BROKEN ARROW PUBLIC SCHOOLS

Educating Today *Leading Tomorrow*

Contract Committee Review Request
MUST BE COMPLETED IN FULL

Date: 04/01/2024

Contract/Agreement Vendor: State and Local Cybersecurity Grant Program
Name of Vendor & Contact Person

Vendor Email Address

Technology Grants
Describe Contract (Technology, program, consultant-prof Development, etc.)

Please use Summary below to fully explain the contract purchase , any titles, and details for the Board of Education to review.

District
Reason/Audience to benefit

04/15/2024
BOE Date

Amount of agreement

Person Submitting Contract/Agreement for Review: Ashley Bowser

PLEASE SEND THROUGH APPROPRIATE APPROVAL ROUTING BEFORE SENDING TO BOARD CLERK

Principal ***&/or*** Director or Administrator:

Does this Contract/Agreement utilize technology? [✓ YES]/NO
If yes, Technology Admin:

Cabinet Team Member:

Funding Source:
Fund/Project
OCAS Coding

□ ***Consent***

□ ***Action***

Accept and approve the grants awarded to Broken Arrow Public Schools by the State and Local Cybersecurity Grant Program. Three (3) applications were submitted and approved. The grant funds will be used to enhance the strength and health of cybersecurity throughout the District. The cost to the District is a cost match of 10% of the awarded amount. / A.Bowser

Summary *This area must be complete with full explanation of contract*

The Contract/Agreement should be received at least 2 weeks prior to a Board Meeting to ensure placement on the Agenda. The Contract Committee meets most Tuesdays at 8:00a.m. All Contracts/Agreements, regardless the amount, must be first approved by the Contract Committee and then presented to the Board of Education for approval and signature. The item will be placed on Electronic School Board for the board agenda by Janet Brown. By following this process, the liability of entering into an agreement is placed with the district rather than an individual.

OKLAHOMA OFFICE OF HOMELAND SECURITY

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) TEMPLATE INTRODUCTION AND INSTRUCTIONS

PRIVACY ACT STATEMENT

AUTHORITY: Act of 2007, 6 U.S.C. §§ 605 and 606 The Homeland Security Act of 2002, as amended by Title I of the Implementing Recommendations of the 9/11 Commission), and Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117, Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g-58).

PRINCIPAL PURPOSE(S): This information is being collected for the primary purpose of facilitating correspondence between the grant applicant and the Oklahoma Office of Homeland Security and the State of Oklahoma Cybersecurity Planning Committee and for determining eligibility and administration of FEMA Preparedness Grant Programs, specifically, the State and Local Cybersecurity Grant Program.

DISCLOSURE: The disclosure of information on this form is voluntary; however, failure to provide the information requested may delay or prevent the organization from receiving grant funding.

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) INSTRUCTIONS

Each sub-applicant can submit one application/investment justification per State Cybersecurity Plan objective.

The IJ Template is useful for the **Program Narrative** portion of the application.

Requirements:

- **Application level:** Each application must include between one (1) IJ. The IJ must be associated with one of the four objectives outlined in the NOFO and State Cybersecurity Plan. No more than four (4) IJ's can be submitted.
  - **Projects:** Project-level information will vary based on the associated SLCGP objectives and sub-objectives as outlined in the NOFO and State Cybersecurity Plan.
  - **The State of Oklahoma Cybersecurity Planning Committee requires a quote to be attached for each request.**
  - Once each IJ is complete it must be submitted, along with required attachments to hsgrants@okohs.ok.gov

ELIGIBILITY

Eligible Subrecipient Entities

"Local government" is defined in 6 U.S.C. § 101(13) as:

1. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government;

2. *An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

3. A rural community, unincorporated town or village, or other public entity.

*Although tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government.

Each individual SAA may determine whether and how much SLCGP funding to pass through to tribal entities. Additionally, funding will be directly available to eligible tribal entities under the Tribal Cybersecurity Grant Program.

Ineligible subrecipient entities include:

1. Nonprofit organizations; and

2. Private corporations.

SUB-APPLICANT POINT OF CONTACT (POC) INFORMATION

STATE, LOCAL, TRIBAL AGENCY: Broken Arrow Public Schools	SLT UEI Number: E79CJDH2JE91
SLT POC Name: Ashley Bowser	SLT POC Title: Chief Technology Officer
SLT Address: 701 S. Main Street Broken Arrow, OK 74012	
SLT POC Phone Number: 918-259-7445	SLT POC Email Address: agbowser@baschools.org

PART I. BACKGROUND FOR PROJECT NARRATIVE

1. A. Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this Investment Justification (IJ). Also, please include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks.

Cybersecurity Gaps, Risks, and Threats for 2FA: Credential Theft, Account Takeover, Social Engineering Attacks, SMS Interception, Phishing and Spoofing.

We need to implement the 2FA solutions for Broken Arrow Public Schools to add an extra layer of security to our user accounts and systems. We ensured that the technology infrastructure supports the implementation and management of 2FA solutions securely. Establishing and enforcing security policies and procedures that manage the use of 2FA for accessing sensitive systems, applications, and data.

Duo provides a console that we will be using to monitoring and detect suspicious login attempts or unusual activities related to users account using 2FA, and having incident response procedures in place to address potential security incidents promptly.

Broken Arrow Public Schools are employing 2FA with Office 365, which is complimentary for O365. We are endeavoring to implement 2FA with Windows OS on the district staff workstations, a feature not currently provided by the Office 365 2FA product.

1. B. Describe how this IJ and the associated project(s) addresses gaps and/or sustainment in the approved Cybersecurity Plan.

Addressing Gaps: Enhanced Authentication Security, Protection Against Credential Theft, Reduced Impact of Phishing Attacks, and Mitigation of SMS Interception Attacks.

Sustaining Cybersecurity:
Continuous Authentication Improvement:
Implementing 2FA reflects a commitment to continuously enhancing authentication security. As cyber threats evolve, sustaining an effective cybersecurity posture requires ongoing improvements in authentication methods. 2FA provides a scalable solution that can adapt to changing security requirements. User Education and Awareness, Compliance and Regulatory Requirements, and Adaptability to Emerging Threats. In summary, integrating 2FA into the approved Cybersecurity Plan helps address existing gaps in authentication security while sustaining a resilient security posture by promoting continuous improvement, users awareness, compliance, and adaptability to emerging threats.

PART II. SPECIFIC INVESTMENT INFORMATION

2. A. Investment Name: Provide the Investment Name:

Cisco Duo subscription for Education

2. B. Investment Type: Please identify the corresponding SLCGP Objective Number for this IJ (Objective 1, 2, 3 or 4). Each objective must have at least one project. Objective 3 -

2. C. Funding Year: Please identify the corresponding SLCGP funding year. You may select more than one.

2022 – Cost Share Waived ☑ 2024 – 30% Cost Share ☑

2023 – 20% Cost Share Waived ☑ 2025 – 40% Cost Share ☑

2. D. Funding Year: If funding is no lon Yes year you selected are you okay with us moving your funding to the next available grant year which may have a higher cost share. Choose an item.

2. F. Cost Share Type: Monetary

2. E. Describe how your agency plans to meet the cost share requirements for this grant:

Allocate funds from the school's budget specifically for the project outlined in the grant application. This may involve reallocating existing resources or setting aside funds in the budget for the grant's purposes. Broken Arrow Public Schools and our leadership are in agreement when it comes to cost share requirements for this grant.

PART III. PROJECT INFORMATION

3. A. Project Name: Provide the name(s) of the project(s).

Cisco Duo 2FA for BAPS

3. B. Project(s) Alignment to the 16 Required Cybersecurity Elements as detailed in the Statewide Cybersecurity Plan: Please describe how this project(s) aligns to the cybersecurity elements in the Statewide Cybersecurity Plan on pages 13 and 14.

1. Manage, monitor, and track information systems, applications, and user accounts
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)
5. a. Implement multi-factor authentication
5. b. Implement enhanced logging.
5. d. End use of unsupported/end of life software and hardware that are accessible from the Internet.
5. e. Prohibit use of known/fixed/default passwords and credentials
5. h. Adhere to the applicable federal regulations (ex. CJIS, HIPAA, FIRPA, etc.)
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity).
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats

PART IV. PROJECT IMPLEMENTATION SCHEDULE

4. A. Please describe project implementation and estimated timeline:

Implementing Duo Cisco 2FA for Broken Arrow Public Schools involves several steps and considerations. Here's a summery of the implementation process along with an estimated timeline:

1- Contacting the vendor and scheduling a Project Kick off meeting this will include agreeing on the Assessment and Planning for BAPS. 2- Procurement and Licensing. 3- Integration and Configuration. 4- User Enrollment and Training. 5- Testing and Validation. 6- Deployment and Rollout. Monitoring and Optimization.

Estimated Timeline:
Assessment and Planning: 2 weeks
Procurement and Licensing: 2 weeks
Integration and Configuration: 2 -3 weeks
User Enrollment and Training: 2-4 weeks
Testing and Validation: 1 weeks
Deployment and Rollout: 2-4 weeks
Monitoring and Optimization: Ongoing

4. B. In this section, list all proposed equipment, projects, or activities, the vulnerability any of those items will address, and the estimated funding requested (round up to the nearest dollar) for each. AEL – Authorized Equipment List

AEL Number	Equipment, Project, or Activity	Vulnerability Addressed	Estimated Cost	Estimated Cost Share
05AU-00-BIOM	Cisco Duo 2FA for BAPS	District Staff systems and Computers.	$ 81,000.00	$ 8,100.00
		Total Funding Requested	$ 81,000.00	$ 8,100.00

SLCGP SUB-APPLICANT CONTACT INFORMATION

This application was written by: Ahmed Mohamed

☒ By clicking this box, I certify that I am an employee or affiliated volunteer on behalf of the organization or have been hired by the organization to apply on their behalf for the State and Local Cyber Security Grant Program, have reviewed the SLCGP NOFO, as well as the Oklahoma Cyber-Security Plan and agree to the terms and conditions of all on behalf of the organization.

FULL NAME Ashley Bowser	POSITION/TITLE Chief Technology Officer
EMAIL agbowser@baschools.org	WORK PHONE 918-259-7445

Chickasaw
TELECOM, INC.
www.chickasawtel.com

Date	January 26, 2024
Quotation #	40232
Customer #	

5115 South 110th East Avenue
Tulsa, OK 74146
Telephone (918) 663-3565 Fax (918) 664-6590

Quotation valid until: February 25, 2024
Prepared by: Darin Dout
Payment Terms: Due upon receipt of goods

Bill To Information:

Customer Name	Broken Arrow Public Schools
Contact Name	Ali Shehada
Street Address	210 North Main Street
City, State & Zip Code	Broken Arrow, OK 74012
Telephone Number	(918) 259-5748
Fax Number	(918) 259-7437
E-mail Address	

Special Comments: Broken Arrow Public Schools DUO MFA 3 year subscription
Qty 3000

OSF State Contract: ITSW1006C

Product #	Product Description	Qty.	Unit List Price	Term	Customer Discount	Customer Unit Price	Customer Extended Price
	Equipment & Software				**25.00%**		
	DUO Multifactor Authentication						
DUO-EDU-SUB	Cisco Duo subscription for Education	1	0		0.00	0.00	0.00
DUO-EDU-MFA-F	Duo MFA for education Faculty/Staff users	3000	12.00	36	3.00	9.00	81,000.00
SVS-DUO-SUP-B	Cisco Duo Basic Support	1	0		0.00	0.00	0.00
			Sub Total Equipment				**$ 81,000.00**
	Miscellaneous				**10%** **100%**		
					0.00	0.00	0.00
					0.00	0.00	0.00
					0.00	0.00	0.00
			Sub Total Smartnet		$ -	$ -	$ -
	Peripherals						
					0.00	0.00	0.00
					0.00	0.00	0.00
					0.00	0.00	0.00
			Sub Total Peripherals		$ -	$ -	$ -
	Freight and Shipping (Included)					$ -	$ -
CTI-INST-LBR	Installation, Confuguration and Training (Not Requested)					$ -	
	THANK YOU FOR YOUR BUSINESS					**TOTAL**	**$ 81,000.00**
						Annual Billing Year 1	**$ 27,000.00**
						Annual Billing Year 2	**$ 27,000.00**
						Annual Billing Year 3	**$ 27,000.00**

Ship To Information:

Customer Name	
Contact Name	
Street Address	
City, State & Zip Code	
Telephone Number	
Fax Number	
E-mail Address	

If you have a project deadline please let us know when you place the order.

Company Name:	Chickasaw Telecom Inc.
Address:	5115 South 110th East Avenue Tulsa, OK 74146
Bidder:	DARIN DOUT
Signature:	
Direct Telephone # :	1-918-720-3010
Federal Identification # :	73-1354410
Service Provider ID (SPIN) # :	143028698

** Lead time is a Cisco estimate in business days plus shipping.*
All Sales are final. No returns without Manufacturer's approval.

OKLAHOMA OFFICE OF HOMELAND SECURITY

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) TEMPLATE INTRODUCTION AND INSTRUCTIONS

PRIVACY ACT STATEMENT

AUTHORITY: Act of 2007, 6 U.S.C. §§ 605 and 606 The Homeland Security Act of 2002, as amended by Title I of the Implementing Recommendations of the 9/11 Commission), and Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117, Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g-58).

PRINCIPAL PURPOSE(S): This information is being collected for the primary purpose of facilitating correspondence between the grant applicant and the Oklahoma Office of Homeland Security and the State of Oklahoma Cybersecurity Planning Committee and for determining eligibility and administration of FEMA Preparedness Grant Programs, specifically, the State and Local Cybersecurity Grant Program.

DISCLOSURE: The disclosure of information on this form is voluntary; however, failure to provide the information requested may delay or prevent the organization from receiving grant funding.

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) INSTRUCTIONS

Each sub-applicant can submit one application/investment justification per State Cybersecurity Plan objective.

The IJ Template is useful for the **Program Narrative** portion of the application.

Requirements:

- **Application level:** Each application must include between one (1) IJ. The IJ must be associated with one of the four objectives outlined in the NOFO and State Cybersecurity Plan. No more than four (4) IJ's can be submitted.
  - **Projects:** Project-level information will vary based on the associated SLCGP objectives and sub-objectives as outlined in the NOFO and State Cybersecurity Plan.
  - **The State of Oklahoma Cybersecurity Planning Committee requires a quote to be attached for each request.**
  - Once each IJ is complete it must be submitted, along with required attachments to hsgrants@okohs.ok.gov

ELIGIBILITY

Eligible Subrecipient Entities

"Local government" is defined in 6 U.S.C. § 101(13) as:

1. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government;

2. *An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

3. A rural community, unincorporated town or village, or other public entity.

*Although tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government.

Each individual SAA may determine whether and how much SLCGP funding to pass through to tribal entities. Additionally, funding will be directly available to eligible tribal entities under the Tribal Cybersecurity Grant Program.

Ineligible subrecipient entities include:

1. Nonprofit organizations; and

2. Private corporations.

SUB-APPLICANT POINT OF CONTACT (POC) INFORMATION

STATE, LOCAL, TRIBAL AGENCY: Broken Arrow Public Schools	SLT UEI Number: E79CJDH2JE91
SLT POC Name: Ashley Bowser	SLT POC Title: Chief Technology Officer
SLT Address: 701 S. Main Street Broken Arrow, OK 74012	
SLT POC Phone Number: 918-259-7445	SLT POC Email Address: agbowser@baschools.org

PART I. BACKGROUND FOR PROJECT NARRATIVE

1. A. Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this Investment Justification (IJ). Also, please include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks.

Cybersecurity Gaps, Risks, and Threats without Darktrace Email - Office 365 Email Filtering:
Advanced Persistent Threats (APTs).
Malware and Ransomware Attacks:Absence of email filtering increases the risk of malware and ransomware infections through malicious email attachments or links, potentially causing system downtime, data loss, and financial losses.
Phishing and Business Email Compromise (BEC).
Data Leakage and Unauthorized Access.
Compliance Violations.

Summary of Current Capabilities to Address Threats and Risks:
Firewall and Intrusion Detection Systems (IDS/IPS). Endpoint Protection.
Incident Response Planning.
Security Policy Enforcement.

While these current capabilities provide a foundation for cybersecurity defense, the absence of Darktrace and/or any other email filtering solutions leaves the school network vulnerable to advanced threats and targeted attacks. Implementing Darktrace and robust email filtering mechanisms would significantly enhance threat detection, incident response capabilities, and overall cybersecurity resilience within Broken Arrow Public Schools.

1. B. Describe how this IJ and the associated project(s) addresses gaps and/or sustainment in the approved Cybersecurity Plan.

Integrating Darktrace Email and Office 365 email filtering into the approved Cybersecurity Plan at Broken Arrow Public Schools District significantly strengthens the overall cybersecurity posture and addresses several gaps and sustainability concerns.
Here's how these solutions contribute - Addressing Gaps: Advanced Threat Detection, Real-time Threat Monitoring, Behavioral Analysis, and Email Filtering and Protection.

Sustaining Cybersecurity:
Continuous Monitoring and Analysis: Darktrace Email and Office 365 - email filtering solutions facilitate continuous monitoring and analysis of email communications, ensuring sustained visibility into potential security threats and vulnerabilities. This allows for proactive threat management and mitigation, sustaining a high level of security posture over time.

Adaptive Threat Response, User Education and Awareness, Compliance and Regulatory Requirements, and Continuous Improvement and Adaptation.

By integrating Darktrace Email and Office 365 - email filtering into the approved Cybersecurity Plan, Broken Arrow Public Schools District can effectively address existing gaps in threat detection, response, and email security while sustaining a proactive and adaptive approach to cybersecurity defense.

PART II. SPECIFIC INVESTMENT INFORMATION

2. A. Investment Name: Provide the Investment Name:

Darktrace/Email/Office365

2. B. Investment Type: Please identify the corresponding SLCGP Objective Number for this IJ (Objective 1, 2, 3 or 4). Each objective must have at least one project. Objective 3 -

2. C. Funding Year: Please identify the corresponding SLCGP funding year. You may select more than one.

2022 – Cost Share Waived ☑ 2024 – 30% Cost Share ☑

2023 – 20% Cost Share Waived ☑ 2025 – 40% Cost Share ☑

2. D. Funding Year: If funding is no lon Yes year you selected are you okay with us moving your funding to the next available grant year which may have a higher cost share. Choose an item.

2. F. Cost Share Type: Monetary

2. E. Describe how your agency plans to meet the cost share requirements for this grant:

Allocate funds from the school's budget specifically for the project outlined in the grant application. This may involve reallocating existing resources or setting aside funds in the budget for the grant's purposes. Broken Arrow Public Schools and our leadership are in agreement when it comes to cost share requirements for this grant.

PART III. PROJECT INFORMATION

3. A. Project Name: Provide the name(s) of the project(s).

Darktrace Email Filtering for BAPS

3. B. Project(s) Alignment to the 16 Required Cybersecurity Elements as detailed in the Statewide Cybersecurity Plan: Please describe how this project(s) aligns to the cybersecurity elements in the Statewide Cybersecurity Plan on pages 13 and 14.

1. Manage, monitor, and track information systems, applications, and user accounts.
2. Monitor, audit, and track network traffic and activity.
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts.
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk.
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)
5. c. Data encryption for data at rest and in transit.
5. d. End use of unsupported/end of life software and hardware that are accessible from the Internet.
5. h. Adhere to the applicable federal regulations (ex. CJIS, HIPAA, FIRPA, etc.).
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity).
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity.
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department.
12. Leverage cybersecurity services offered by the Department.
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.
15. Ensure rural communities have adequate access to, and participation in plan activities.
16. Distribute funds, items, services, capabilities, or activities to local governments.

PART IV. PROJECT IMPLEMENTATION SCHEDULE

4. A. Please describe project implementation and estimated timeline:

Implementing an Email Office 365 - email filtering project involves several steps to ensure effective deployment and integration with existing systems. Here's a summery of the implementation process along with an estimated timeline:
Darktrace Email Filtering Project Implementation Steps: 1- Contacting the vendor and scheduling a Project Kick off meeting this will include agreeing on the Assessment and Planning for BAPS. 2- Procurement and Licensing. 3- Integration and Configuration. 4- User Enrollment and Training. 5- Testing and Validation. 6- Deployment and Rollout. Monitoring and Optimization.

Estimated Timeline:
Assessment and Planning: 2-4 weeks
Vendor Selection and Procurement: 2-4 weeks
Configuration and Integration: 2 weeks
Testing and Validation: 2-4 weeks
User Training and Communication: 2-4 weeks
Deployment and Rollout: 1 month
Monitoring and Maintenance: Ongoing

4. B. In this section, list all proposed equipment, projects, or activities, the vulnerability any of those items will address, and the estimated funding requested (round up to the nearest dollar) for each. AEL – Authorized Equipment List

AEL Number	Equipment, Project, or Activity	Vulnerability Addressed	Estimated Cost	Estimated Cost Share
05EN-00-ECRP	Darktrace Email Filtering for BAPS	Our staff are vulnerable through email to Malware, Data exfiltration, URL phishing, Lat	$ 255,216.00	$ 25,521.60
		Total Funding Requested	$ 255,216.00	$ 25,521.60

SLCGP SUB-APPLICANT CONTACT INFORMATION

This application was written by: Ahmed Mohamed

■ By clicking this box, I certify that I am an employee or affiliated volunteer on behalf of the organization or have been hired by the organization to apply on their behalf for the State and Local Cyber Security Grant Program, have reviewed the SLCGP NOFO, as well as the Oklahoma Cyber-Security Plan and agree to the terms and conditions of all on behalf of the organization.

FULL NAME Ashley Bowser	POSITION/TITLE Chief Technology Officer
EMAIL agbowser@baschools.org	WORK PHONE 918-259-7445

DARKTRACE

PRODUCT QUOTE

CUSTOMER INFORMATION:

Customer Name:	Broken Arrow Public Schools	**Quote Ref:**	Q136904-202401-30-950027
Shipping Address:	210 N. Main Street Broken Arrow, OK 74012	**Date Prepared:**	2024/01/30
Invoice Address:	210 N. Main Street Broken Arrow, OK 74012	**Expiry Date:**	2024/02/01
Attn:	Ashley Bowser		
Email:	agbowser@baschools.org		

DARKTRACE OFFERING:

Line Item	Product/Services Description	Qty.	Subscription Period (months)	Annual Customer Price USD	Extended Customer Price USD
Product & Services			36	85,072	255,216
1	Darktrace/Email/Office365	3,000 Mailboxes			
Training					
2	eLearning Training	1			
	Public Online Training	1			
	Private Training (Remote)	2 Sessions			
Commencing on 2024/02/29 ("Commencement Date")					
Installation Services					
Standard Support Services					
Total price over term:					**255,216**

Product Quote for Information Purposes Only

PRODUCT DESCRIPTIONS

Product Families

The Cyber AI Loop represents the world's first always-on, end-to-end, interconnected set of cyber security solutions. It empowers defenders to reduce cyber risk at every stage of the attack lifecycle. Each product within the Cyber AI Loop is powered by Self-Learning AI that understands its unique digital surroundings. Rather than being trained on attack data it learns the bespoke details of your organization, so it can identify subtle patterns that indicate a vulnerability or an emerging threat. And each capability feeds back into the Loop as a whole; autonomously and continuously strengthening the entire system.

Darktrace PREVENT™	Darktrace PREVENT reduces cyber risk by prioritizing vulnerabilities and hardening defenses inside and out. It allows the security team to get ahead of the attack and pre-empt attacks. By knowing your organization, it surfaces vulnerable assets and attack pathways and tells you where you can most effectively spend your time proactively hardening your defenses. Darktrace PREVENT consists of two core products - Darktrace PREVENT/Attack Surface Management (or PREVENT/ASM) and Darktrace PREVENT/End-to-End (or PREVENT/E2E).
Darktrace DETECT™	Powered by a bespoke, continuously evolving understanding of self, Darktrace DETECT delivers instant visibility of threats - even those using novel malware strains or new techniques.
Darktrace RESPOND™	By making a series of micro-decisions at machine speed, Darktrace RESPOND disarms an attack in seconds. It uses Darktrace's evolving and bespoke understanding of your organization to pinpoint signs of a potential attack and interrupt the malicious activity, all while letting your normal business operations continue.
Darktrace HEAL™	Darktrace HEAL is an AI engine that learns on your data to provide an ongoing assessment of human and system readiness to mitigate an active security incident and determine the most effective path to eradicate the threat, recover to an operational state, and adapt its security posture to harden against repeat or similar offenses.
Cyber AI Analyst	Using Explainable AI, Cyber AI Analyst continuously investigates to generate meaningful outputs that a human team can easily understand. With PREVENT, Explainable AI plays a key role in allowing a human operator to immediately understand why Darktrace has suggested certain mitigation actions, or why a certain attack path has been identified as critical. At the DETECT stage AI Analyst automatically investigates every security event, autonomously triaging and reporting on the full scope of the security incident, dramatically reducing the time to meaning for security teams. With RESPOND, AI Analyst helps human security teams immediately understand what action, if any, the AI took and why, helping teams build trust in the AI's decision-making over time.

Coverage Areas

Darktrace brings its Self-Learning AI to your data wherever it resides. Darktrace offers a unified approach to cyber defense across diverse and fractured digital environments covering Cloud, Apps, Email, Network, OT & Zero-Trust environments.

Services

Installation Services	Darktrace's expert Cyber Defense Engineers and Cyber Technologists will work closely with your team to ensure the successful design and implementation of the Cyber AI Loop.
Ask the Expert	Available from within the User Interface, Ask the Expert is a feature that lets users send queries to a Darktrace Cyber Analyst for expert assistance during threat investigations.
Proactive Threat Notification	Powered by your Darktrace deployment and manned by our world-class Darktrace Cyber Analysts, this service notifies you of threats that cross the threshold. Having an extra set of eyes-on-glass, we'll notify you of the threat and provide expert triage assistance.
POV Reports	Proof of Value Reports provide an executive summary and technical analysis of the most significant threats that Darktrace technology has detected over a specified period of time.

Deployment Usage Fees

Appliances	Darktrace appliances are highly tuned, high performance pieces of hardware. There are multiple types of Darktrace appliance with different throughput capacities and options for data ingestion.
Cloud Masters	Darktrace deploys lightweight software component to host your deployment into virtualized or third party cloud environments.

OKLAHOMA OFFICE OF HOMELAND SECURITY

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) TEMPLATE INTRODUCTION AND INSTRUCTIONS

PRIVACY ACT STATEMENT

AUTHORITY: Act of 2007, 6 U.S.C. §§ 605 and 606 The Homeland Security Act of 2002, as amended by Title I of the Implementing Recommendations of the 9/11 Commission), and Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117, Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g-58).

PRINCIPAL PURPOSE(S): This information is being collected for the primary purpose of facilitating correspondence between the grant applicant and the Oklahoma Office of Homeland Security and the State of Oklahoma Cybersecurity Planning Committee and for determining eligibility and administration of FEMA Preparedness Grant Programs, specifically, the State and Local Cybersecurity Grant Program.

DISCLOSURE: The disclosure of information on this form is voluntary; however, failure to provide the information requested may delay or prevent the organization from receiving grant funding.

CYBERSECURITY GRANT PROGRAMS INVESTMENT JUSTIFICATION (IJ) INSTRUCTIONS

Each sub-applicant can submit one application/investment justification per State Cybersecurity Plan objective.

The IJ Template is useful for the **Program Narrative** portion of the application.

Requirements:

- **Application level:** Each application must include between one (1) IJ. The IJ must be associated with one of the four objectives outlined in the NOFO and State Cybersecurity Plan. No more than four (4) IJ's can be submitted.
- **Projects:** Project-level information will vary based on the associated SLCGP objectives and sub-objectives as outlined in the NOFO and State Cybersecurity Plan.
- **The State of Oklahoma Cybersecurity Planning Committee requires a quote to be attached for each request.**
- Once each IJ is complete it must be submitted, along with required attachments to hsgrants@okohs.ok.gov

ELIGIBILITY

Eligible Subrecipient Entities

"Local government" is defined in 6 U.S.C. § 101(13) as:

1. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government;

2. *An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

3. A rural community, unincorporated town or village, or other public entity.

*Although tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government.

Each individual SAA may determine whether and how much SLCGP funding to pass through to tribal entities. Additionally, funding will be directly available to eligible tribal entities under the Tribal Cybersecurity Grant Program.

Ineligible subrecipient entities include:

1. Nonprofit organizations; and

2. Private corporations.

SUB-APPLICANT POINT OF CONTACT (POC) INFORMATION

STATE, LOCAL, TRIBAL AGENCY: Broken Arrow Public Schools	SLT UEI Number: E79CJDH2JE91
SLT POC Name: Ashley Bowser	SLT POC Title: Chief Technology Officer
SLT Address: 701 S. Main Street Broken Arrow, OK 74012	
SLT POC Phone Number: 918-259-7445	SLT POC Email Address: agbowser@baschools.org

PART I. BACKGROUND FOR PROJECT NARRATIVE

1. A. Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this Investment Justification (IJ). Also, please include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks.

Understanding the cybersecurity landscape without SentinelOne Endpoint Detection and Response (EDR) is crucial for identifying gaps, risks, and threats faced by Broken Arrow Public Schools. Here's a short overview along with a summary of current capabilities to address these challenges:
Cybersecurity Gaps, Risks, and Threats without SentinelOne EDR:
Endpoint Security Vulnerabilities, Advanced Threat Detection, Insufficient Incident Response Capabilities, Lack of Behavioral Analysis, and Compliance and Regulatory Risks.

Summary of Current Capabilities to Address Threats and Risks:
Endpoint Protection Software, Firewall and Network Security, User Education and Awareness, Incident Response Planning, Patch Management, and Security Policy Enforcement.

While these current capabilities provide a foundation for cybersecurity defense, the addition of SentinelOne EDR would significantly enhance the school's ability to detect, respond to, and mitigate advanced threats targeting endpoints within the network. It's essential for Broken Arrow Public Schools to assess the benefits of implementing SentinelOne EDR and integrate it into our cybersecurity strategy to strengthen endpoint security posture effectively.

1. B. Describe how this IJ and the associated project(s) addresses gaps and/or sustainment in the approved Cybersecurity Plan.

SentinelOne Endpoint Detection and Response (EDR) offers several features and capabilities that can significantly enhance the approved Cybersecurity Plan for the Broken Arrow Public Schools district. Here's a summary of how SentinelOne EDR addresses gaps and sustains cybersecurity efforts:

Addressing Gaps: Advanced Threat Detection: SentinelOne EDR employs advanced machine learning algorithms and behavioral analysis to detect sophisticated threats, including zero-day attacks, fileless malware, and advanced persistent threats (APTs). This addresses the gap in detecting and mitigating evolving cybersecurity threats that traditional antivirus solutions may miss.
Real-Time Threat Response, Endpoint Visibility and Forensics, and Behavioral Analysis and Anomaly Detection.

Sustaining Cybersecurity:
Continuous Monitoring and Threat Hunting:
SentinelOne EDR continuously monitors endpoint activity, analyzes security events in real-time, and proactively hunts for threats across the our district network. This sustains cybersecurity efforts by providing continuous threat visibility and detection capabilities.

Automated Response and Remediation, Threat Intelligence Integration, Compliance and Reporting, and Adaptive Security Policies.

By integrating SentinelOne Endpoint Detection and Response into the approved Cybersecurity Plan, Broken Arrow Public Schools can enhance it's ability to detect, respond to, and mitigate advanced cyber threats effectively, thereby improving overall cybersecurity posture and resilience.

PART II. SPECIFIC INVESTMENT INFORMATION

2. A. Investment Name: Provide the Investment Name:

SentinelOne Endpoint Detection and Response (EDR)

2. B. Investment Type: Please identify the corresponding SLCGP Objective Number for this IJ (Objective 1, 2, 3 or 4). Each objective must have at least one project. Objective 3 -

2. C. Funding Year: Please identify the corresponding SLCGP funding year. You may select more than one.

2022 – Cost Share Waived ☑ 2024 – 30% Cost Share ☑

2023 – 20% Cost Share Waived ☑ 2025 – 40% Cost Share ☑

2. D. Funding Year: If funding is no lon Yes year you selected are you okay with us moving your funding to the next available grant year which may have a higher cost share. Choose an item

2. F. Cost Share Type: Monetary

2. E. Describe how your agency plans to meet the cost share requirements for this grant:

Allocate funds from the school's budget specifically for the project outlined in the grant application. This may involve reallocating existing resources or setting aside funds in the budget for the grant's purposes. Broken Arrow Public Schools and our leadership are in agreement when it comes to cost share requirements for this grant.

PART III. PROJECT INFORMATION

3. A. Project Name: Provide the name(s) of the project(s).

SentinelOne EDR for BAPS

3. B. Project(s) Alignment to the 16 Required Cybersecurity Elements as detailed in the Statewide Cybersecurity Plan: Please describe how this project(s) aligns to the cybersecurity elements in the Statewide Cybersecurity Plan on pages 13 and 14.

1. Manage, monitor, and track information systems, applications, and user accounts.
2. Monitor, audit, and track network traffic and activity.
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts.
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk.
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST).

5. c. Data encryption for data at rest and in transit.

5. d. End use of unsupported/end of life software and hardware that are accessible from the Internet.

5. h. Adhere to the applicable federal regulations (ex. CJIS, HIPAA, FIRPA, etc.).

6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.

8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity).

9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks.

10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity.

11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department.

12. Leverage cybersecurity services offered by the Department.

13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.

PART IV. PROJECT IMPLEMENTATION SCHEDULE

4. A. Please describe project implementation and estimated timeline:

Implementing SentinelOne Endpoint Detection and Response (EDR) for Broken Arrow Public Schools District involves several steps to ensure effective deployment and integration with existing systems. Here's a quick summery outline of the implementation process along with an estimated timeline:
SentinelOne EDR Implementation Steps: 1- Assessment and Planning. 2- Vendor Selection and Procurement. 3- Configuration and Integration. 4- Pilot Testing and Validation. 5- User Training and Communication. 6- Deployment and Rollout. 7- Monitoring and Maintenance.

Estimated Timeline:
Assessment and Planning: 1-2 weeks
Vendor Selection and Procurement: 1-2 weeks
Configuration and Integration: 2 weeks
Pilot Testing and Validation: 1 weeks
User Training and Communication: 1 weeks
Deployment and Rollout: 1 weeks
Monitoring and Maintenance: Ongoing

4. B. In this section, list all proposed equipment, projects, or activities, the vulnerability any of those items will address, and the estimated funding requested (round up to the nearest dollar) for each. AEL – Authorized Equipment List

AEL Number	Equipment, Project, or Activity	Vulnerability Addressed	Estimated Cost	Estimated Cost Share
05HS-00-MALW	SentinelOne EDR for BAPS	The district computers will be vulnerable for any Malicious viruses or spyware which c	$ 271,773.00	$ 27,177.30
		Total Funding Requested	$ 271,773.00	$ 27,177.30

SLCGP SUB-APPLICANT CONTACT INFORMATION

This application was written by: Ahmed Mohamed

■ By clicking this box, I certify that I am an employee or affiliated volunteer on behalf of the organization or have been hired by the organization to apply on their behalf for the State and Local Cyber Security Grant Program, have reviewed the SLCGP NOFO, as well as the Oklahoma Cyber-Security Plan and agree to the terms and conditions of all on behalf of the organization.

FULL NAME Ashley Bowser	POSITION/TITLE Chief Technology Officer
EMAIL agbowser@baschools.org	WORK PHONE 918-259-7445

Arete Advisors
Experience matters.

4800 T-Rex Avenue, Suite 350
Boca Raton, FL 33431

QUOTE

Customer:	Broken Arrow Public Schools
	701 South Main Street, Broken Arrow, OK 74012

Prepared for:	Ahmed Mohamed
Phone:	918-259-7452
Email:	amohamed@baschools.org

Date:	Jan 29,2024
Quote Expires:	Apr 25,2024
Quote ID	20240129-113538

Prepared by:	Paul Elias
Phone:	(561) 414-7687
Email:	pelias@areteir.com

Code	Description	Sub Mon	Qty (Seats)	Unit Price	Disc	Unit Net Price	Extended Net Price
S1-CMP-EN-T5-S	Complete Protection Platform (Per Workstation). EPP + EDR, with NGAV (AI), Rogues IoT, Firewall Control, Device Control, Remote Shell, Deep Visibility and up to 100 concurrent STAR Rules, Standard Support Plan	36	3,000	$ 174.18	69.51 %	$ 53.11	$ 159,318.90
PF-PLT-FF-T1-S	Singularity XDR Platform. Access to the Singularity XDR Platform, includes initial XDR Ingest	36	1	$ 4,800.00	100.00 %	$ 0.00	$ 0.00
SS-VRP-ND-T5-S	Vigilance Respond Pro (Per Endpoint). Vigilance Respond Pro: 24x7 MDR, and incident response	36	3,000	$ 90.33	61.26 %	$ 34.99	$ 104,984.10
PS-GO-ND-T5-S	Guided Onboarding (Per Endpoint). 90 Days, Remote Deployment Assistance, Initial Threat Triaging, Ongoing Configuration Review and Health Checks, Designated Customer Success Manager	36	3,000	$ 23.91	89.59 %	$ 2.49	$ 7,470.00

Instructions:
Sign this Quote (or create a Purchase Order referencing the above Quote ID)
and email it to sales@areteir.com

Grand Total: $ 271,773.00
Payment Terms: Net 30
Billing Frequency: Prepaid in Full

TERMS AND CONDITIONS

This Quote and these associated terms and conditions constitute a binding agreement ("Agreement") between the Customer identified herein ("Customer") and Arete Advisors, LLC ("Arete"), which shall become effective upon the receipt of a purchase order ("Purchase Order" or "PO") from Customer. In the event of a conflict between the provisions of this Agreement and any provisions contained in any Purchase Order, the provisions of these terms and conditions shall govern. This Agreement supersedes any previous or contemporaneous communications, statements, or understandings between the parties and can be amended or modified only by means of a written document that expressly purports to amend this Agreement. The terms and conditions on any separate order form or similar document Customer may submit to Arete are rejected by Arete and will have no legal effect.

1. Acceptance. All POs are subject to acceptance by Arete, and Arete reserves the right to reject a PO in its sole discretion. A PO shall be deemed to be accepted by Arete, however, unless Arete notifies Customer of Arete's rejection within five (5) business days of Arete' receipt of the PO.

2. Payment Terms. Arete will issue an invoice against a PO after shipment. All amounts invoiced shall be due and payable net thirty (30) days from the date of invoice. All payments shall be made to Arete in US dollars via wire transfer or in such other manner as Arete shall reasonably designate. Based on its assessment of Customer's financial situation and/or payment history, Arete may refuse to extend credit terms to

Customer, in which case Arete may reject a PO or require advance payment or other indication of security as a condition of acceptance and order fulfilment. In the event any payment to be made hereunder is overdue, such payment shall accrue interest at the rate of one and one-half percent (1.5%) per month or, if it is lower than this, the maximum percentage permitted by law, and in addition, if Arete incurs any legal or collection fees cost in connection with enforcing payment obligations hereunder, Customer shall reimburse Arete for all such costs reasonably incurred.

3. Taxes. Prices stated on a PO do not include any taxes or other governmental charges, including, without limitation, import or export duties, value-added, sales, use or privileges taxes, or excise or similar taxes levied by any government, now or hereafter enacted. **Depending on your tax jurisdiction, taxes may be added (at the applicable rate) when your order is invoiced**.

4. Compliance with Laws; Export. Customer shall comply with all laws (including but not limited to those relating to payments to officials and to the control of imports and exports) that may be applicable to Customer's import, use, transfer, resale, export or re-export of the Service and shall obtain all licenses, approvals and permits required under applicable laws to import, export, or use the Service and make the payment of fees under the PO. Without limiting the generality of the foregoing, Customer hereby acknowledges that the Service is subject to export controls under the laws and regulations of the United States.

5. General. Any waiver, amendment or modification of any right, remedy or other term set forth in these terms and conditions will not be effective unless in writing and signed by an authorized person of the party against whom enforcement is sought. Any modifications of these terms and conditions must make specific reference to the provision(s) hereof to be so modified and must be in writing and signed by both parties. The validity, interpretation, and performance of a PO and these terms and conditions shall be controlled by and construed under the law of Florida. Exclusive jurisdiction of all disputes arising out of or in connection with these terms and conditions and/or a PO or the performance or breach of either shall reside in the appropriate court in Palm Beach County, Florida, USA. Each PO together with these terms and conditions constitutes the entire agreement between the parties as to the subject matter hereof and supersedes any and all written or oral agreements previously existing between the parties with respect to such subject matter. Nothing herein is intended, however, to limit the effectiveness of any End User License Agreement (EULA) or Terms of Service.

Signature: ______________________________ Date____________________

Name and Title: ____________________________