Name:

State and Local Cybersecurity Grant Program (SLCGP) – Mitigation Projects, FY 2025

Available
01/15/2024

Due Date
03/14/2024

Purpose:

The State and Local Cybersecurity Grant Program (SLCGP) supports cybersecurity efforts to address imminent cybersecurity threats to local information systems including implementing investments that support local governments with managing and reducing systemic cyber risk associated with the SLGCP 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.

The purpose of this announcement is to solicit applications for Objective 3 - Mitigation projects.

Information about funding opportunities related to other SLCGP Objectives is available on the *Funding Opportunities* tab of the eGrants homepage.

Available Funding:

Federal funds are authorized under Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g). State and Local Cybersecurity Grant Program (SLCGP) funds are made available through a Congressional appropriation to the United States

Department of Homeland Security (DHS). All awards are subject to the availability of appropriated federal funds and any modifications or additional requirements that may be imposed by law.

Eligible Organizations:

1. Units of local government;
2. Federally recognized Native American tribes

Application Process:

Applicants must access the PSO's eGrants grant management website at https://eGrants.gov.texas.gov to register and apply for funding. Applicants should select the Criminal Justice Division (CJD) as the desired funding agency when beginning the application.

Key Dates:

Action	Date
Funding Anouncemtent Release	01/15/2024
Online System Opening Date	01/15/2024
Final Date to Submit and Certify an Application	03/14/2024 at 5:00PM CST
Earliest Project Start Date	09/01/2024

Project Period:

Projects selected for funding must begin on or after September 1, 2024 and expire on or before August 31, 2025.

Funding Levels

Minimum: $10,000.00
Maximum: None.
Match Requirement: 10%.

Standards

Grantees must comply with standards applicable to this fund source cited in the Texas Grant Management Standards (TxGMS), Federal Uniform Grant Guidance, and all statutes, requirements, and guidelines applicable to this funding.

Eligible Activities and Costs

All SLCGP **Objective 3 Mitigation** projects must support the implementation of the approved State SLCGP Plan. Additionally, projects can only support one-time services that reduce

cybersecurity risks to; and identify, respond to, and recover from cybersecurity threats to information systems owned or operated by or on behalf of local governments within the Texas. Project examples include:

1. **Multi Factor Authentication:** Implementing multi-factor authentication for all remote access and privileged accounts.
2. **Data Encryption:** Implementing data encryption for data at rest and data in transit.
3. **End-of-Support (EoS)/End-of-Life (EoL) Hardware/Software:** End use of unsupported EoS/ (EoL) software and hardware.
4. **Default Passwords:** Prohibiting use of known/fixed/default passwords and credentials on all systems.
5. **Backups:** Ensuring the ability to reconstitute critical systems (backups).
6. **.gov Domain:** Migration to the .gov domain.
7. **Endpoint Detection and Response:** Implementing Endpoint Detection and Response.
8. **Cloud Migration:** Migrating applications and data to the cloud.
9. **Uninterruptible Power Supply (UPS) Backup Power:** Deploying UPS systems to support critical systems.
10. **Firewalls:** Implementing web application firewalls to monitor and filter web traffic.
11. **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** Implementing IDS/IPS to detect and prevent cyber-attacks.
12. **Vulnerability Patching:** Implementing patching solution to patch vulnerabilities in IT assets.
13. **Web Filtering:** Implementing web filtering solution to scan web traffic for cyber threats.
14. **Virtual Private Network (VPN):** Implementing VPN solutions to encrypt all traffic to/from remote users.

Program-Specific Requirements

1. All Grantees will be required to participate in a limited number of free services by the Cybersecurity & Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of an application but is a post-award requirement.

- **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.

- **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.

2. Grantees will be required to complete the most recent 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/.

3. 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.

Eligibility Requirements

1. 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 Governments. 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.

2. 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. This 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.

3. 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.

4. 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.

5. Eligible applicants must be registered in the federal System for Award Management (SAM) database and have an UEI (Unique Entity ID) number assigned to its agency (to get registered in the SAM database and request an UEI number, go to https://sam.gov/).
Failure to comply with program or eligibility requirements may cause funds to be withheld and/or suspension or termination of grant funds.

Prohibitions

Grant funds may not be used to support the unallowable costs listed in the **Guide to Grants** or any of the following unallowable costs:

1. To pay a ransom;

2. For recreational or social purposes;

3. To pay for cybersecurity insurance premiums;

4. To acquire land;

5. To construct, renovate, remodel, or perform alternations of buildings or other physical facilities including but not limited to:

- Modifications to existing buildings or structures;
- Installation or replacement of equipment where the equipment is physically attached to walls, ceilings, floors or doors;
- Installation or replacement of racks that involve attaching racks to floors or walls;
- Installation of new equipment cabling where new holes are made through walls, floors, or ceilings;
- Installation of new conduit onto existing walls, ceilings, or floors;
- Floor raising to install new cabling;
- Installation of electrical outlets;
- Installation of uninterrupted power supply units (UPS) that involved attaching to floors or walls or new cabling through walls, ceilings, or floors;
- Any activities (grant funded or not) that are connected to the grant funded project that involve the building utility infrastructure such as installing new electrical, water, or gas lines;
- Installation of generators;
- Installation of new equipment at communications towers or building roofs such as antennas or internet systems such as Starlink or satellite dishes;
- Any interior renovations to office spaces that change the layout such as removing walls or creating new walls. Also includes replacing or hardening of doors and windows;
- Installation or replacement of fencing or bollards;
- Any activities that involve ground disturbance;

6. For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity; or

7. Any other prohibition imposed by federal, state, or local law

Selection Process

Application Screening: PSO will screen all applications to ensure that they meet the requirements included in the funding announcement. SLCGP applications will be reviewed through a two-phased State and Federal review process for completeness, adherence to programmatic guidelines, and feasibility.

State Review:

1. Merit Review: The Texas SLCGP Planning Committee will review applications to understand the overall demand for the project, cost effectiveness, feasibility and alignment with the objectives listed in the State's SLCGP Plan.
2. PSO will consider comments and recommendations from the SLCGP Planning Committee along with other factors and make all final funding recommendations to DHS/CISA. Other factors may include cost effectiveness, overall funds availability, priorities and strategies, legislative directives, and geographic distribution. PSO may not recommend funding for all applications or may only recommend part of the amount requested. In the event that funding requests exceed available funds, PSO may revise projects to address a more limited focus.

Federal Review: DHS/CISA will evaluate whether proposed projects are: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the period of performance. Projects must be approved by DHS/CISA before PSO releases an award.

Contact Information

For more information, contact the eGrants help desk at eGrants@gov.texas.gov or (512) 463-1919.

Total Funds
$TBD