TDEM\)](#)



Sign Up for Security News, Bulletins, and Updates

Learn more about a variety of technology-related topics and collaborate with others online. Go to [collaboration](#) to see available discussion lists.

Other General Security Resources

Find additional cybersecurity information and tools from cybersecurity leaders:

- [DIR Guide to Cybersecurity Resources](#)
- [Exercise and Preparedness Tools | FEMA](#)
- [DIR Virtual Collaboration Tools Security Tips](#)
- [US CERT CISA Tips for Home Network](#)
- [Texas.gov Cyber Safety Corner](#)
- [NSA Best Practices for Securing Your Home Network](#)
- [US CERT CISA Tips for Home and Business](#)
- [TEA Best Practices for Video Learning](#)
- [Tabletop Exercises \(TTX\) | cisecurity](#)

[Malicious Domain Blocking and Reporting \(MDBR\)](#) is available at no cost to US State, Local, Tribal, and Territorial (SLTT) government members of the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Request a Gartner Professional License

Open enrollment for the Gartner Technical Professional License is offered. If no seat is available at the time of your request, you will be put on a waiting list and notified when a seat becomes available. [Request your license](#).

Other Cybersecurity Community Resources

- The [Texas Cybersecurity Council](#) was created by the Legislature under DIR to develop enduring partnerships between private and public sector organizations and a cybersecurity workforce to protect technology from increasing threats.
- [Information Security Advisory Committee \(SISAC\)](#) is a committee made up of information security professionals from state and local government, that convenes monthly and is led by the Texas Chief Information Security Officer (CISO).
- [Multi-State Information Sharing and Analysis Center \(MS-ISAC\)](#) is a membership-based collaborative working to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial (SLTT) governments.
- [MS-ISAC Membership Application](#)
- [Cybersecurity and Infrastructure Security Agency \(CISA\) Cyber Essentials](#)
- [Texas Division of Emergency Management \(TDEM\)](#)

Reporting Dates to Remember

School Districts and Local Government

Report/Survey	School Districts	Local Government	DIR	Date	Year
Cybersecurity Awareness Training Complete	Input via Web Form		Collect	August 31	Even/Odd
Cyber Threats or Cybersecurity Incidents	TX-ISAO. Submit a Threat Report to TX-ISAO		N/A	ASAP	Even/Odd

State Agencies, Institutions of Higher Education, and Public Junior Colleges

Report/Survey	State Agency	Institution of Higher Education	Public Junior College	DIR	Date	Year
<u>Cybersecurity Awareness Training Complete</u>	Input via Web Form			Collect	August 31	Even/Odd
Information Security Assessment and Report	*See Note Below			Collect	Within 60 Days of Completion	Even
Information Security Plan Data Plan for Mobile/ Web Application Consolidated Report on Information Security Vulnerability Report Executive Written Acknowledgment of Risk	Input via SPECTRIM			Collect	June 1	Even
<u>Prioritization of Cybersecurity and Legacy Systems (PCLS)</u>	As Needed	N/A	N/A	Collect	Prior to LAR Appropriations Request Due Date	Even/Odd
Security Breach Notification (All Incidents) Security Breach Post-Mortem Report	Input via SPECTRIM			Collect	Within 48 Hours	Even/Odd
					Within 10 Days of Closure After Breach Incident	Even/Odd
Security Breach Notification (of 250+ Texans)	<u>Submit to Office of the Attorney General (OAG) Data Breach Reporting</u>			N/A	ASAP	Even/Odd
Election Data Breach	<u>Contact the Secretary of State</u>			N/A	ASAP	Even/Odd

* Within 60 days of completion of a security assessment, the report deliverable must be submitted to DIR. If DIR funded a TCF Assessment for you, DIR receives a copy of the report upon completion, fulfilling this requirement. If your assessment was completed another way, contact DIRSecurity@dir.texas.gov for further instructions on submitting the report.



OCISO DIR Security Services
DIRSecurity@dir.texas.gov