FY 2020 UASI Grant Application

NCTCOG Portal: https://content.nctcog.org/ep/UASI/2020/

Eligibility

Texas Payee/Taxpayer ID # (9 Digits) :

Profile

Jurisdiction / Agency Name:
Division or Unit to Administer the Project:
Agency Address:
City:
State:
Zip Code + 4:
Start Date:
End Date:
Jurisdiction Located in what County:
Geographic Impact of Project:
Counties within the Project's Impact Area:

Grant Officials

Authorized Official Email Address:
Financial Officer Email Address:
Project Director Email Address:
Grant Writer Email Address:

Grant Vendor Information

Agency State Payee ID #:
DUNS #:

Narrative

Responses to the next three sections should be consistent with the region's (1) Threat and Hazard Identification and Risk Assessment (THIRA); (2) State Preparedness Report; and (3) Texas Homeland Security Strategic Plan.

Project Title: (2020 UASI City or County and Project Name)
Law Enforcement Project: Yes

Project Summary (Briefly summarize the project, including proposed activities and intended impact. 7000 character max)
Right now, end-users are under attack, 93% of all successful cyber attacks start with a phishing email. Hackers and threat groups target end-users on the network to gain a foothold and, from there, use several tactics and techniques to maintain persistence and spread across the network. The Election Department currently uses antivirus (AV) to protect election computers, which uses signatures to identify known viruses/malware. AV provides a valid and useful service; however, hackers and threat groups are continually modifying their malware, so AV providers are always playing catchup. The hacker's toolset includes built-in windows applications, fileless attacks, and many more that traditional AV doesn't detect.

This means the Election Department is left vulnerable and unable to detect most current threats. They are not just at risk to advanced groups that use zero-day exploits. Without better detection, the Election Department is at risk of being compromised by commodity malware easily accessible on the internet.

Managed detection and response (MDR) services fill this cybersecurity gap. MDR is a 24/7 threat monitoring, detection, incident analysis, and response service that correlates specific threat intelligence and telemetry collected from the

Election Department's environment. MDR utilizes endpoint detection and response (EDR) client software as well as network and threat intelligence to facilitate effective outcomes. Combining improved detection with a 24/7 security operations center (SOC) to monitor and respond to threats, MDR services will significantly improve the security posture of the Elections Department.

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.)

Cyber Security has become a national concern and USAI requires 5% of all USAI be utilized for cyber security at local level.

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.)
IT cyber security team of 4 and cyber security software tools to assist us with this project. Currently doing CISA assessment.

Existing Capability Gaps (Describe the existing capability gap(s) which will be addressed by the project. For Federal Homeland Security grants, include specific references to the regional or statewide State Preparedness Report (SPR).)

Currently the elections department doesn't have 24/7 cybersecurity monitoring and doesn't have the ability to detect the current tactics an techniques that hackers use today. This includes voter resgistration and the elections computing infrastructure but, because the voting machines and systems are a separate system not on a network they are not included

There are no 24/7 cybersecurity measures for Collin County Elections infrastructure. This project will provide 24/7 protection for the elections hardware technology environment.

Impact Statement (Describe the project goals/objectives and how this project will maintain capabilities or reduce capability gaps.)
Currently Collin County does not have this capabilities and this project will reduce the gaps.

This project will add 24/7 cybersecurity monitoring of the current hacking tatics and techniques for the elections voter registration system and computer infrastructure. It does not include the voting machines as those are not connected to the county network.

Homeland Security Priority Actions (Select 1 Goal, Objective, and Priority Action per section) (See Attached reference Sheet for the list)

Priority action to reduce cybersecurity vulnerabilities for Collin County elections.

UASI Strategy Priority Actions (Select 1 Goal, Objective, and Priority Action per section) (See Attached reference Sheet for the list)

Enhancing Cybersecurity

Target Group (Identify the target group and population expected to benefit from this project)

This protects our Election infrastructure from threats of cyber-attacks. The target group includes Collin County Elections Department.

Long-Term Approach (Describe how the applicant agency will maintain the capabilities supported by this project without additional federal funds. If sustainment is dependent upon federal grants, describe the ongoing need for future grants, as applicable.)

Funding will provide initial capabilities to reduce cyber threats.

Support a DHS Recognized Fusion Center: Yes

Project Activities

Investment Justification (Select One):

1. Enhancing Cybersecurity

Provide a Brief Description of how the project activity is performed.
Managed detection and response (MDR) services fill this cybersecurity gap. MDR is a 24/7 threat monitoring, detection, incident analysis, and response service that correlates specific threat intelligence and telemetry collected from the Election Department's environment. MDR utilizes endpoint detection and response (EDR) client software as well as network and threat intelligence to facilitate effective outcomes. Combining improved detection with a 24/7 security operations center (SOC) to monitor and respond to threats, MDR services will significantly improve the security posture of the Elections Department.

Capabilities

DHS Project Type:
Core Capability:
Does this Investment focus on: New Capabilities or Sustaining Existing Capabilities
Are the Assets or Activities: Deployable or Shareable or Neither
Will this investment require New Construction or Renovations (EHP): Yes or No
Will these funds support a project that was previously funded with HSGP funds: Yes or No
If yes, which grant year and list the project name.

Project Management and Milestones

Does this project support a NIMS Typed Resource? Yes or No
If Yes enter the Resource number.

Enter the amount for each funding category

Personnel:	$
Plannin:	$
Organization:	$
Equipment:	$
Training:	$
Exercises:	$
M&A:	$39,104.59
Total Project:	$

Provide a detailed description of what will be purchased in each category.
Personnel

Planning

Organization

Equipment

Training

Exercises

M&A
Managed detection and response, software and services(MDR).

List 3-5 Milestones with completion date for this project.
Milestone #1 – Completion Date: OCT 2020
Description: Court approval of the grant adjustment process

Milestone #2 – Completion Date: Jan 2021
Description: Purchase software and services

Milestone #3 – Completion Date: June 2021
Description: Install and turn up MDR solution

Milestone #4 – Completion Date:
Description:

Milestone #5 – Completion Date:
Description: