Frequently Asked Questions
State and Local Cybersecurity Grant Program (SLCGP)

GENERAL INFORMATION

The SLCGP was established by the Bipartisan Infrastructure Law, also known as the Infrastructure Investment and Jobs Act (IIJA) in 2021. The SLCGP will appropriate $1 billon to be awarded over four years with the intent of helping state, local, and territorial governments address cybersecurity risks and threats. Funding for each state is calculated by a formula determined by the Cybersecurity and Infrastructure Security Agency (CISA).

The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states, local governments, rural areas, and territories address cybersecurity risks and cybersecurity threats to information systems.

This program is being jointly managed by CISA and the Federal Emergency Management Agency (FEMA). In Kansas, the SLCGP is administered by the Kansas Information Security Office (KISO) and projects are reviewed and approved by the Kansas Cybersecurity Planning Committee.

In Kansas we have about 3,600 public entities across the state who are eligible to potentially participate in this program. You must be a public entity to submit an application and receive funds from this program. Some examples of public entities are counties, cities, municipalities, public hospitals, public school districts, public utilities, state funded colleges, and public water/wastewater systems. Entities like 501c3 organizations, vendors, contractors, or private sector entities are NOT eligible to participate in this program.

Q: Who can submit an application?

A: You must be a public entity to submit an application and receive funds from this program. Some examples of public entities are counties, cities, municipalities, public hospitals, public school districts, public utilities, state funded colleges, and public water/wastewater systems.

Q: Can non-profit organizations submit an application?

A: No. Non-profit organizations, vendors, contractors, and private sector entities are NOT eligible to participate in this program.

Q: What is considered a rural area?

A: Per 49 U.S.C. 5302 “rural” is any area with a population of less than 50,000 individuals. In Kansas rural/non-rural is determined by the population of the county.

Q: Can we submit more than one project?

A: Yes. Applicants are encouraged to separate your projects based on area of need and submit separate applications for each area of need. The Kansas Cybersecurity Planning Committee will not fund partial applications. The application will either be approved or denied. They will not fund specific projects within the application.

Q: Do you have a way for us to do a self-assessment for cybersecurity?

A: CISA has a checklist called the Cybersecurity Program Goal or (CPG). It's a checklist that covers a variety of different areas and if you haven't gone through that with your organization, we recommend it. It can help you see where your entity currently is with your cyber posture and point out some areas where you might want to focus for areas that aren't as strong.

Q: What type of projects can we submit for grant funding?

A: All projects submitted must tie back to the Kansas Cybersecurity Plan Kansas Cybersecurity Plan and address an identified threat, hazard, gap, or need. Entities are strongly encouraged to include projects related to K-12 education, healthcare, water/wastewater, energy, defense, and elections infrastructure.

Some specific areas of need are:

- Implementation of Multi-Factor Authentication (MFA).
- Enhanced logging.
- Security Awareness Training.
- Data encryption for data at rest and in transit.
- End use of unsupported/end of life software and hardware that are accessible from the internet.
- Endpoint detection and monitoring.
- Ensure the ability to reconstitute systems (backups).
- Creation of Technology/Cyber Resiliency Plans.
- Utilizing only enterprise email platforms that are secure.
- Testing of existing plans, policies, procedures.
- Prohibit use of known/fixed/default passwords and credentials
- Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

Q: One of the program goals mentions Technology/Cyber Resiliency Planning, what is that?

A: The Technology/Cyber Resiliency Program(TCRP) is a series of plans for preparing on the technology side to support the operational function of an entity or agency in the case of an incident. Many entities are already familiar with Continuity of Operations or COOP, which is operational planning or what an entity does from an operational standpoint on a daily, weekly, monthly, and yearly basis. COOP planning tends to only focus on your mission essential or mission critical functions, but TCRP looks at all of the business functions that the agency/entity does. It assists the entity with making sure that the priorities on the technology side align with providing the resources to meet the operational side of the house.

Q: If we want to create policies/procedures for our entity, do you have any suggestions for creating those?

A: In Kansas we have the Information Technology Executive Council (ITEC). It is a legislatively created body that creates the policies and standards that all state agencies adhere to and maintain. Most of that is in lockstep with any federal compliances that we have, but it's a great resource to look at if you're looking for different types of policies, procedures, or standards.

Q: Can we ask for funds for items that are going to be end of life soon? Or does it have to already be past end of life?

A: You can request funding for those items. Best practice is not to wait until after they are past end of life.

Q: Are there limits to what we can use grant funds for?

A: Grant funds may not be used for any of the following:

- 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;
- 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.

Q: Does "cybersecurity" also cover access control systems for school buildings and security camera systems. Are those IoT possible options or do we need to focus on primary options that directly impact Internet access?

A: The physical access control and cameras for security would fall under the Homeland Security Grant that is administered by the Kansas Highway patrol. At this time these physical accesses are not outlined in our whole of state plan as we have multiple entities including schools around the state with past end of life computer equipment and little or no IT/Cybersecurity infrastructure. I would contact your local Emergency Management in your county. They could assist you will physical assessments and can probably assist with the grant information for HSGP grant.

Q: Is there a limit to the dollar amount that each entity can ask for?

A: No, but we have a set amount of funds to distribute. Funding for individual projects will be determined based on availability of funds and in consideration of various factors, including number of applications received, total amount of funding requested by all entities for projects, cost-effectiveness, impact on cybersecurity, and whether the project will benefit rural communities.

Q: Why does it matter whether the project will benefit rural communities?

A: 25% of the total federal award must go to rural areas. This pass-through to rural areas is a part of the overall 80% pass-through; however, it should be emphasized that 25% of the total federal amount must be passed through to rural areas. (See Qualified Entities section for further information on rural areas.)

Q: Who should we put as the Authorized Official on our application?

A: The Authorized Official is the person who has the authority to sign documents/contracts on behalf of the entity. They must have legal authority to sign the documents if grant funding is awarded.

COST MATCH

Q: What is cost match?

A: Cost match is the required contribution to the project the subrecipient will make for the grant funds they are awarded. The match will either be Hard Match (Cash) or Soft Match (In-kind). The Cost Match for FY23 is 20% per project and must be verifiable, reasonable, allocable, necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations.

Q: What is Hard Match?

A: Hard Match (Cash) includes cash spent for project-related costs such as State or local general fund monies.

Q: What is Soft Match?

A: Soft Match (In-kind) is contributions of the reasonable value of property or services in lieu of cash. Includes things like such as salaries and fringe benefits, equipment, supplies, etc. Soft match items must be related to the SLCGP program's goals, objectives, NOFO, etc.

Q: Can we use other grant funds to cover the cost match for this program?

A: No. You cannot use funds from a different grant to cover the cost match for this grant. You also cannot use these grant funds to cover the cost match for another grant. It cannot be paid through any grant funding. It cannot be used to match any other grants.

PROCUREMENT/FINANCIAL

Q: What is procurement?

A: Procurement is the process for purchasing the good, services, etc. It includes the Federal, State, and Local laws, rules, guidelines, and procedures for purchasing. When using grant funds, the most restrictive regulations must be used. If the subrecipient uses their own procurement rules you must prove that they are equal to or more restrictive than the Federal 2CFR requirements.

Q: Are there contracts that are already in place that we can use to purchase items instead of dealing with bids?

A: There are State of Kansas contracts for IT and cybersecurity that have been opened to any political subdivision. If there is a state contract for the items you need, you can use it and would not need to go out for bids. The State's procurement regulations/process meets the requirements for 2 C.F.R. You can search the State's contracts here: State of Kansas Contract Search

Q: If we already use a product or service, can we apply for grant funds to pay for them?

A: If you already use a basic program, you can submit an application for the upgrade/additional services. You would have to pay the cost for the basic program and the grant would pay the cost for the upgrade. The invoice must clearly document the basic rate and the cost for the upgrade. You cannot use grant funds to pay for the basic service you already have, that is considered supplanting.

Q: What is supplanting?

A: SLCGP funding cannot be used to replace (i.e., "supplant") what an organization is already spending (or had already budgeted to spend) on services/solutions. Existing projects that were already included in a budget or put out for bids may not be submitted for grant funds.

Q: Can vendors help prepare our applications for grant funds?

A: If a vendor helps prepare the grant application, it would conflict them out of bidding the project or providing the services. Per the Notice of Funding Opportunity "…contractors that develop or draft specifications, requirements, statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a non-federal entity develop its grant application, project plans, or project budget."

Q: Are there any vendors/contractors that we cannot work with?

A: It is your responsibility to be sure that the vendor/contractor is not suspended or debarred. You can check that information by searching for them at: SAM.gov | Search

---

Q: What laws do we have to follow if we are awarded grant funds?

A: The Code of Federal Regulations, Title 2 (2 C.F.R. §§ 200.317 – 200.327) are the Federal regulations for procurement.

The State of Kansas regulations for procurement are K.S.A. 75-3739.

All applicants must have and use their own documented procurement procedures that reflect applicable local laws and regulations.

Q: Can grant money be used to pay for multi-year service contracts upfront?

A: If you want to purchase a multi-year service contract, it must be done as a one-time payment. You cannot make payments over multiple years.

Q: When can we make purchases using grant funds?

A: Purchases/expenditures must be made during the period of performance of the grant to be reimbursable. They must also be purchased after the grant is awarded and all related award paperwork has been signed.

Q: Do we have to include a quote from a vendor with the application?

A: No. To avoid any potential conflict of interest, you should not get quotes or bids from any vendor/contractor before the grant funds are awarded. You can get general information, but not quotes for specific products/services.

REQUIRED PARTICIPATION

Q: Do we have to have a UEI number?

A: Every subrecipient of award funds is required to have a Unique Entity ID (UEI) number. Pursuant to 2 C.F.R. Part 25, Appendix A, no entity may receive a subaward until the entity has provided its UEI number to us. If you already have a UEI number, you do not need to register for another one.

Q: Do we have to be on a .gov domain?

A: FEMA/CISA are requiring subrecipients to transition to the .gov domain. Educational institution subrecipients using .edu are exempted from transiting to the .gov internet domain due to the nature of the .edu internet domain. All other subrecipients are required to be on the .gov domain or in the process of transitioning to the .gov domain.

Q: Do we have to be members of any groups to be eligible for grant funding?

A: Entities are not required but are encouraged to be a member of the Multi-State Information Sharing & Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing & Analysis Center (EI-ISAC). Membership is free and there are a lot of resources available through them.

Q: What CISA services do we have to participate with to be eligible for FY23 grant funds?

A: For FY23, all subrecipients are required to actively participate with the CISA Cyber Hygiene Program - Vulnerability scanning service. This service monitors and assesses internet-accessible network assets to evaluate their vulnerability status. You will receive weekly reports of findings and alerts about urgent findings, like potentially risky services and known exploited vulnerabilities. You can get additional information here: CISA Vulnerability Scanning. You must also Complete the NCSR through MS-ISAC. Open registration for NCSR is Oct 1-Feb 28th and you must be registered to complete this before making application.

Q: Do we have to complete the NCSR before we submit an application?

A: You do not have to compete the review before applying, but you must begin it. Eligible entities and their subrecipients are required to complete the NCSR, administered by MS-ISAC, during the first year of the award/subaward period of performance and annually. If you aren't familiar with the NCSR, it's a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the NIST Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. You can get additional information here: Nationwide Cybersecurity Review (NCSR). Registration for the NCSR is only open through MS-ISAC from October 1, 2024 – February 28, 2025. You must register to complete the assessment before applying for this grant.

APPLICATION PROCESS/SCHEDULE

Q: How soon will the FY23 funds be awarded?

A: It will take several months after the application period closes. All projects have to be reviewed by the Kansas Cybersecurity Planning Committee, FEMA, and CISA. If you have a project that you need to implement in the next few months, there probably will not be time to get it through the process.

Q: What if we do the project and then are awarded funds for doing the project?

A: No project can be started or completed before the award is granted and accepted. You also cannot submit a project and then use grant funds for something different. If you change the project, you could forfeit all or part of the funding.

Q: How do we apply for grant funds?

A: Applications will be handled through eCivis Portal, a grants management system. All applicants will need to create an account to access the application. The portal can be accessed at: eCivis Portal | Login

---

Q: How does eCivis work?

A: There is a guide to using eCivis on the KISO website: Kansas eCivis Portal User Guide

---

Q: How long will we have to apply for grant funds?

A: The link to apply will be live starting on January 20th and will be valid through the end of the day February 28th.

Q: How does this process work?

A: The process begins with eligible entities submitting applications. Then those applications have to be reviewed by the Kansas Cybersecurity Planning Committee (KCPC). The KCPC will meet to vote on the projects and the projects will be sent to FEMA and CISA for review and approval. We will receive notification from FEMA and CISA which projects are approved. When we receive those approvals, we will contact applicants to get award documents signed.