Print This Page

Agency Name: Fort Bend County
Grant/App: 5747301 **Start Date:** 1/1/2027 **End Date:** 12/31/2027

Project Title: Cybersecurity Mitigation
Status: Application Pending Submission

Eligibility Information

Your organization's Texas Payee/Taxpayer ID Number:
174600196

Application Eligibility Certify:
Created on:1/13/2026 10:21:38 AM By:Emmanuel Effiong

Profile Information

Applicant Agency Name: Fort Bend County
Project Title: Cybersecurity Mitigation
Division or Unit to Administer the Project: Fort Bend County Information Technology
Address Line 1: 500 Liberty St
Address Line 2:
City/State/Zip: Richmond Texas 77469-4428
Start Date: 1/1/2027
End Date: 12/31/2027

Regional Council of Goverments(COG) within the Project's Impact Area: Houston-Galveston Area Council
Headquarter County: Fort Bend
Counties within Project's Impact Area: Fort Bend

Grant Officials:
Authorized Official
Name: KP George
Email: county.judge@fortbendcountytx.gov
Address 1: 301 Jackson Street
Address 1: Office of the County Judge
City: Richmond, Texas 77469
Phone: 281-341-8608 Other Phone: 281-633-7769
Fax: 832-471-1858
Title: The Honorable
Salutation: Judge
Position: County Judge

Financial Official
Name: Robert Sturdivant
Email: Ameena.Khan3@fortbendcountytx.gov
Address 1: 301 Jackson, Suite 533
Address 1:
City: Richmond, Texas 77469
Phone: 281-341-3769 Other Phone:
Fax:
Title: Mr.
Salutation: Mr.
Position: County Auditor

Project Director
Name: Arthur Lattimore
Email: arthur.lattimore@fortbendcountytx.gov
Address 1: 500 Liberty Street
Address 1:

City: Richmond, Texas 77469
Phone: 346-840-1881 Other Phone:
Fax:
Title: Mr.
Salutation: --- Select One ---
Position: CyberSecurity Supervisor Fort Bend County

Grant Writer
Name: Emmanuel Effiong
Email: emmanuel.effiong@fortbendcountytx.gov
Address 1: 500 Liberty Street
Address 1:
City: Richmond, Texas 77469
Phone: 281-725-4687 Other Phone: 281-725-4687
Fax:
Title: Mr.
Salutation: --- Select One ---
Position: IT Security Analyst II

Grant Vendor Information

Organization Type: County
Organization Option: applying to provide services to all others
Applicant Agency's State Payee Identification Number (e.g., Federal Employer's Identification (FEI) Number or Vendor ID): 174600196
Unique Entity Identifier (UEI):

Narrative Information

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

Resolution from Governing Body
Applications from nonprofit corporations, local units of governments, and other political subdivisions must submit a fully executed resolution with the application to be considered eligible for funding. The resolution must contain the following elements (see Sample Resolution):

- Authorization by your governing body for the submission of the application to the Public Safety Office (PSO) that clearly identifies the name of the project for which funding is requested;
- A commitment to provide all applicable matching funds;
- A designation of the name and/or title of an authorized official who is given the authority to apply for, accept, reject, alter, or terminate a grant;
- A designation of the name and/or title of a financial officer who is given the authority to submit financial and/or performance reports or alter a grant; and
- A written assurance that, in the event of loss or misuse of grant funds, the governing body will return all funds to PSO.

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.

Compliance with State and Federal Laws, Programs and Procedures – Local Units of Government
Local units of government, including cities, counties and other general purpose political subdivisions, as appropriate, and institutions of higher education that operate a law enforcement agency, must comply with all aspects of the programs and procedures utilized by the U.S. Department of Homeland Security ("DHS") to: (1)

notify DHS of all information requested by DHS related to illegal aliens in Agency's custody; and (2) detain such illegal aliens in accordance with requests by DHS. Additionally, counties and municipalities may NOT have in effect, purport to have in effect, or make themselves subject to or bound by, any law, rule, policy, or practice (written or unwritten) that would: (1) require or authorize the public disclosure of federal law enforcement information in order to conceal, harbor, or shield from detection fugitives from justice or aliens illegally in the United States, 8 U.S.C. § 1324(a)(1)(A)(iii); (2) impede federal officers from exercising authority under 8 U.S.C. § 1226(a), § 1226(c), § 1231(a), § 1357(a), § 1366(1), or § 1366(3); (3) encourage or induce an alien to come to, enter, or reside in the United States in violation of law, 8 U.S.C. § 1324(a)(1)(A)(iv); (4) result in the illegal transport or movement of aliens within the United States, 8 U.S.C. § 1324(a)(1)(A)(ii). Lastly, eligible applicants must comply with all provisions, policies, and penalties found in Chapter 752, Subchapter C of the Texas Government Code.

Each local unit of government, and institution of higher education that operates a law enforcement agency, must download, complete and then upload into eGrants the CEO/Law Enforcement Certifications and Assurances Form certifying compliance with federal and state immigration enforcement requirements. This Form is required for each application submitted to PSO and is active until August 31, 2027 or the end of the grant period, whichever is later.

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 https://www.cisa.gov/cyber-hygiene-services.

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.
X I certify to all of the application content and requirements.

Project Summary :
Briefly summarize the project, including proposed activities and intended impact.
Fort Bend County proposes a cybersecurity mitigation project focused on reducing systemic cyber risk through enhanced identity and access controls, privileged access management, and improved security visibility. Aligned with SLCGP Objective 3 – Mitigation, this one-time initiative will deploy tools such as Privileged Access Management (PAM), Multi-Factor Authentication (MFA), and endpoint privilege enforcement to address high-risk attack vectors including credential theft, privilege escalation, and unauthorized system access. The project aims to reduce the likelihood and impact of cyber incidents, improve forensic readiness, and ensure continuity of secure county operations and services.

Problem Statement :
Provide a detailed account of the issues, threats or hazards that your project will target. For federal Homeland Security Grants, include specific references to the regional or state *Threat and Hazard Identification and Risk Assessment (THIRA)*, as applicable.
The county faces growing threats from ransomware, credential compromise, insider misuse, and exploitation of administrative access. Current reliance on shared or default credentials, limited enforcement of least privilege, and inconsistent audit logging elevates the risk of undetected compromise and lateral movement. Regional and statewide THIRA assessments consistently identify ransomware and account compromise as high-impact risks. Without stronger controls around privileged access and authentication, these threats undermine operational resilience and the protection of sensitive data.

Existing Capability Levels :
Describe the existing capability levels, including resources that are currently in place to support this project prior to the use of grant funds.
Fort Bend County maintains foundational cybersecurity controls including perimeter firewalls, endpoint protection, Active Directory authentication, and standard account management policies. Limited MFA coverage and basic logging are in place. However, capabilities are fragmented and heavily manual, with no centralized privileged access enforcement, session auditing, or credential rotation. Visibility into elevated activity across systems remains inconsistent.

Capability Gaps:
Describe the capability gaps which will be addressed by the project. For federal Homeland Security Grants, include specific references to the regional or statewide State Preparedness Report (SPR).
This project addresses key cybersecurity capability gaps: Reliance on shared or static privileged credentials Lack of centralized credential vaulting and session logging Inconsistent enforcement of least privilege across endpoints Partial MFA coverage for privileged and remote access These gaps conflict with the State Preparedness Report (SPR), NIST 800-53 (e.g., AC-2, AC-6, IR-4), and CIS Controls 4, 5, and 16.

Impact Statement :
Describe the project goals/objectives and how this project will maintain capabilities or reduce capability gaps.
This project will measurably reduce cyber risk by: Eliminating shared and default credentials via centralized PAM Enforcing least privilege across all administrative endpoints Applying consistent MFA for privileged and remote access Enhancing logging and auditability of elevated activity The result will be a stronger cybersecurity posture, faster threat detection, and improved incident response capacity—all within the grant period.

Homeland Security Priority Actions:
Identify the Texas Homeland Security Priority Action most closely aligned with this project. Each Priority Action is linked with an *Objective from the Texas Homeland Security Strategic Plan (HSSP)*. List the Priority Action by number and text (e.g. *1.2.3 Expand and enhance the network of human sources that can provide detailed and relevant information on known or suspected terrorist and criminal enterprises*.)
2.1.2 – Enhance cybersecurity and protect critical infrastructure from cyber threats. This project directly advances the Texas Homeland Security Strategic Plan by fortifying local government infrastructure against credential-based attacks and service disruption.

Target Group :
Identify the target group and population expected to benefit from this project.
Primary Beneficiaries: Fort Bend County IT staff and system administrators County departments relying on secure systems Secondary Beneficiaries: Fort Bend County residents, through more secure, uninterrupted services and better protection of personal data

Long-Term Approach:
Describe how the applicant agency will maintain the capabilities supported by this project without additional federal or state funds. If sustainment is dependent upon federal or state grants, describe the ongoing need for future grants, as applicable.
Fort Bend County will sustain these capabilities by budgeting for license renewals, maintenance, and support within its standard IT operational budget. The deployed tools will be integrated into the county's long-term cybersecurity framework without ongoing dependence on state or federal grant funding.

Project Activities Information

SLCGP Instructions for Project Activity Selection

State and Local Cybersecurity Grant Program (SLCGP) applicants should only select one project activity. The eGrants system will allow multiple selections, but each SLCGP subrecipient project must fit into one and only one of the Investment Categories that are listed as project activities under the "Activity List".

Selected Project Activities:

ACTIVITY	PERCENTAGE:	DESCRIPTION
Default Passwords	100.00	This activity implements privileged access management to eliminate shared and default administrative credentials, enforce least privilege across endpoints, and extend MFA coverage for privileged accounts. It supports centralized credential vaulting, rotation, and session logging.

Measures Information

Objective Output Measures

OUTPUT MEASURE	TARGET LEVEL
Number of networks/systems prohibiting the use of known/fixed/default passwords and credentials	3

Objective Outcome Measures

OUTCOME MEASURE	TARGET LEVEL

Custom Output Measures

CUSTOM OUTPUT MEASURE	TARGET LEVEL

Custom Outcome Measures

CUSTOM OUTCOME MEASURE	TARGET LEVEL

Lobbying

For applicant agencies requesting grant funds in excess of $100,000, have any federally appropriated funds been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant loan, or cooperative agreement?

Select the appropriate response:
_ Yes
X No
_ N/A

For applicant agencies that selected either **No** or **N/A** above, have any non-federal funds been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress in connection with this federal contract, loan, or cooperative agreement?
_ Yes
X No
_ N/A

Debarment

Each applicant agency will certify that it and its principals (as defined in 2 CFR Part 180.995):

- Are not presently debarred, suspended, proposed for debarment, declared ineligible, sentenced to a denial of Federal benefits by a State or Federal Court, or voluntarily excluded from participation in this transaction by any federal department or agency;
- Have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; or
- Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in the above bullet; and have not within a three-year period preceding this application had one or more public transactions (federal, state, or local) terminated for cause or default.

Select the appropriate response:
X I Certify
_ Unable to Certify

Enter the debarment justification:

Fiscal Capability Information

Section 1: Organizational Information

*** FOR PROFIT CORPORATIONS ONLY ***

Enter the following values in order to submit the application
Enter the Year in which the Corporation was Founded: 0
Enter the Date that the IRS Letter Granted 501(c)(3) Tax Exemption Status: 01/01/1900
Enter the Employer Identification Number Assigned by the IRS: 0
Enter the Charter Number assigned by the Texas Secretary of State: 0

Enter the Year in which the Corporation was Founded:
Enter the Date that the IRS Letter Granted 501(c)(3) Tax Exemption Status:
Enter the Employer Identification Number Assigned by the IRS:
Enter the Charter Number assigned by the Texas Secretary of State:

Section 2: Accounting System

The grantee organization must incorporate an accounting system that will track direct and indirect costs for the organization (general ledger) as well as direct and indirect costs by project (project ledger). The grantee must establish a time and effort system to track personnel costs by project. This should be reported on an hourly basis, or in increments of an hour.
Is there a list of your organization's accounts identified by a specific number (i.e., a general ledger of accounts)?

Select the appropriate response:
_ Yes
_ No

Does the accounting system include a project ledger to record expenditures for each Program by required budget cost categories?

Select the appropriate response:
_ Yes
_ No

Is there a timekeeping system that allows for grant personnel to identify activity and requires signatures by the employee and his or her supervisor?

Select the appropriate response:
_ Yes
_ No

If you answered 'No' to any question above in the Accounting System section, in the space provided below explain what action will be taken to ensure accountability.

Enter your explanation:

Section 3: Financial Capability

Grant agencies should prepare annual financial statements. At a minimum, current internal balance sheet and income statements are required. A balance sheet is a statement of financial position for a grant agency disclosing assets, liabilities, and retained earnings at a given point in time. An income statement is a summary of revenue and expenses for a grant agency during a fiscal year.
Has the grant agency undergone an independent audit?

Select the appropriate response:
_ Yes
_ No

Does the organization prepare financial statements at least annually?

Select the appropriate response:
_ Yes
_ No

According to the organization's most recent Audit or Balance Sheet, are the current total assets greater than the liabilities?

Select the appropriate response:
_ Yes
_ No

If you selected 'No' to any question above under the Financial Capability section, in the space provided below explain what action will be taken to ensure accountability.

Enter your explanation:

Section 4: Budgetary Controls

Grant agencies should establish a system to track expenditures against budget and / or funded amounts.

Are there budgetary controls in effect (e.g., comparison of budget with actual expenditures on a monthly basis) to include drawing down grant funds in excess of:

a) Total funds authorized on the Statement of Grant Award?
_ Yes
_ No

b) Total funds available for any budget category as stipulated on the Statement of Grant Award?
_ Yes
_ No

If you selected 'No' to any question above under the Budgetary Controls section, in the space provided below please explain what action will be taken to ensure accountability.

Enter your explanation:

Section 5: Internal Controls

Grant agencies must safeguard cash receipts, disbursements, and ensure a segregation of duties exist. For example, one person should not have authorization to sign checks and make deposits.
Are accounting entries supported by appropriate documentation (e.g., purchase orders, vouchers, receipts, invoices)?

Select the appropriate response:
_ Yes
_ No

Is there separation of responsibility in the receipt, payment, and recording of costs?

Select the appropriate response:
_ Yes
_ No

If you selected 'No' to any question above under the Internal Controls section, in the space provided below please explain what action will be taken to ensure accountability.

Enter your explanation:

Budget Details Information

Budget Information by Budget Line Item:

CATEGORY	SUB CATEGORY	DESCRIPTION	OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL	UNIT/%
Equipment	Other Authorized Equipment (Equipment)	DILENEA Secret Server Cloud PAM Line Item Description: Privileged Access Management for vaulting, rotating, and auditing credentials. Aligns with NIST 800-53 AC-2, AC-5, and AC-17. Supports	$21,028.88	$9,012.37	$0.00	$0.00	$30,041.25	1

		zero-trust and passwordless compliance strategies.						
Equipment	Other Authorized Equipment (Equipment)	BeyondTrust Privileged Remote Access Line Item Description: Secure remote access solution for internal and third-party users without VPN. Maps to NIST 800-53 AC-17, SC-12, and SC-13.	$14,049.67	$6,021.28	$0.00	$0.00	$20,070.95	1
Equipment	Other Authorized Equipment (Equipment)	Imprivata Confirm ID – Identity Access + MFA (Quote 1) Line Item Description: Enterprise-grade MFA and authentication management for healthcare and CJIS-aligned use cases. Aligns with NIST 800-53 IA-2, IA-5, and CJIS 5.9.	$20,029.14	$8,583.92	$0.00	$0.00	$28,613.06	1
Equipment	Other Authorized Equipment (Equipment)	Imprivata Confirm ID – EPCS + SSO (Quote 2) Line Item Description: rf IDEAS WAVE ID Nano SDK HID Vertical Nano V2 Black Vertical. Reader - RF proximity reader - USB - black. RF IDeas - Part#: RDR-6012AKU-V2. Adds Single Sign-On and EPCS capabilities for	$23,591.40	$10,110.60	$0.00	$0.00	$33,702.00	1

		medical and CJIS users. Supports compliance with DEA regulations, NIST 800-63, and FIPS 140-2.						

Source of Match Information

Detail Source of Match/GPI:

DESCRIPTION	MATCH TYPE	AMOUNT
General Budget	Cash Match	$33,728.17

Summary Source of Match/GPI:

Total Report	Cash Match	In Kind	GPI Federal Share	GPI State Share
$33,728.17	$33,728.17	$0.00	$0.00	$0.00

Budget Summary Information

Budget Summary Information by Budget Category:

CATEGORY	OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
Equipment	$78,699.09	$33,728.17	$0.00	$0.00	$112,427.26

Budget Grand Total Information:

OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
$78,699.09	$33,728.17	$0.00	$0.00	$112,427.26

Condition Of Fundings Information

Condition of Funding / Project Requirement	Date Created	Date Met	Hold Funds	Hold Line Item Funds

You are logged in as **User Name**: emmanueleffiong