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: City of Norman, OK	SLT UEI Number: MTD4M7LKSKJ4
SLT POC Name: Jeremy Kilgore	SLT POC Title: Security Engineer
SLT Address: 313 N. Webster, Norman OK 73069	
SLT POC Phone Number: 405-217-7749	SLT POC Email Address: Jeremy.Kilgore@NormanOK.gov

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.

To-date, the City of Norman does not have any tools for monitoring, mapping and notification of events in the operational technology environments at the SCADA implementations for water and water reclamation. We lack tools that map our environments in a way to show all assets (PLC's, HMI's, etc.) in a graphical view with reference to known vulnerabilities, firmware versions, how the devices are connected, communicating including protocols used and their direction of communication.

As you are aware we have a Security Engineer position and have been granted the opportunity to add a Security Technician to assist our City. Tools such as these will greatly benefit our City and our security staff. They are necessary and will be used to assist our Utilities Department in their critical and core function of providing recipients safe and secure drinking water and sewer services.

The tool provides a criticality score that helps determine the urgency of addressing or re-mediating issues. We believe this tool is so important due to the insight of say concerns with a PLC that is not easily updated but we would have insight to address issues with vendor partners on how to correct situations without disruption to plant services such as schedule replacements, updates, etc. To date we don't have any mapping of the plant devices at this level to even know such vulnerabilities exist, where they are in the plants, and their criticality.

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

The funding will provide the much needed resources to bolster our IT /OT security infrastructure. This will be accomplished with the threat intelligence and vulnerability management afforded with these tools. It provides the ability to mitigate risks, and ensure compliance with essential security standards, thereby safeguarding the City of Norman's OT assets within our SCADA environments for water and water reclamation thereby ensuring sustainability of critical and core infrastructure and operations.

PART II. SPECIFIC INVESTMENT INFORMATION

2. A. Investment Name: Provide the Investment Name:
OT Threat Intelligence & Vulnerability Management

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 – Cost Share Waived ☑ 2025 – 40% Cost Share ☐

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

2. F. Cost Share Type: In-kind

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

PART III. PROJECT INFORMATION

3. A. Project Name: Provide the name(s) of the project(s).
OT Threat Intelligence & Vulnerability Management

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.

2. Monitor, audit, and track network traffic and activity
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk
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

3. C. Please describe project implementation and estimated timeline:

Within 3 to 6 months.

3. D. 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
05NP-00-IDPS 05NP-00-SCAN	Dragos OT threat intelligence, vulnerability monitoring and management tools	Provides IT OT threat intelligence & vulnerability monitoring that is not in place to-date	145000.00	145000.00
	Deployment & Implementation	Assist with the deployment and configuration of the appliances and software	4400.00	4400.00
		Total Funding Requested	149400	149400

4. Please describe how your entity plans to sustain this project once the grant funds are gone:

We will request recurring funds in operating budgets for the utilities in the annual budget process. We will stress the grant provided the foundation for these tools and capabilities. Staff and Management are very supportive of this initiative.

Milestone 1	Milestone 2	Milestone 3
Provide a graphical view and real-time data of the OT environment of critical SCADA infrastructure at our Water and Water Reclamation facilities. To-date we have plant operations from a plant manager views but we do not have tools to provide graphical views of all of the operational technology components including the communications between devices and any vulnerabilities that may be associated with each.	Obtain a criticality score as well as possible solutions to address vulnerabilities if a device cannot be easily updated without disruptions to the plant operations. This will provide a means of remediation efforts, policies that could be applied to address vulnerabilities, as well as time for planning updates to sensitive devices that today we lack the insight for.	Establish a monitoring view with notification alerts to vulnerabilities within the SCADA environments for IT security staff to receive and respond to. This type of monitoring capability will further augment and support proper compliance of critical infrastructure.

SLCGP SUB-APPLICANT CONTACT INFORMATION	
This application was written by:	
■ 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 Jeremy Kilgore	POSITION/TITLE Security Engineer
EMAIL Jeremy.Kilgore@NormanOK.gov	WORK PHONE 405-217-7749