Transforming How Texas Government Serves Texas

Texas Cyberstar Certificate

Program Manual

Texas Department of Information Resources

May 1, 2022

Contents

Overview

Texas Government Code (TGC), section 2054.5181, requires the state cybersecurity coordinator to establish a Cyberstar Certificate Program to recognize public and private entities in Texas that implement the best practices for cybersecurity. The state cybersecurity coordinator is part of the Office of the Chief Information Security Officer (OCISO) within the Texas Department of Information Resources (DIR). The state cybersecurity coordinator and OCISO are responsible for overseeing cybersecurity in Texas, including developing and sharing best practices so entities will be better positioned to prevent and respond to cybersecurity threats.

This document describes the requirements to obtain and maintain a Cyberstar certificate. The certificate indicates the entity's compliance with the program's established requirements and does not alter any other regulatory or statutory obligations.

Approach

The cybersecurity coordinator seeks to provide support and resources to strengthen security throughout Texas. The Texas Cyberstar Certificate Program enhances this goal by encouraging cybersecurity best practices and promoting some of DIR's services and recommendations to public and private sector entities. Entities certified through the program may include the certification in advertisements and other public communications.

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 or its ability to withstand an attempted cyber breach, hack, attack, etc.

Requirements

In alignment with Government Code section 2054.5181, the state cybersecurity coordinator, in consultation with the Texas Cybersecurity Council, selected the following five criteria for entities seeking to obtain a Cyberstar certificate. An entity must:

1) Adopt a cybersecurity risk management program including:

   a) Executing a leadership declaration that affirms security as a priority.

   b) Identifying a representative to serve as a liaison for security matters.

   c) Developing and routinely updating security policies that align with the organization's security priorities.

   d) Including information security in procurement processes.

2) Provide appropriate training and information for employees by:

   a) Ensuring employees supporting the program or product annually complete a DIR-certified cybersecurity training program.

b) Maintaining compliance with DIR's published Information Resources Employees Continuing Education Guidelines for Cybersecurity.

3) Maintain consistency with National Institute of Standards and Technology (NIST) standards for cybersecurity by:

a) Adopting a security framework that is aligned with NIST, ex. the Texas Cybersecurity Framework.

b) Implementing and testing back-ups.

c) Developing and testing an incident response plan.

d) When procuring cloud services, prioritizing TX-RAMP certified products.

4) Incorporate public service announcements to encourage cybersecurity awareness by:

a) Issuing public service announcements to promote cybersecurity awareness or leveraging social media platforms to share best practices with customers.

5) Coordinate with local and state governmental entities by:

a) Sharing information with the community through joining the Texas Information Sharing and Analysis Organization (TX-ISAO). Additional engagement activities could include participating in a regional cybersecurity working group, implementing a mutual aid agreement for security incidents, or partnering with a school to sponsor a Cyber Patriot team or promote CyberStart America.

Request

Entities seeking to obtain a Cyberstar certificate can request the form on the DIR website, https://dir.texas.gov/information-security. Certificates will be awarded within each calendar year. Entities will be required to provide:

- Entity information:
  - Name (as registered with the Texas Comptroller of Public Accounts, for private sector)
  - Mailing address
  - Phone number
  - Website
- Requester information:
  - Legal name
  - Title
  - Work mailing address
  - Work phone number
  - Work email address
- The name of the program or product the entity is requesting a Cyberstar certificate for.

- Information that demonstrates the entity is meeting the certificate requirements:
  - Copy of leadership declaration affirming security as a priority, signed by a member of executive management.
  - Name and contact information for representative serving as liaison for security matters.
  - Selected DIR certified cybersecurity training program.
  - The name of the adopted security framework.
  - Details on how the entity is incorporating public service announcements to encourage cybersecurity awareness.
  - Details on how the entity is coordinating with local and state governmental entities.

The requester, and by correlation the entity that the certificate is being requested for, will be required to digitally sign a certification that they are compliant with all the requirements.

- Additional information may be requested to determine compliance.

Approval

Upon receiving each request, DIR will evaluate the program information and will review each application for conformance to the best practices and standards listed above.

Renewal

Entities seeking to have their programs reapproved after an initial certificate must submit a request via the DIR website.

Failure, Disqualification, and Revoking Certificates

Certain activities and conditions may cause an entity to fail or to be disqualified from earning a Cyberstar certificate. Additional conditions will cause the immediate revocation of any certificates, as outlined below. DIR will provide reasoning for each failure, disqualification, or revocation and the entity may resubmit a request for certificate after remediation of any issues.

Failure

If an entity fails to achieve a Cyberstar certificate because it failed to provide the required information or to meet the criteria required for a certificate, that entity may not reapply for a Cyberstar certificate until the first anniversary of the unsuccessful request.

Disqualification

Conditions that disqualify an entity from a Cyberstar certificate include the following:

- If the entity is owned, wholly or in part, by an individual or other entity that is banned from doing business with or within either the United States of America or the State of Texas; or

- The entity being barred from access to critical infrastructure as defined in Texas Business and Commerce Code chapter 113; or
- Appearance on the Texas Comptroller or Public Accounts' debarred vendor list, during the period of their disbarment.

Entities that have been disqualified may not apply for a certificate until the condition that resulted in their disqualification has been removed or first anniversary of their last request, whichever is later.

Revoking Certificates

If an entity that received a Cyberstar certificate later meets any of the conditions for disqualification outlined above, any existing Cyberstar certificates awarded to that entity will be revoked.

A Cyberstar certificate may also be revoked under the following conditions:

- Changing the name of the program that has been Cyberstar certified. Entities that change the name of the program must request a new certificate under the new name of the program.
- Sale, dissolution, or merger in whole or in part, of the entity that has an interest in the Cyberstar-certified program. Any certified programs belonging to the entity must re-apply for a certificate.
- The program awarded the Cyberstar certificate is the victim of a successful cyberattack. Entities may re-apply on the first anniversary of the cyberattack once they remediate all identified issues relating to the cyberattack and complete a new security assessment on the program.
- There are material changes to the cybersecurity stance of the program that earned a Cyberstar certificate. Programs that make material changes to their cybersecurity stance must re-apply for a certificate.

Expiration

A Cyberstar certificate is valid only for the 12-month period immediately following the award of the certificate. This is in alignment with the training requirements necessary to be Cyberstar certified.

Usage Rights

Logos and certificate documents awarded as part of the Cyberstar program can be used as evidence of certification by the entire program. Only the appropriate logos awarded may be used in promoting the program's certificate status to customers, provided:

- The logo may not be modified in any way.
- When displayed, the size of the logo is equal to or smaller than the program provider's logo.

- The logo is used only to communicate the certificate status of the program to customers.
- No other use of the logo is authorized without obtaining prior written permission from DIR for use.

Logos may be updated each year with awarding of or renewal of certificate.

Resources

The following resources are provided to help entities meet the requirements to be awarded a Texas Cyberstar Certificate, under Section 2054.5181 of the Texas Government Code.

Requirement	Resource	Link
1a. Executing a leadership declaration that affirms security as a priority.	Leadership declaration template	See Appendix A
1c. Developing and routinely updating security policies that align with the organization's security priorities.	A library of comprehensive cybersecurity policy templates from the SANS Institute	https://www.sans.org/information-security-policy/
2a. Ensuring employees supporting the program or product annually complete a DIR-certified cybersecurity training program.	Details on the certified cybersecurity training programs, including criteria, how to request certification of a training program, and timelines for training program evaluation	https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training
2b. Maintaining compliance with DIR's published Information Resources Employees Continuing Education Guidelines for Cybersecurity.	Continuing education guidelines for cybersecurity training for Information Resources Employees	https://dir.texas.gov/resource-library-item/information-resources-employees-continuing-education-guidelines
3a. Adopting a security framework that is aligned with NIST, ex. the Texas Cybersecurity Framework.	NIST Standards	https://www.nist.gov/cyberframework
	Texas Cybersecurity Framework	https://dir.texas.gov/information-security/security-policy-and-planning/texas-cybersecurity-framework
3c. Developing and testing an incident response plan	Texas DIR Incident Response Team Redbook Template	https://dir.texas.gov/resource-library-item/texas-dir-incident-response-team-redbook-template
3d. When procuring cloud services, prioritizing TX-RAMP certified products.	TX-RAMP is a state risk and authorization management program that provides a standardized approach for	https://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp

Requirement	Resource	Link
	security assessment, authorization, and continuous monitoring of cloud computing services.	
5a. Sharing information with the community through joining the Texas Information Sharing and Analysis Organization (TX-ISAO). Additional engagement activities could include participating in a regional cybersecurity working group, implementing a mutual aid agreement for security incidents, or partnering with a school to sponsor a Cyber Patriot team or promote CyberStart America.	The Texas ISAO is 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.	https://dir.texas.gov/information-security/txisao
	The Texas Framework for Mutual Aid Agreements for Security Incidents is a framework for regional cybersecurity working groups to execute mutual aid agreements that allow state and local entities, the private sector, and the incident response team to assist with responding to a cybersecurity event in Texas.	https://dir.texas.gov/resource-library-item/texas-framework-mutual-aid-agreements-security-incidents
	Cyber Patriot is a program for students in grades K-12 to inspire students towards careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines.	https://www.uscyberpatriot.org/
	CyberStart America is a program for students in grades 9th-12th to learn about cybersecurity through a series of games and challenges.	https://www.cyberstartamerica.org/

Appendix A

Leadership Declaration Template

By signing this document, I acknowledge that the role of information security is to manage information risk to an acceptable level to meet organizational goals, and I commit to making information security a priority.

Further, I understand and agree that:

- I am ultimately responsible for the organization's information resources;
- I, or a designated representative, will:
    - administer information security requirements;
    - allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the organization lead;
    - ensure that senior management and information-owners, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control;
    - ensure that the organization has trained personnel to assist the organization in complying with security requirements and related policies;
    - approve high residual risk management decisions;
    - review and approve, at least annually, the organization's information security program; and
    - ensure that information security management processes are integrated with strategic and operational planning processes.

_____(Signature) _____ (Date)

_____(Printed name) _____(Title)