Print This Page

Agency Name: Fort Bend County
Grant/App: 5136001 **Start Date:** 9/1/2024 **End Date:** 8/31/2025

Project Title: Fort Bend County - Cybersecurity Mitigation
Status: Application Pending Submission

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

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

Project Summary :
Briefly summarize the project, including proposed activities and intended impact.
The project aims to enhance cybersecurity capabilities within Fort Bend County by implementing a comprehensive suite of security tools and conducting targeted training programs. Proposed activities include the deployment of ThreatLocker, Tanium, and Infoblox software solutions, along with conducting cybersecurity awareness training sessions for county employees. The intended impact is to strengthen the county's defense against cyber threats, improve incident response capabilities, and safeguard critical infrastructure and data assets.

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.
Fort Bend County faces significant cybersecurity threats, including malware infections, ransomware attacks, and data breaches. The increasing sophistication of cyber threats poses a considerable risk to county operations, critical infrastructure, and citizen data. Without adequate cybersecurity measures in place, the county remains vulnerable to disruptive cyber incidents that could result in financial losses, operational disruptions, and reputational damage.

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 currently relies on a range of cybersecurity tools encompassing endpoint security, vulnerability management, privileged access management, email security, compliance management, and network security. While these measures provide a baseline defense against cyber threats, they lack advanced capabilities such as real-time threat detection, comprehensive endpoint visibility, granular storage policy control, and advanced DNS security features. While effective for basic security functions like endpoint protection and email filtering, these tools require enhancement to effectively combat modern cyber threats.

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).
Lack of Granular Data Access Control: Currently, Fort Bend County lacks granular control over data access, making it challenging to prevent unauthorized copying or transfer of sensitive information. ThreatLocker Storage Control addresses this gap by enabling precise policy control over storage devices, including local folders, network shares, and USB drives. Limited Monitoring and Incident Response Capabilities: The county faces challenges in monitoring storage access activities and responding to security incidents effectively. ThreatLocker Storage Control provides a centralized audit trail of storage access, enhancing monitoring capabilities and streamlining incident response processes. Inadequate Endpoint Management: Fort Bend County struggles with endpoint visibility and management across its network, hindering its ability to detect and manage devices effectively. Tanium addresses this capability gap by offering comprehensive endpoint visibility and control, improving endpoint management capabilities. Delayed Threat Detection and Remediation: The county lacks real-time threat detection capabilities, leading to delays in identifying and addressing security incidents. Tanium's real-time threat detection feature enables prompt detection and remediation of security threats, enhancing the county's cybersecurity resilience. Vulnerabilities in DNS Security: Fort Bend County's current DNS security measures are inadequate, leaving it vulnerable to DNS-based attacks such as malware infections and data exfiltration. Infoblox enhances DNS security by offering advanced DNS security features, protecting against DNS-based threats and strengthening network defense. Inefficient IP Address Management: The county faces challenges in managing IP addresses efficiently and accurately, posing risks to network integrity and availability. Infoblox's IP Address Management (IPAM) capabilities address this gap by facilitating efficient and accurate management of IP addresses, ensuring network integrity and availability.

Impact Statement :
Describe the project goals/objectives and how this project will maintain capabilities or reduce capability gaps.
The project's objectives are to enhance cybersecurity capabilities within Fort Bend County by deploying advanced solutions such as ThreatLocker Storage Control, Tanium, and Infoblox. These solutions aim to address existing capability gaps and maintain a robust security posture by achieving the following objectives: Enhanced Visibility: Implementing ThreatLocker Storage Control, Tanium, and Infoblox will provide comprehensive visibility into network endpoints, storage devices, and DNS traffic. This enhanced visibility will allow Fort Bend County to better understand its network environment, identify vulnerabilities, and detect potential security threats in real-time. Granular Policy Control: By leveraging ThreatLocker Storage Control, the project aims to establish granular policies for controlling access to storage devices, including USB drives, network shares, and local folders. This capability will enable the county to enforce strict data access controls, reducing the risk of unauthorized data transfer or leakage. Improved Incident Response: Tanium's endpoint management and threat detection capabilities will empower Fort Bend County to respond swiftly and effectively to security incidents. By detecting and remediating threats in real-time, the project will enhance the county's ability to contain and mitigate cyber attacks, minimizing their impact on critical infrastructure and services. Strengthened Network Security: Infoblox's DNS security features will bolster Fort Bend County's defenses against DNS-based attacks, such as malware infections and DNS hijacking. By implementing proactive measures to secure DNS traffic, the project will reduce the likelihood of successful cyber-attacks targeting the county's network infrastructure. Centralized Monitoring and Management: The deployment of these advanced cybersecurity solutions will enable Fort Bend County to centralize monitoring and management tasks, streamlining security operations and improving overall efficiency. This centralized approach will facilitate better coordination among security teams and ensure consistent enforcement of security policies across the county's network.

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 priority action directly

corresponds to Objective 2.1 in the Texas Homeland Security Strategic Plan (HSSP), which focuses on strengthening cybersecurity measures and safeguarding critical infrastructure against cyber threats. By deploying ThreatLocker Storage Control, Tanium, and Infoblox, the project aims to bolster cybersecurity capabilities within Fort Bend County, aligning with the overarching objective of enhancing cyber resilience and protecting vital assets from cyberattacks.

Target Group :
Identify the target group and population expected to benefit from this project.
The target group and population expected to benefit from this project encompass various stakeholders: Fort Bend County Government Agencies and Employees: All departments and employees within Fort Bend County will directly benefit from the enhanced cybersecurity measures provided by ThreatLocker Storage Control, Tanium, and Infoblox deployments. This includes improved data protection, streamlined access controls, and strengthened incident response capabilities. Fort Bend County Residents: The general population of Fort Bend County will indirectly benefit from this initiative as it contributes to the stability and reliability of critical infrastructure and public services. Strengthened cybersecurity measures ensure the safety and integrity of county operations, ultimately benefiting residents.

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.
The agency will earmark a portion of its annual budget specifically for cybersecurity initiatives, including the maintenance and renewal of licenses, subscriptions, and support contracts for ThreatLocker Storage Control, Tanium, and Infoblox. By prioritizing cybersecurity within the budgetary framework, the agency ensures ongoing funding for essential tools and services.

Print This Page

Agency Name: Fort Bend County
Grant/App: 5136001 **Start Date:** 9/1/2024 **End Date:** 8/31/2025

Project Title: Fort Bend County - Cybersecurity Mitigation
Status: Application Pending Submission

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
Endpoint Detection and Response	30.00	Projects that implement Endpoint Detection and Response (EDR).
Firewalls	30.00	Projects that implement web application firewalls to monitor and filter web traffic.
Vulnerability Patching	40.00	Projects that implement patching solutions to patch vulnerabilities in IT assets.

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

Print This Page

Agency Name: Fort Bend County
Grant/App: 5136001 **Start Date:** 9/1/2024 **End Date:** 8/31/2025

Project Title: Fort Bend County - Cybersecurity Mitigation
Status: Application Pending Submission

Resolution from Governing Body

Applications from nonprofit corporations, local units of governments, and other political subdivisions must include a resolution that contains the following:

1. 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;
2. A commitment to provide all applicable matching funds;
3. 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 (Note: If a name is provided, you must update the PSO should the official change during the grant period.); and
4. A written assurance that, in the event of loss or misuse of grant funds, the governing body will return all funds to PSO.

Upon approval from your agency's governing body, upload the approved resolution to eGrants by going to the **Upload.Files** tab and following the instructions on Uploading eGrants Files.

Contract Compliance

Will PSO grant funds be used to support any contracts for professional services?

Select the appropriate response:
X Yes
_ No

For applicant agencies that selected **Yes** above, describe how you will monitor the activities of the sub-contractor(s) for compliance with the contract provisions (including equipment purchases), deliverables, and all applicable statutes, rules, regulations, and guidelines governing this project.

Enter a description for monitoring contract compliance:
All contracts and purchases will be approved in the egrants system and will be procured using county purchasing policies and regulations. Contracts and purchases will be monitored by the sub-grantee to ensure deliverables and timelines are met and that the deliverables are as requested.

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

Fiscal Year

Provide the begin and end date for the applicant agency's fiscal year (e.g., 09/01/20xx to 08/31/20xx).

Enter the Begin Date [mm/dd/yyyy]:
10/1/2024
Enter the End Date [mm/dd/yyyy]:
9/30/2025

Sources of Financial Support

Each applicant must provide the amount of grant funds expended during the most recently completed fiscal year for the following sources:
Enter the amount (in Whole Dollars $) of Federal Grant Funds expended:
116214776
Enter the amount (in Whole Dollars $) of State Grant Funds expended:
7053433

Single Audit

Applicants who expend less than $750,000 in federal grant funding or less than $750,000 in state grant funding are exempt from the Single Audit Act and cannot charge audit costs to a PSO grant. However, PSO may require a limited scope audit as defined in 2 CFR Part 200, Subpart F - Audit Requirements.

Has the applicant agency expended federal grant funding of $750,000 or more, or state grant funding of $750,000 or more during the most recently completed fiscal year?

Select the appropriate response:
X Yes
_ No

Applicant agencies that selected **Yes** above, provide the date of your organization's last annual single audit, performed by an independent auditor in accordance with the State of Texas Single Audit Circular; or CFR Part 200, Subpart F - Audit Requirements.

Enter the date of your last annual single audit:
3/31/2023

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:

FFATA Certification

Certification of Recipient Highly Compensated Officers – The Federal Funding Accountability and Transparency Act (FFATA) requires Prime Recipients (HSGD) to report the names and total compensation of each of the five most highly compensated officers (a.k.a. positions) of each sub recipient organization for the most recently completed fiscal year preceding the year in which the grant is awarded if the subrecipient answers **YES** to the **FIRST** statement but **NO** to the **SECOND** statement listed below.
In the sub recipient's preceding completed fiscal year, did the sub recipient receive: (1) 80 percent or more of its annual gross revenue from Federal contracts (and subcontracts), loans, grants (and subgrants) and cooperative agreements; AND (2) $25,000,000 or more in annual gross revenue from Federal contracts (and subcontracts), loans, grants (and subgrants) and cooperative agreements?
_ Yes
X No

Does the public have access to information about the compensation of the senior executives through periodic reports filed under Section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or Section 6104 of the Internal Revenue Code of 1986?
_ Yes
X No

If you answered **YES** to the **FIRST** statement and **NO** to the **SECOND** statement, please provide the name and total compensation amount of each of the five most highly compensated officers (a.k.a. positions) within your agency for the current calendar year. If you answered NO to the first statement you are NOT required to provide the name and compensation amounts. NOTE: ''Total compensation'' means the complete pay package of each of the sub recipient's compensated officers, including all forms of money, benefits, services, and in-kind payments (see SEC Regulations: 17 CCR 229.402).
Position 1 - Name:
Position 1 - Total Compensation ($):
0
Position 2 - Name:
Position 2 - Total Compensation ($):
0
Position 3 - Name:
Position 3 - Total Compensation ($):
0
Position 4 - Name:
Position 4 - Total Compensation ($):
0
Position 5 - Name:
Position 5 - Total Compensation ($):
0

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

1:44 PM

Agency Name: Fort Bend County

Grant/App: 5136001

Start Date: 9/1/2024

Project Title: Fort Bend County - Cybersecurity Mitigation

Status: Application Pending Submission

End Date: 8/31/2025

Fund Source: CY-State and Local Cybersecurity Grant Program

Current Program Manager:

Liquidation Date:

Original Award: $0.00

Current Budget: $0.00

Current Award: $0.00

CFDA: 97.137

OOG Solicitation: State and Local Cybersecurity Grant Program Mitigation Announcement

Eligibility Profile Narrative Activities Measures Budget Documents Cyber.Security Conditions.of.Funding Submit.Application Summary Upload.Files My.Home

Printer Friendly

Capabilities

Identify if this investment focuses on building new capabilities or sustaining existing capabilities.

● New Capabilities (Build)
○ Existing Capabilities (Sustain)

□ Check if these funds will support a project that was previously funded with SLCGP funding

Project Management Step Involved:

Check the step that most closely resembles the phase of the project activities to be completed during the grant period.

Select	Steps	Description	Process
☑	Initiate	The authorization to begin work or resume work on any particular activity.	Involves preparing for, assembling resources and getting work started. May apply to any level, e.g. program, project, phase, activity, task.
□	Plan	The purpose of establishing, at an early date, the parameters of the project that is going to be worked on as well as to try to delineate any specifics and/or any peculiarities to the project as a whole and/or any specific phases of the project.	Involves working out and extending the theoretical, practical, and/or useful application of an idea, concept, or preliminary design. This also involves a plan for moving a project concept to a viable project.
□	Execute	The period within the project lifecycle during which the actual work of creating the project's deliverables is carried out.	Involves directing, accomplishing, managing, and completing all phases and aspects of work for a given project.
□	Control	A mechanism w hich reacts to the current project status in order to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring.	Involves exercising corrective action as necessary to yield a required outcome consequent upon monitoring performance. Or, the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate corrective action as needed.
□	Close Out	The completion of all work on a project. Can also refer to completion of a phase of the project.	Involves formally terminating and concluding all tasks, activities, and component parts of a particular project, or phase of a project.

Milestones

List 3 to 5 milestones of this project, and then list the intended completion date for each milestone.

Milestones should occur throughout the project.

Enter dates as MM-DD-YYYY

Milestone	Completion Date	Edit	Delete
Start procurement process with selecting vendor	10-01-2024	✎	Delete
Execute PO's and contract	01-31-2025	✎	Delete
Receive deliverables	06-01-2025	✎	Delete

Create New Milestone

Note from Grantee to OOG

Save Note from Grantee to OOG

Previous Save and Continue

Save Only

Printer Friendly