STATE OF MICHIGAN
FISCAL YEAR 2023 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

APPLICATION GUIDANCE FOR SUBAPPLICANTS

Contents

State and Local Cybersecurity Grant Program (SLCGP) Overview

Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of state, local, and tribal (SLT) governments is an important homeland security mission and the primary focus of SLCGP. Through funding from the Infrastructure Investment and Jobs Act referred to as the Bipartisan Infrastructure Law throughout this document, the SLCGP enables the Department of Homeland Security (DHS) to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their communities.

This guidance document is being provided to assist eligible entities in Michigan with applying for grant funds under the Fiscal Year (FY) 2023 SLCGP. The FY 2023 SLCGP grant funds will be awarded competitively. Submitting a grant application does not guarantee funding. Applicants should not enter into any contracts or obligations dependent upon the use of FY 2023 SLCGP funds until after award announcements are made, all required documentation has been submitted to the Michigan State Police, Emergency Management and Homeland Security Division, and appropriate procurement standards have been followed. No costs incurred prior to the State of Michigan subaward date, which will be outlined in the subrecipient grant agreement, will be eligible for reimbursement.

Objectives

The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk.

In FY 2023, Michigan is focusing on the following program objectives:

- Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Implement security protections commensurate with risk.
- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Eligibility

The State of Michigan is the direct recipient of FY 2023 SLCGP funds and will subgrant a minimum of 80% of funds to successful subapplicants. Eligible subapplicants under the FY 2023 SCLGP include local and tribal governments located in the state of Michigan. Local government is defined in 6 U.S.C. § 101(13) as:

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
- An Indian tribe or authorized tribal organization; and
- A rural community, unincorporated town or village, or other public entity.

Organizations listed above must complete the subgrant application to be considered for FY 2023 SCLGP funding as a subrecipient.

Allowable Project Areas

The State of Michigan has identified eight project areas that will be considered for funding. All project requests must align with one of these eight areas, as described below.

Endpoint Detection & Response
Purchase subscriptions for Endpoint Detection and Response, Managed Detection and Response, and Extended Detection and Response licensing vendor selected utilizing entities established procurement policies and grant performance and spend period time frames. Subscriptions cannot go past November of 2027.
Cybersecurity Assessments
Purchase an independent Cybersecurity Assessment OR Penetration Testing for the organization utilizing existing MiDEAL negotiated contractors.
Multifactor Authentication Solutions (MFA)
Purchase authentication devices, MFA Software, or other systems/hardware supporting MFA such as Identity and Access Management systems.
Advanced Backup Solutions
Purchase backup software, cloud services, backup servers, storage devices, or other services that support recovery and reconstitution of entity backup data.
Migration to the .gov Domain
Pay for services that support the migration of the organization's domain to a .gov internet domain. Managed Service Provider services to pay support vendors to perform migration tasks to a.gov domain.
Managed Service Provider Costs to pay for Cybersecurity Services
Pay Managed Service Providers for cybersecurity services that mitigate risk, improve cyber resiliency, and perform cybersecurity work where an organization does not have onsite staff to support.
Cybersecurity Awareness Training
Purchase subscriptions for cybersecurity awareness training for employees to better understand cyber threats, best practices, incident response, compliance, and policies. KnowBe4, Proofpoint, SANS Institute & Infosec IQ are examples of vendors providing security awareness training.
Cybersecurity Professional Training for IT/Security Staff
Purchase professional cybersecurity training for those responsible for mitigating risk and maintaining resiliency in the organization's environment. Example Trainings: CompTIA, CySA+, PenTest+ Certification Training, SANS Institute Enterprise Cloud Security Architecture, Certified Ethical Hacker, Security Training, and Certifications that will increase the skills and knowledge of systems and security IT administration teams.

How to Apply

To apply, complete and submit the State of Michigan FY 2023 SLCGP Subgrant Application using the link below:

FY 2023 Michigan SLCGP Subgrant Application

All applications must be submitted by **11:59 PM, December 30, 2024**.

If you would like a copy of your submission, please be sure to check the box at the bottom of the form, "Please send me a copy of my responses".

Completing the Application

Follow the instructions below when completing the subgrant application. You may want to initially compile your responses in Microsoft Word and paste the data into the subgrant application form. The application link above will not save your data until you submit the application. You cannot start an application and return to it later.

NOTE: Do not specify a vendor or brand name in your grant application as the product you intend to purchase. All procurement under federal grants must adhere to federal procurement standards. Refer to the Procurement Integrity section of this document for additional information.

Subapplicant Information

- Organization: Enter the title of the organization requesting funds.
- Primary Point of Contact (POC) First Name: Enter the first name of the individual who should be contacted with questions regarding the subgrant application.
- Primary POC Last Name: Enter the last name of the individual who should be contacted with questions regarding the subgrant application.
- Point of Contact (POC) Email: Enter the email address for the identified Primary POC.
- Primary POC Telephone Number: Enter the telephone number for the identified Primary POC.
- Secondary POC First Name: Enter the first name of a second individual who can be contacted with questions regarding the subgrant application. This individual may be contacted if the Primary POC is unable to be reached and is necessary in the event of potential staffing changes.
- Secondary POC Last Name: Enter the last name of a second individual who can be contacted with questions regarding the subgrant application. This individual may be contacted if the Primary POC is unable to be reached and is necessary in the event of potential staffing changes.
- Secondary POC Email: Enter the email address for the identified Secondary POC.
- Secondary POC Telephone Number: Enter the telephone number for the identified Secondary POC.
- County: Select the county where your organization is located from the dropdown list.
- Unique Entity Identifier (UEI): Enter your organization's UEI. The UEI is issued by the System for Award Management (SAM). A UEI is required to receive federal funds. Instructions for requesting a UEI can be found at: SAM.gov | Entity Registrations.
- Vendor ID Number: Enter your organization's State of Michigan (SOM) Vendor ID number. A SOM vendor ID is required to receive reimbursement for FY 2023 SLCGP funded projects. To receive a vendor ID, register with the SOM SIGMA Vendor Self Service at: Doing Business with the State (michigan.gov).

Project Information

- Project Identification: Select the project area to which your funding request aligns from the dropdown menu.

- Project Narrative: Provide a brief narrative of your project request. The project description should provide enough detail to provide the reviewer with a thorough understanding. Please be sure to address the following questions:
    - What is being requested?
    - How was the need for the requested project identified?
    - What impact will the implementation of the project have on your cybersecurity posture?
    - Why is this currently the best solution for your organization's cybersecurity needs?
    - How will the project be sustained once grant funds are exhausted?
- Funding Request Total: Enter the total amount of funding being requested under this project.
- Solution Area: Select the appropriate solution area(s) from the dropdown list. Please see the Allowable Costs - planning, organization, equipment, training, or exercises (POETE) Solution Areas section of this document for additional information.
- Budget Narrative: Provide a brief budget narrative describing how funds will be used. Itemize the costs and provide the unit costs, total units, and total cost for each item.
- Partial Funding: Select yes or no from the dropdown to indicate if your project could be effectively implemented with a reduced amount of funding than what is being requested. If you select yes to this question, you will be asked to describe the partial funding option.
- Description of Partial Funding: This question will only appear if you answer yes to the Partial Funding question. If your project can be effectively implemented with less funding, please describe what would be funded, in priority order, and the cost for each item. Describe any limitations partial funding may cause and what could still be accomplished with a reduced amount.
- Previously Funded: Identify if your organization received funding under the FY 2022 SLCGP by selecting yes or no from the dropdown list.
- Organization Size: Identify if your organization is small, medium, larger, or extra large by selecting the appropriate option from the dropdown list. The organization size is based on the total number of endpoints in your organization.
- Number of Endpoints: Enter the total number of endpoints in your organization.
- Was Need Identified Through an Assessment: Indicate if the need for the requested project was identified through a cybersecurity assessment by selecting yes or no.

Certifications and Executive Compensation

- Non-Supplanting Certification: Check the box to indicate you understand that supplanting is unallowable. Supplanting occurs when state or local funds that were appropriated for the same purpose are replaced with federal dollars. Grant funds must be used to supplement existing funds and not replace (supplant) due to the receipt of federal funds.
- Suspension and Debarment: From the dropdown list, select yes if your organization is currently suspended or debarred from doing business with the federal government; select no if your organization is not suspended or debarred.

  Suspension and debarment are administrative remedies that prevent individuals and entities from participating in government contracts, subcontracts, grants, loans, and other covered transactions. You can search your organization's status by searching for Exclusions on SAM.gov | Home. Guidance for searching Exclusions on SAM.gov can be found here: GSAFSD Tier 0 Knowledge Base - How do I search for active exclusions?

- Executive Compensation: If your organization received 80% or more of its annual gross revenue in United States federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements AND received $25 million or more in annual gross revenues from Federal procurement contacts (and subcontracts) and/or Federal financial assistance (subawards) in the preceding fiscal year, select yes. If not, select no. If you select yes, you will be prompted to answer another question.

  Information provided in this section will be used by the MSP/EMHSD for compliance under 2 Code of Federal Regulations (CFR), Chapter 1, Part 170. Reporting Sub-Award and Executive Compensation Information.

- Executive Compensation – Public Access: This question will only appear if you answer yes to the question above. If the public has access to information about the compensation of the five highest paid executives in your agency through periodic reports filed under section 13(a) or 15(d) of the Security Exchange Act or section 6104 of the Internal Revenue Code, select yes. If not, select no. If you select no, you will be prompted to provide the name and salary from the previous fiscal year of the top five highest paid executives in your organization.
- Executive Name: This question will only appear if you answer yes to the first executive compensation question and no to the second executive compensation question. It will also be duplicated for a total of five entries. Enter the name of the top five highest paid executives in your organization.
- Executive Amount: This question will only appear if you answer yes to the first executive compensation question and no to the second executive compensation question. It will also be duplicated for a total of five entries. Enter the total salary from the preceding fiscal year of the top five highest paid executives in your organization.

Requirements and Restrictions

Required Cybersecurity and Infrastructure Security Agency (CISA) Services if awarded:

All SLCGP subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a subgrant but is a post-award requirement.

- **Web Application Scanning** is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
- **Vulnerability Scanning** evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Completing the Nationwide Cybersecurity Review (NCSR)**, administered by the Multi-state Information Sharing and Analysis Center, during the first year of the award/subaward period of performance and annually thereafter. The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs.

Prohibitions on Expending Federal Emergency Management Agency (FEMA) Award Funds for Covered Telecommunications Equipment or Services:

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 CFR §§ 200.216, 200.327, 200.471, and Appendix II

to 2 CFR Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services or superseding document.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards (fema.gov).

Effective August 13, 2020, FEMA recipients and subrecipients may not use any FEMA funds under open or new awards to:

- Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
- Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
- Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Allowable Costs - POETE Solution Areas

Allowable costs must fall into the categories of POETE, aligned to closing capability gaps or sustaining capabilities.

Planning

The SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide Cybersecurity Plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements.

Organization

Subapplicants must justify proposed expenditures of SLCGP funds to support organization activities within their subgrant application. Organizational activities may include the following:

- Program management;
- Development of whole community partnerships that support the approved Cybersecurity Planning Committee;
- Structures and mechanisms for information sharing between the public and private sector; and
- Operational support.

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP POETE activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators. **The subapplicant must demonstrate that the personnel will be sustainable once grant funds are no longer available.**

Equipment

The 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 government entities.
All equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using SLCGP funds. Please refer to FEMA's Authorized Equipment List | FEMA.gov. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM guidance recommendations. Such investments must be coordinated with the Statewide Inoperability Coordinator and the State Interoperability Governing Body to ensure interoperability and long-term compatibility.

The 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.

The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees is allowable, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by the maintenance or warranty plan must not exceed the period of performance of the specific grant funds used to purchase the plan or warranty.

Training

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 with the state's approved Cybersecurity Plan, address a performance gap identified through assessments, and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to underserved communities (e.g., children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity, and other underserved populations that may be more impacted by disasters) should be identified in the assessment and addressed in the state's training cycle. Subrecipients are encouraged to use existing training rather than developing new courses. When developing new courses, subrecipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate model of instructional design.

Subrecipients are also encouraged to use FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness, the Emergency Management Institute, and FEMA's Training Partner Programs, including the Continuing Training Grants, the National Domestic Preparedness Consortium, the Rural Domestic Preparedness Consortium, and other partners. The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, and territorial audiences.

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**. Additional information on training requirements and EHP review can be found online at Environmental & Historic Preservation Guidance for FEMA Grant Applications | FEMA.gov.

Cybersecurity and Infrastructure Security Agency (CISA's) Federal Virtual Training Environment offers cybersecurity training to federal, state, local, tribal, and territorial government employees, which offers education and certifications aligned with the NICE Framework. Additional information can be found at https://fedvte.usalearning.gov.

Exercises

Exercises conducted with grant funding should be managed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). The 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 exercise activities require 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**. Additional information on exercise requirements and EHP review can be found online at Environmental & Historic Preservation Guidance for FEMA Grant Applications | FEMA.gov.

Procurement Integrity

Through audits conducted by the DHS Office of Inspector General and FEMA grant monitoring, findings have shown that some FEMA recipients and subrecipients have not fully adhered to the proper procurement requirements at *2 CFR §§ 200.317 – 200.327* when spending grant funds. Anything less than full compliance with federal procurement requirements jeopardizes the integrity of the grant as well as the grant program. For detailed guidance on the federal procurement standards, subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT), such as the PDAT Field Manual and Contract Provisions Guide. Additional resources, including an upcoming training schedule, can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

All procurement activity must be conducted in accordance with federal procurement standards at *2 CFR §§ 200.317 – 200.327*. Select requirements under these standards are listed below. All subrecipients must have and use their own documented procurement procedures that reflect applicable state, local, and tribal laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in *2 CFR Part 200*. These standards include but are not limited to, providing for full and open competition consistent with the standards of *2 CFR § 200.319* and the required procurement methods at *§ 200.320*.

Important Changes to Procurement Standards in 2 CFR Part 200

The federal Office of Management and Budget (OMB) recently updated various parts of Title 2 of the CFR, among them, the procurement standards. All subrecipients should, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States per *2 CFR § 200.322*. More information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: OMB Revisions.

The recognized procurement methods in 2 CFR § 200.320 have been reorganized into informal procurement methods, which include micro-purchases and small purchases; formal procurement methods, which include sealed bidding and competitive proposals; and noncompetitive procurements. The federal micro-purchase threshold is currently $10,000, and subrecipients may use a lower threshold when using micro-purchase procedures under a FEMA award. If a subrecipient wants to use a micro-purchase threshold higher than the federal threshold, it must follow the requirements of 2 CFR § 200.320(a)(1)(iii)-(v). The federal simplified acquisition threshold is currently $250,000, and a subrecipient may use a lower threshold but may not exceed the federal threshold when using small

purchase procedures under a FEMA award. *See* 2 CFR § 200.1 (citing the definition of simplified acquisition threshold from 48 CFR Part 2 Subpart 2.1).

See *2 CFR §§ 200.216, 200.471* and the Requirements and Restrictions section of this document regarding prohibitions on covered telecommunications equipment or services.

Competition and Conflicts of Interest

Among the requirements of *2 CFR § 200.319(b)* applicable to all subrecipients, in order to ensure objective contractor performance and eliminate unfair competitive advantage, 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. The 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. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the non-federal entity.

Under this prohibition, unless the subrecipient solicits for and awards a contract covering both the development and execution of specifications (or similar elements as described above) and this contract was procured in compliance with *2 CFR §§ 200.317 – 200.327*, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post-award costs, such as grant management fees.

Additionally, some of the situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Organizational conflicts of interest;
- Specifying only a “brand name” product instead of allowing “an equal” product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Per *2 CFR § 200.319(c),* subrecipients must conduct procurements in a manner that prohibits the use of statutorily or administratively imposed state, local, tribal, or territorial geographical preferences in the evaluation of bids or proposals, except in those cases where applicable federal statutes expressly mandate or encourage geographic preference. Nothing in this section preempts state licensing laws. When contracting for architectural and engineering services, geographic location may be a selection criterion provided its application leaves an appropriate number of qualified firms, given the nature and size of the project, to compete for the contract.

Under *2 CFR § 200.318(c)(1),* subrecipients are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. **No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if they have a real or apparent conflict of interest.** Such conflicts of interest would arise when the employee, officer or agent, any member of their immediate family, their partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the non-federal

entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, subrecipients may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the subrecipient.

Under *2 CFR 200.318(c)(2),* if the subrecipient has a parent, affiliate, or subsidiary organization that is not a state, local, tribal, or territorial government, the subrecipient must also maintain written standards of conduct covering organizational conflicts of interest. In this context, an organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the subrecipient is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The subrecipient must disclose in writing any potential conflicts of interest to the MSP/EMHSD, in accordance with applicable FEMA policy.

Supply Schedules and Purchasing Programs

Generally, a subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement. See related compliance requirements below.

General Services Administration Schedules

State, local, and tribal(SLT) governments and any instrumentality thereof (such as local education agencies or institutions of higher education) may procure goods and services from a General Services Administration (GSA) schedule. The GSA offers multiple efficient and effective procurement programs for SLT governments, and instrumentalities thereof, to purchase products and services directly from pre-vetted contractors. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term government-wide contracts with commercial firms that provide access to millions of commercial products and services at volume discount pricing.

Information about GSA programs for SLT governments, and instrumentalities thereof, can be found at https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments.

For SLT governments and their instrumentalities that purchase off of a GSA schedule, this will satisfy the federal requirements for full and open competition provided that they follow the GSA ordering procedures; however, tribes, local governments, and their instrumentalities will still need to follow the other rules under *2 CFR §§ 200.317 – 200.327*, such as solicitation of minority businesses, women's business enterprises, small businesses, or labor surplus area firms *(§ 200.321*), domestic preferences *(§ 200.322*), contract cost and price *(§ 200.324*), and required contract provisions *(§ 200.327 and Appendix II*).

Other Supply Schedules And Programs

For subrecipients that want to procure goods or services from a state supply schedule, cooperative purchasing program, or other similar program, in order for such procurements to be permissible under federal requirements, the following must be true:

- The procurement of the original contract or purchasing schedule and its use by the subrecipient complies with state and local law, regulations, and written procurement procedures.
- The state or other entity that originally procured the original contract or purchasing schedule entered the contract or schedule with the express purpose of making it available to the subrecipient/non-federal entity and other similar types of entities.

- The contract or purchasing schedule specifically allows for such use, and the work to be performed for the subrecipient falls within the scope of work under the contract as to type, amount, and geography.
- The procurement of the original contract or purchasing schedule complied with all the procurement standards applicable to a non-federal entity other than states under *2 CFR §§ 200.317 – 200.327*. and
- With respect to the use of a purchasing schedule, subrecipients must follow ordering procedures that adhere to applicable state, tribal, and local laws and regulations and the minimum requirements of full and open competition under *2 CFR Part 200*.

If a subrecipient seeks to use a state supply schedule, cooperative purchasing program, or other similar type of arrangement, it is recommended the subrecipient discuss the procurement plans with the MSP/EMHSD prior to procurement.

Procurement Documentation

Per 2 CFR § 200.318(i), subrecipients are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. For any cost to be allowable, it must be adequately documented per *2 CFR § 200.403(g)*.

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

Additional information on required procurement records can be found on pages 24-26 of the PDAT Field Manual.