

Print This Page

Agency Name: El Paso County

Grant/App: 5376201 **Start Date:** 10/1/2024 **End Date:** 9/30/2026

Project Title: IT - Workforce Development Program

Status: Application Pending Submission

Eligibility Information

Your organization's Texas Payee/Taxpayer ID Number:

746000762

Application Eligibility Certify:

Created on:1/15/2025 10:37:00 AM By:Ricardo Samaniego

Profile Information

Applicant Agency Name: El Paso County

Project Title: IT - Workforce Development Program

Division or Unit to Administer the Project: IT

Address Line 1: 500 E Overland

Address Line 2:

City/State/Zip: El Paso Texas 79901-2420

Start Date: 10/1/2024

End Date: 9/30/2026

Regional Council of Governments(COG) within the Project's Impact Area: Rio Grande Council of Governments

Headquarter County: El Paso

Counties within Project's Impact Area: El Paso

Grant Officials:

Authorized Official

Name: Ricardo Samaniego

Email: cjdjudge@epcounty.com

Address 1: 500 E San Antonio, st. 301

Address 1:

City: El Paso, Texas 79901

Phone: 915-546-2098 Other Phone: 915-546-2175

Fax:

Title: The Honorable

Salutation: Judge

Position: County Judge

Financial Official

Name: Barbara Parker

Email: b.parker@epcountytexas.gov

Address 1: 320 S. Campbell

Address 1: Suite 140

City: El Paso, Texas 79901

Phone: 915-273-3262 Other Phone: 915-887-1044

Fax: 915-273-3266

Title: Ms.

Salutation: Ms.

Position: County Auditor

Project Director

Name: Jorge Garza

Email: jo.garza@epcountytexas.gov

Address 1: 800 E Overland

Address 1:

City: El Paso, Texas 79901

Phone: 915-273-3301 Other Phone:

Fax:

Title: Mr.

Salutation: --- Select One ---

Position: IT Cybersecurity Manager

Grant Writer

Name: Ana Campos

Email: A.campos@epcountytexas.gov

Address 1: 800 E. Overland

Address 1:

City: El Paso, Texas 79901

Phone: 915-273-3301 Other Phone: 915-224-1114

Fax:
Title: Ms.
Salutation: Ms.
Position: IT Division Manager

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): 746000762
Unique Entity Identifier (UEI): GJJHZSZVQWR6

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 SLCGP. For more information, visit CISA's Cyber Hygiene Information Page <https://www.cisa.gov/cyber-hygiene-services>

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.

This project seeks funding to develop and implement a comprehensive cybersecurity training program for our newly formed El Paso County IT Cybersecurity Division. Recent upticks in ransomware attacks and attempted intrusions in nearby municipalities and school districts highlight the urgent need for specialized, ongoing security education. Through collaboration with a trusted cybersecurity firm, we will deliver targeted training modules, simulation exercises, and certification opportunities. These activities will equip our team with the skills to swiftly detect, respond to, and prevent cyber threats against our systems. Ultimately, this project will bolster the county's defense against cyberattacks, protecting vital public services and safeguarding sensitive community data.

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.

Our county recently established a dedicated IT Cybersecurity Division in response to the growing threat of cyberattacks on local government entities. However, our Information Technology Department (ITD) team lacks the resources and specialized training to protect and respond to cybersecurity threats effectively. Funding is needed to develop and deliver comprehensive cybersecurity training, ensuring that our county's essential services and sensitive data remain secure. Without proper training, the ITD team is at risk of being underprepared to deal with sophisticated threats, leaving our local government systems and citizens' personal information vulnerable. Pg#42 Cybersecurity

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.

The El Paso County Information Technology Department comprises six internal divisions: infrastructure, Support Services, Software, Administration, Project Management, and IT Cybersecurity. This effort will require the Administration and IT Cybersecurity Divisions to prepare the procurement of specialized cybersecurity training and define and organize needed resources.

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).

In the last two years, multiple surrounding municipalities and entities, such as school districts within our region, have experienced ransomware attacks, leading to both financial and operational disruptions. Some of these municipalities reported that the root cause was insufficient cybersecurity training among staff. Additionally, the county's information technology department has documented a 35% increase in attempted intrusions over the past year, underscoring the urgent need to invest in proactive security measures. These cybersecurity incidents that have been happening around us, demonstrate that the cybersecurity threats to our county are both real and pressing, and we must build capabilities now to avoid similar breaches. There is currently only one person in the IT Cybersecurity Division, which is the IT cybersecurity Manager, and one person assisting IT Cybersecurity Division half-time. Skill gaps are one of the main constraints we have since we need to train some IT personnel in specific cybersecurity skills in order for them to understand new requirements. Our IT Cybersecurity Manager needs to attend seminars and Conferences so he can be up to date on the current threat environment Pg#58 Cybersecurity: Assess Capabilities

Impact Statement :

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

1. Curriculum Development: Partner with a recognized cybersecurity firms to design a curriculum tailored to our county's specific technology stack, compliance requirements, and threat profile. 2. Training Delivery: On-demand and on site/off-site trainings and conferences 3. Certification & Continuous Learning: Provide opportunities for team members to attain recognized cybersecurity certifications (e.g., ISC2 curriculums, SANS GIAC Cybersecurity Curriculums (starting with GSEC/GCIH). 4. Evaluation & Debrief: Conduct discussions and brainstorming sessions after each training to gauge retention and identify areas needing additional focus. By following these steps, the ITD team and the IT Cybersecurity Division will develop and maintain the skills necessary to safeguard our local government's critical infrastructure and data.

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.*)

Goal 4: Respond- Increase the capability of the state's response system to minimize damage and loss of life from terrorist and criminal attacks and natural and technological disasters. Objective 4 – Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Target Group :

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

The direct beneficiaries of this project are the newly created county IT Cybersecurity Division and some other staff members from ITD who may need specialized cybersecurity training based on their responsibilities, which currently include a mix of IT professionals, technical support staff, and security analysts. Indirectly, all county agencies and residents will benefit from enhanced data protection and critical infrastructure. Improving our cybersecurity posture ensures the continuity of essential services such as public safety, healthcare, and emergency management.

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.

We selected our proposed training model based on established best practices from organizations such as the National Institute of Standards and Technology (NIST), ISC2, and the SANS Institute. Several local government offices nationwide have successfully partnered with private-sector cybersecurity firms to implement similar training, seeing documented improvements in threat detection and incident response times. Our approach integrates evidence-based methods such as hands-on simulation drills—proven to improve comprehension—while also aligning with recognized security frameworks (e.g., NIST SP 800-53). These guiding standards and success stories underscore the proven effectiveness of our project’s design.

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
Cyber/IT Staff Training	100.00	Projects that provide cybersecurity training to organizational staff.

Measures Information

Objective Output Measures

OUTPUT MEASURE	TARGET LEVEL
Number of exercises conducted.	0
Number of individuals participating in exercises.	1
Number of people trained.	3100
Number of phishing trainings conducted	12
Number of role-based cybersecurity trainings conducted	50
Number of trainings conducted.	4

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
- ☒ 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
- ☐ 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
- ☒ 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]:

9/1/2024

Enter the End Date [mm/dd/yyyy]:

8/31/2025

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:

44622835

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

10168498

Single Audit

Applicants who expend less than \$1,000,000 in federal grant funding or less than \$1,000,000 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 \$1,000,000 or more, or state grant funding of \$1,000,000 or more during the most recently completed fiscal year?

Select the appropriate response:

☒ 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:

9/16/2024

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:

☒ I Certify
☐ Unable to Certify

Enter the debarment justification:

DO NOT DELETE THIS PLACE HOLDER ITEM

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
☒ 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
☐ 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/%
Travel and Training	In-State Registration Fees (Training)	SANS Training vouchers cost per person (2): \$8,780 x 2 \$17,560 ISC2 training Cost per person: \$5,500 (2):\$5500 x 2 \$11,000 Total in state registration costs: \$28,560 . Air Travel \$2000. Lodging \$1800. Total In state Air Travel and Lodging \$3800. Total in state travel and training amount: \$32,360	\$25,888.00	\$6,472.00	\$0.00	\$0.00	\$32,360.00	0
Travel and Training	Out-of-State Registration Fees (Training)	RSA Conference Registration approximate registration cost: \$2,695 . Black Hat Conference approximate cost: \$3,299. Total training registration costs: \$5994. Air Travel \$1750. Lodging \$1800. Total air and lodging: \$3,550. Total out of state travel and training: \$9,544	\$7,635.00	\$1,909.00	\$0.00	\$0.00	\$9,544.00	0
Supplies and Direct Operating Expenses	Participant Travel Expenses/Stipend (Training)	Meals \$2500 Transportation \$2000	\$3,600.00	\$900.00	\$0.00	\$0.00	\$4,500.00	0

Source of Match Information

Detail Source of Match/GPI:

DESCRIPTION	MATCH TYPE	AMOUNT
general funds	Cash Match	\$9,281.00

Summary Source of Match/GPI:

Total Report	Cash Match	In Kind	GPI Federal Share	GPI State Share
\$9,281.00	\$9,281.00	\$0.00	\$0.00	\$0.00

Budget Summary Information

Budget Summary Information by Budget Category:

CATEGORY	OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
Supplies and Direct Operating Expenses	\$3,600.00	\$900.00	\$0.00	\$0.00	\$4,500.00
Travel and Training	\$33,523.00	\$8,381.00	\$0.00	\$0.00	\$41,904.00

Budget Grand Total Information:

OOG	CASH MATCH	IN-KIND MATCH	GPI	TOTAL
\$37,123.00	\$9,281.00	\$0.00	\$0.00	\$46,404.00

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:** cjdjudge