2024 – DIR Grant Program

- State and Local Cybersecurity Grant Program Mitigation.
- Grant Announcement - https://egrants.gov.texas.gov/fundingopp/state-and-local-cybersecurity-grant-program-slcgp-mitigation-projects-fy-2025
- Grant Number: 5191401

Overview

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

This program will support efforts to address imminent cybersecurity threats to state and local information systems by providing funding to implement investments that support local governments with managing and reducing systemic cyber risk associated with the objectives listed below:

Objective 1 - Governance and Planning: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Objective 2 – Assessment and Evaluation: Understand the current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
Objective 3 - Mitigation: Implement security protections commensurate with risk.
Objective 4 – Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Eligibility Requirements

Cybersecurity Training Requirement
Local units of governments must comply with the Cybersecurity Training requirements described in Section 772.012 and Section 2054.5191 of the Texas Government Code. Local governments determined to not be in compliance with the cybersecurity requirements

required by Section 2054.5191 of the Texas Government Code are ineligible for OOG grant funds until the second anniversary of the date the local government is determined ineligible. Government entities must annually certify their compliance with the training requirements using the Cybersecurity Training Certification for State and Local Government. A copy of the Training Certification must be uploaded to your eGrants application. For more information or to access available training programs, visit the Texas Department of Information Resources Statewide Cybersecurity Awareness Training page.

Criminal History Reporting

Entities receiving funds from PSO must be located in a county that has an average of 90% or above on both adult and juvenile dispositions entered into the computerized criminal history database maintained by the Texas Department of Public Safety (DPS) as directed in the *Texas Code of Criminal Procedure, Chapter 66*. The disposition completeness percentage is defined as the percentage of arrest charges a county reports to DPS for which a disposition has been subsequently reported and entered into the computerized criminal history system.

Counties applying for grant awards from the Office of the Governor must commit that the county will report at least 90% of convictions within five business days to the Criminal Justice Information System at the Department of Public Safety.

Uniform Crime Reporting (UCR)

Eligible applicants operating a law enforcement agency must be current on reporting complete UCR data and the Texas specific reporting mandated by 411.042 TGC, to the Texas Department of Public Safety (DPS) for inclusion in the annual Crime in Texas (CIT) publication. To be considered eligible for funding, applicants must have submitted a full twelve months of accurate data to DPS for the most recent calendar year by the deadline(s) established by DPS. Due to the importance of timely reporting, applicants are required to submit complete and accurate UCR data, as well as the Texas-mandated reporting, on a no less than monthly basis and respond promptly to requests from DPS related to the data submitted.

Entities That Collect Sexual Assault/Sex Offense Evidence or Investigate/Prosecute Sexual Assault or Other Sex Offenses

In accordance with Texas Government Code, Section 420.034, any facility or entity that collects evidence for sexual assault or other sex offenses or investigates or prosecutes a sexual assault or other sex offense for which evidence has been collected, must participate in the statewide electronic tracking system developed and implemented by the Texas Department of Public Safety. Visit DPS's Sexual Assault Evidence Tracking Program website for more information or to set up an account to begin participating. Additionally, per Section 420.042 "A law enforcement agency that receives evidence of a sexual assault or other sex offense...shall submit that evidence to a public accredited crime laboratory for analysis no later than the 30th day after the date on which that evidence was received." A law enforcement agency in possession of a significant number of Sexual Assault Evidence Kits (SAEK) where the 30-day window has passed may be considered noncompliant,

Program Requirements

Participation in Cybersecurity & Infrastructure Security Agency (CISA) services

All grantees will be required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

1. Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
2. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page

Nationwide Cyber Security Review
Grantees will be required to complete the Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for each recipient agency should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. For more information about the NCSR, visit: https://www.cisecurity.org/ms-isac/services/ncsr/.

Texas Information Sharing and Analysis Organization (TX-ISAO)
Eligible applicants are required to join the Texas Information Sharing and Analysis Organization (TX-ISAO): a free membership to a forum for entities in Texas to share information regarding cybersecurity threats, best practices, and remediation strategies. To request membership, visit: https://qat.dir.texas.gov/request-list-access.html.

Overall Certification

Each applicant agency must certify to the specific requirements detailed above as well as to comply with all requirements within the PSO Funding Announcement, the *Guide to Grants*, the *Grantee Conditions and Responsibilities*, any authorizing or applicable state and federal statutes and regulations to be eligible for this program.