Agency Name: Brazoria County, Texas
Grant/App: 5067901 **Start Date:** 9/1/2024 **End Date:** 8/31/2025

Project Title: Breach Attack Simulation
Status: Application Pending AO Certification

Eligibility Information

Your organization's Texas Payee/Taxpayer ID Number:
17460000445019

Application Eligibility Certify:
Created on:1/25/2024 3:33:33 PM By:Russell Webb

Profile Information

Applicant Agency Name: Brazoria County, Texas
Project Title: Breach Attack Simulation
Division or Unit to Administer the Project: Information Systems
Address Line 1: 111 E. Locust
Address Line 2: Suite 305
City/State/Zip: Angleton Texas 77515-4621
Start Date: 9/1/2024
End Date: 8/31/2025

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

Grant Officials:
Authorized Official
Name: L. M. "Matt" Sebesta, Jr.
Email: matts@brazoria-county.com
Address 1: 111 E. Locust Ste 102A
Address 1:
City: Angleton, Texas 77515
Phone: 979-864-1200 Other Phone: 979-864-1695
Fax: 979-849-4655
Title: The Honorable
Salutation: Judge
Position: Brazoria County Judge

Financial Official
Name: Kaysie Stewart
Email: kaysies@brazoria-county.com
Address 1: 111 E. Locust, Rm 303
Address 1:
City: Angleton, Texas 77515
Phone: 979-864-1275 Other Phone:
Fax: 979-864-1585

Title: Ms.
Salutation: Ms.
Position: County Auditor

Project Director
Name: Russell Webb
Email: rwebb@brazoriacountytx.gov
Address 1: 237 E. Locust
Address 1: Suite 505
City: Angleton, Texas 77515
Phone: 979-864-1777 Other Phone: 979-997-1432
Fax:
Title: Mr.
Salutation: Mr.
Position: Director - Information Systems

Grant Writer
Name: Russell Webb
Email: rwebb@brazoriacountytx.gov
Address 1: 237 E. Locust
Address 1: Suite 505
City: Angleton, Texas 77515
Phone: 979-864-1777 Other Phone: 979-997-1432
Fax:
Title: Mr.
Salutation: Mr.
Position: Director - Information Systems

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): 17460000445019
Unique Entity Identifier (UEI): N1GLHP8EWHD9

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.

In response to the escalating and dynamic nature of cyber threats, our organization is undertaking a strategic initiative to implement a Breach Attack Simulation (BAS) solution. This project aims to fortify our cybersecurity posture by proactively identifying and mitigating vulnerabilities within our digital infrastructure through realistic and controlled simulations of potential cyber attacks.

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 contemporary cybersecurity landscape is characterized by an ever-evolving and sophisticated threat environment, presenting organizations with a multitude of issues, threats, and hazards that can compromise the integrity, confidentiality, and availability of their sensitive information. Traditional security measures, while crucial, often fall short in addressing the dynamic nature of cyber threats. In this context, the emergence of Breach Attack Simulation Solutions becomes imperative as organizations seek proactive strategies to identify, assess, and mitigate vulnerabilities in their digital infrastructure. THREATS NOTED ON PAGE 5 OF THE 2023 REGIONAL THIRA. Key Issues, Threats, and Hazards: Dynamic and Evolving Threat Landscape: Issue: The rapid evolution of cyber threats poses a continuous challenge for organizations to keep pace with emerging attack vectors and techniques. Threat: Advanced persistent threats, zero-day vulnerabilities, and novel attack methods. Inadequate Preparedness and Response: Issue: Organizations often lack comprehensive insights into their cybersecurity posture, leaving them vulnerable to unforeseen attacks. Threat: Ineffective incident response, slow detection of security gaps, and inadequate understanding of the organization's own vulnerabilities. Insider Threats and Human Error: Issue: Human factors, whether intentional or unintentional, contribute significantly to security incidents. Threat: Insider threats, negligent behavior, and inadvertent disclosure of sensitive information. Incomplete Security Coverage: Issue: Conventional security measures may leave gaps in protection, providing adversaries with opportunities to exploit vulnerabilities. Threat: Unidentified weak points in the network, applications, or configurations that remain unaddressed. Lack of Realistic Testing Environments: Issue: Simulating real-world attack scenarios in a controlled environment is challenging, limiting the ability to accurately assess an organization's security resilience. Threat: Inaccurate risk assessments, inability to predict actual consequences of cyber attacks. Resource Constraints and Prioritization Challenges: Issue: Organizations often face resource constraints, making it difficult to prioritize and address all potential security risks adequately. Threat: Inadequate allocation of resources, leaving critical assets exposed to potential exploitation. Compliance and Regulatory Risks: Issue: Failure to comply with industry regulations and cybersecurity standards can result in legal and financial consequences. Threat: Non-compliance with data protection laws, industry standards, and regulatory requirements. Limited Visibility and Monitoring: Issue: Incomplete visibility into network activities and insufficient monitoring can lead to delayed detection of security incidents. Threat: Undetected malicious activities, prolonged dwell time for attackers within the network. Breach Attack Simulation Solutions aim to address these critical issues by providing organizations with a proactive and iterative approach to cybersecurity. Through

the emulation of real-world cyber threats, these solutions enable organizations to identify vulnerabilities, test their defense mechanisms, and enhance their overall cybersecurity posture, thereby mitigating the multifaceted challenges posed by the contemporary threat landscape.

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.

Brazoria County has developed a capable and experienced information systems department which includes a dedicated cyber security analyst and a Chief Information Security Officer who shares her time across multiple clients. These two resources will be the key operators of a breach attack simulation asset. They will be guided by our management team and assisted in executing controls and standards by our network and server teams. Brazoria County scored a 6.1 on our most recent NCSR Maturity Assessment, which well exceeds the recommended minimum. The County employs the following tools, techniques, methodologies and standards in our current cyber security program. o Multifactor Authentication o Tiered administration accounts with elevation challenge o LAPS that obfuscate local administration accounts o Network segmentation o Continuous phishing testing with remedial training as needed o 24/7 Manager Detection and Response (MDR) o Weekly scans with Nessus Vulnerability Scanner o Membership and close contact with State and Federal cyber security agencies such as MS-ISAC, CISA and DHS. o Regular human driven penetration testing from third parties – both external and internal o Yearly Cyber Security training for every user o IPS/IDS – filtering for malicious packets and sites o Web Security Gateway o DR site & accompanying DR & Incident Response plan with offsite backups o Restrictive physical access to network infrastructure o Centrally managed endpoint detection and response including automated endpoint isolation o 802.1X wireless authentication o Network & server SIEM monitoring for 50+ sites o Zero trust remote access tools o Strict limitation of applications including RDP & PowerShell o Layer 3 network segmentation with FortiGate Firewalls for 50+ sites o Removal of Local Admin privileges from all users & enforced by GPO o Multi layered cloud-based email security filtering o Rigorous Change Control Management & Implementation o Least privileged port access to DMZ o Robust automated, air-gapped & immutable backups o Regular patch of software and OS with expedited workflows for emerging or zero-day threats. o Additional tools and methods not to be disclosed in a public document

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).

The following gaps were noted on page 12-13 of the 2023 Regional SPR: o 9.3.2 The region has not determined a methodology to identify equipment needs to protect local jurisdictions against cyber-attacks. o 9.1.4 The region needs to develop and implement risk analyses of critical infrastructure related to cyber prevention. Brazoria County conducts annual risk assessments to evaluate our security posture. Through these assessments we have determined gaps in our penetration testing. We are currently unable to test for novel and ever-evolving techniques and methods used by todays cyber criminals. Our formal human-performed penetration tests, while helpful and still needed, do not happen often enough to mitigate the risks to an acceptable level. In our search for a solution to this challenge we found breach and attack simulation systems. A Breach Attack Simulation (BAS) software system is designed to assess and improve the cybersecurity posture of an organization by simulating cyber attacks and identifying vulnerabilities in the organization’s infrastructure. Through the use of BAS, the County can test our security posture on an ongoing basis using

the latest methods in an automated way that requires very little human intervention.

Impact Statement :

Describe the project goals/objectives and how this project will maintain capabilities or reduce capability gaps.

There are nine objectives that a BAS system will provide to reduce our capability gaps: 1. Attack Simulation: • The primary function of BAS is to simulate realistic cyber attacks on an organization's networks, systems, and applications. These simulations mimic various attack scenarios, such as phishing, malware infections, ransomware, and other common cyber threats. 2. Vulnerability Assessment: • BAS identifies vulnerabilities within the organization's IT infrastructure. It scans for weaknesses in software, hardware, configurations, and user behaviors that could potentially be exploited by attackers. 3. Scenario Customization: • The software allows organizations to customize attack scenarios based on their specific needs and concerns. This may include simulating targeted attacks, social engineering tactics, or industry-specific threats. 4. Real-time Monitoring: • During the simulation, the BAS software monitors the response of security mechanisms, such as firewalls, intrusion detection systems, and antivirus solutions, providing real-time insights into the organization's ability to detect and respond to simulated attacks. 5. Data Breach Simulation: • BAS solutions simulate data breaches to evaluate how well the organization can detect and respond to unauthorized access or exfiltration of sensitive information. This helps organizations understand the potential impact of a real data breach. 6. Reporting and Analysis: • BAS generates comprehensive reports detailing the results of the simulation, including identified vulnerabilities, successful attack scenarios, and the organization's overall security posture. These reports help security teams prioritize and address the most critical issues. 7. Remediation Guidance: • The software often provides recommendations and guidance on how to remediate identified vulnerabilities and improve overall security. This may include suggestions for patching software, updating configurations, or enhancing security awareness training. 8. Continuous Monitoring: • BAS is often used as part of a continuous monitoring strategy. Regular simulations can be scheduled to ensure that the organization's security defenses are continually tested and improved over time. 9. Compliance Testing: • BAS software can assist organizations in testing and validating their compliance with industry regulations and cybersecurity standards. It helps ensure that security measures are aligned with best practices and regulatory requirements. A BAS system performs these tasks through automation and constant updates from the solution provider integrating detection methods of the latest novel attacks as they are discovered. Such vital near-real-time responses are impossible to perform ourselves.

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*.)

2.6.2 Maintain the Texas Cybersecurity Framework to mitigate risks and improve the resiliency of state information systems and encourage adoption of the Framework's standards by local jurisdictions.

Target Group :

Identify the target group and population expected to benefit from this project.

Direct Target Group – The citizens of and visitors to Brazoria County by providing the maximum assurance possible that: 1. Their data, transactions, documents and records are protected from theft, alteration, dissemination or loss. 2. The County can continue to

provide uninterrupted vital services in accordance with the duties delegated by the State of Texas. Indirect Target Group – The citizens of Texas and the United State through information sharing and collaboration programs facilitated by CISA, MS-ISAC, DHS and like organizations.

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.

1. Initial multi-year contract – we are unsure if a single multi-year contract paid up front is allowable under this grant. If it is then this is the preferrable option. Multiple years would allow Information Systems to build a history of success with metrics and data supporting the worth of a BAS system. With such a history a case for continuation would be strong and we can bring that case to our Commissioners Court who have, in the past, demonstrated a strong commitment to funding cyber security projects. 2. Seek funding in annual budget – Although one year would be a short time frame, we believe that when BAS achieves demonstrated success our Commissioners Court would support continued 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
Penetration Testing	40.00	The BAS system will autonomously run various penetration techniques according to the areas of most concern or based on a repeating schedule. Additionally, emerging threat techniques are consistently added to the menu of options and can be added to the schedule or run ad hoc.
Security Assessments	20.00	After performing a full set of test and assessment protocols, BAS systems can produce comprehensive assessment reports that contain graphical depictions of performance results as well as narrative content. The assessment reports contain prescribed measures to secure the assessed systems.
Vulnerability Scanning	40.00	Bass Systems perform vulnerability scanning similar to penetration testing but with the focus on discovering conditions and configurations that cause systems to be at risk for exploitation. Vulnerability reports are produced with suggested corrective actions. These reports become part of the Security Assessments.

Measures Information

Objective Output Measures

OUTPUT MEASURE	TARGET LEVEL
Number of cybersecurity gaps or issues addressed	50
Number of networks/systems implementing vulnerability scanning	300
Number of networks/systems tested	300
Number of security assessments conducted	156

Objective Outcome Measures

OUTCOME MEASURE	TARGET LEVEL

Custom Output Measures

CUSTOM OUTPUT MEASURE	TARGET LEVEL

Custom Outcome Measures

CUSTOM OUTCOME MEASURE	TARGET LEVEL

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:

_ Yes
X 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:

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]:

10/1/2023
Enter the End Date [mm/dd/yyyy]:

9/30/2024

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:

42045621
Enter the amount (in Whole Dollars $) of State Grant Funds expended:

5671831

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:

3/28/2023

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?

X Yes
_ 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

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/%
Contractual and Professional Services	05NP-00-SCAN Tools, Network Vulnerability Scanning	Breach Attack Simulation SAS Solution	$168,000.00	$0.00	$19,000.00	$0.00	$187,000.00	0

Source of Match Information

Detail Source of Match/GPI:

DESCRIPTION	MATCH TYPE	AMOUNT
Man hours from County Employees and County Contractors	In Kind Match	$19,000.00

Summary Source of Match/GPI:

Total Report	Cash Match	In Kind	GPI Federal Share	GPI State Share
$19,000.00	$0.00	$19,000.00	$0.00	$0.00

Budget Summary Information

Budget Summary Information by Budget Category:

CATEGORY	OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
Contractual and Professional Services	$168,000.00	$0.00	$19,000.00	$0.00	$187,000.00

Budget Grand Total Information:

OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
$168,000.00	$0.00	$19,000.00	$0.00	$187,000.00

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**: webbru46