

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 hsgnants@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:
SLT POC Name: Kari Madden	SLT POC Title: I.T. Manager, Business Systems & Development
SLT Address: 313 N. Webster Norman, OK 73069	
SLT POC Phone Number: 405-366-5361	SLT POC Email Address: Kari.Madden@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. The City of Norman has a backup solution that we are out growing for our off site storage. We are in need of expanding the capacity for critical and core operations. This initiative also renews the licensing for the necessary agreement for the hosted components of this program.	
1. B. Describe how this IJ and the associated project(s) addresses gaps and/or sustainment in the approved Cybersecurity Plan. The proposed solution we are requesting funding for will allow for full backups of all critical virtual servers and data in a day. This will provide encrypted backups in transit and rest to also be stored in near time to a cloud service with the approved vendor. The solution we have implemented and wish to expand further provides threat scan and risk analysis to ensure backups are clean prior to restore.	

PART II. SPECIFIC INVESTMENT INFORMATION

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

City of Norman Backup Contingency Operations

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 1 -**

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 longer available for 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. Choose an item **Yes**

2. F. Cost Share Type: In-kind

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

We will use funds for the Email and Backup Systems Administrator's salary as a match.

PART III. PROJECT INFORMATION

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

City of Norman Backup Contingency Operations Expansion

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.

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

5. f. Ensure the ability to reconstitute system (backups)

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.

The investment will provide reliable backups, meeting requirements for data encryption at rest and in transit as well. This provides needed compliance for providing secure backups and safe and quick recovery when needed to restore critical operations.

PART IV. PROJECT IMPLEMENTATION SCHEDULE

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

State contracts will be used for the purchase of the project. We anticipate the project to implement within days of having funds secured for the project. It is simply renewing a contract amount and paying for licensing for the additional storage that is allocated in the cloud.

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
AEL Code 14CI-00-COOP	Contingency Operations of Critical Operations		188,000	75200.00
		Total Funding Requested	188000.00	75200.00
		Total Funding Requested	188188	150400

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 Kari Madden	POSITION/TITLE IT Manager, Business Systems & Development
EMAIL Kari.Madden@NormanOK.Gov	WORK PHONE 405-366-5361