2024-2025

SLCGP EQUIPMENT LIST

Overview

Allowable investments made in support of this goal must fall into the categories of (POETE):

- Planning
- Organization
- Equipment
- Training
- Exercises

Requested projects must strengthen state and local cybersecurity preparedness by focusing on cybersecurity measures to help manage state and local risk and enhance Oklahoma's cybersecurity posture. The requested project MUST:

1. Close gaps and strengthen capabilities identified in the agencies' Nationwide Cybersecurity Review (NCSR)
2. Align with the state's cybersecurity plan.
3. Align with at least one of the FY 2023 SLCGP Objectives (FY 2023 SLCGP Objectives can be found in Appendix A)

Planning:

- Planning costs are allowable under this program. Funds may be used for planning activities that support the FY 2023 SLCGP objectives, Oklahoma Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's NCSR.

Organization:

Organization costs are allowable under this program. Organizational activities include:

- Program management
- Development of whole community partnerships
- Structures and mechanisms for information sharing between the public and private sector.
- Operational support
- Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP planning, organization, training, exercise, and equipment activities.
- If funding is being used for overtime and backfill, this must be approved by FEMA in writing in advance to applying.
- Personnel expenses may include, but are not limited to, training and exercise coordinators, program managers and planners, Cybersecurity navigators. The grant sub recipient must demonstrate that the personnel will be sustainable once the program ends or funds are no longer available.

Equipment:

- Equipment costs are allowable under this program. SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.
- Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS/FEMA/OHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.
- SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of

equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

Training:

- Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the Oklahoma's Comprehensive Cybersecurity Plan (CCP) and address a performance gap identified through the NCSR and contribute to building a capability that will be evaluated through a formal exercise.

Exercise:

- Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise, design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/ emergency-managers/national- preparedness/exercises/hseep. Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises.

ALLOWABLE COSTS

For FY 2024 SLCGP, grant funds may be used for the following:

1. Cybersecurity Planning and Strategy Development: Funding can be used to create or update cybersecurity plans and strategies for improving overall system security.
2. Cybersecurity Training and Exercises: Costs for training personnel, conducting cybersecurity exercises, and improving workforce capabilities are allowed.
3. Acquisition of Cybersecurity Tools and Technology: This includes software, hardware, and other technical solutions aimed at enhancing the security of information systems.
4. Information Sharing and Analysis Centers (ISACs): Participation in or establishment of ISACs to promote sharing threat intelligence and best practices.
5. Enhancing Security Measures for Critical Infrastructure: Investing in systems that support critical services like emergency response and other public safety functions.

Examples of allowable costs include but are not limited to:

- Upgrading legacy technology.
- Replacing or installing servers or network components onto existing racks and using existing cabling.
- Hardware/Software for enhancing cybersecurity posture.
- Implementing or revising the Cybersecurity Plan.
- Pentesting/Vulnerability Assessments
- Hiring Cybersecurity or Administration Staff
- Cybersecurity Certifications for Employees
- Local end-user cybersecurity training and awareness campaigns
- Network Monitoring Tools and Services
- Network Scanning Tools and Services
- Protection solutions for equipment and networks
- Paying expenses directly relating to the administration of the grant, which cannot exceed 5% of the amount of the grant award.
- One tabletop device such as a computer or workstation for aiding an existing server function or facilitating the setup of a new server acquired through the grant.
- Assisting with allowed activities that address imminent cybersecurity threats confirmed by DHS; and
- Installation of new equipment cabling through existing conduit with no new holes drilled

in walls, ceilings, or floors can be made.

- Classroom only training
- Computer or software training
- Training at a designated training facility that does not involve ground disturbances or equipment installation.

Recipients and subrecipients may use SLCGP funding to perform minor modifications that **do not** substantially affect a building, or other physical facility's, structure, layout or systems; affect critical aspects of a building's safety; or otherwise materially increase the value or useful life of the building or other physical facility. The prohibition would also apply to the nonfederal cost-sharing requirement detailed in Section 2220A(m). As a reminder, all projects and associated budgets must support the approved Cybersecurity Plan and be approved in advance by the Cybersecurity and Infrastructure Security Agency and FEMA.

Examples of the types of minor modifications that could be **allowable** with SLCGP funding, and the non-federal cost share are listed below:

- Fastening equipment to building or other physical facility walls where it does not become a permanent fixture (such as hanging a server rack with servers on a building wall).
- Replacing an outdated existing electrical or internet outlet into which the equipment will connect.
- Installing new cabling.
- Replacing existing cabling.
- Moving cabling.
- Installing and connecting information system equipment to the building's network and power supply and internet.
- Making a hole in the wall to attach the equipment to the building's network, power, or internet.

Because Section 2220A(n)6) does not apply to minor modifications that do not: substantially affect a building or other physical facility's structure, layout or systems; affect critical aspects of a building or other physical facility's safety; or otherwise materially increase the value or useful life of a building or other physical facility, minor modifications **may be permitted under the SLCGP subject to additional reviews.** As a reminder, recipients (and subrecipients through the

State Administrative Agency (SAA)) are required to submit projects for minor building modifications approval to the Grant Programs Directorate Environmental Planning and Historic Preservation Branch.

UNALLOWABLE COSTS

For FY 2024 SLCGP, grant funds may not be used for the following:

1. Unallowable remodeling and alterations include permanent modifications that substantially affect the buildings, or other physical facility's, structure, layout or systems; affect critical aspects of a buildings or other physical facility's safety (such as structural integrity and fire safety systems); or other modifications that materially increase the value or useful life of the building or other physical facility.

- Examples of the types of construction, remodeling and alterations that are unallowable with SLCGP funding, or the non-federal cost share, are listed below:
    - Constructing a new building or other physical facility.
    - Updating an electrical system to a building or other physical facility that involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers.
    - Installing new walls or reconfiguring existing walls.
    - Affixing equipment in such a way that it becomes a permanent part of a building or other physical facility (as this would result in the equipment no longer being personal property).

2. Routine Administrative Costs: Day-to-day administrative expenses and indirect costs that do not directly enhance cybersecurity capabilities are unallowable.
3. Operational and Maintenance Costs for Existing Systems: These include routine maintenance fees for systems already in place that are not being upgraded or enhanced under the grant

Examples of unallowable costs include but are not limited to:

- Spyware
- Construction
- Renovation
- To pay a ransom
- For recreational or social purposes
- To pay for cybersecurity insurance premiums
- To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building.)
- For any purpose that does not address cybersecurity risks or cybersecurity threats on

information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity

- To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses and
- For any recipient or subrecipient cost-sharing contribution.
- Purchase of multiple laptops/computers; a laptop/computer can be requested if it's needed to run a certain application, service, etc.