State and Local Cybersecurity Grant Program (SLCGP)

Federal Fiscal Year

2022 & 2023

Local Grant Guidance

State of Alaska
Department of Military and Veterans Affairs
Division of Homeland Security and Emergency Management

Federal Fiscal Year 2022/2023 State and Local Cybersecurity Grant (SLCGP) State Overview and Guidelines

Overview and Eligibility

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on network technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities. Strengthening cybersecurity practices and the resilience of state and local governments is a vital homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP).

The SCLGP is a reimbursable, federally funded pass-through grant program to assist local and tribal units of government with managing and reducing systematic cyber risk.

“Local government” is defined in 6 U.S.C. § 101(13) as:

A) 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;

B) An Indian tribe or authorized tribal organization, or in Alaska, a Native village or Alaska Regional Native Corporation; and

C) A rural community, unincorporated town, village, or other public entity.

Available Funding

The funding amount for Alaska under the FY2022 SLCGP is $2,245,130, and the FY2023 SLCGP is $4,567,677. For FY2022, $968,814.65 has been awarded for cybersecurity assessments, training, and multi-factor authentication projects. The remaining funds available for FY2022 are $1,276,168.35.

The SLCGP requires a minimum 80% pass-through to local government entities, including a minimum 25% pass-through specifically to rural areas. The FY2022 SLCGP requires a 10% non-federal cost share, or match, raising the total amount of funding to almost $2.5 million. The State of Alaska will provide the entire 10% non-federal cost share (local match) for the FY2022 SLCGP. For FY2023, eligible SLCGP applicants must meet the 20% non-federal cost share (local match). We are currently anticipating the State of Alaska will provide the match requirement, but it can be subject to change depending on the approved state budget.

2022 Period of Performance:

- **Performance Start Date:** February 1, 2024
- **Performance End Date:** December 31, 2025

2023 Period of Performance (subject to change):

- **Performance Start Date:** August 1, 2024
- **Performance End Date:** August 31, 2026

The Alaska Division of Homeland Security and Emergency Management (DHS&EM) solicits jurisdictional applications for the Federal Fiscal Year FY2022/2023 State and Local Cybersecurity Grant (SLCGP). **Applications are due by 11:59 pm, Friday, March 29, 2024.**

The federal Department of Homeland Security (DHS) has released the FY2022 and 2023 SLCGP Notice of Funding Opportunity (NOFO) to states. The NOFOs are posted on the DHS&EM website at DHS&EM | State and Local Cybersecurity Grant Program (SLCGP) (alaska.gov)

Eligible applicants for this program must meet the definition of local government found in 2 CFR Part 200.64 or a tribal government found in 2 CFR Part 200.54.
AND:

The jurisdiction must comply with the standards, regulations, and requirements applicable to subrecipients receiving pass-through subawards found in 2 CFR Part 200—Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=dcda7ff3275e13d43b34534d456521d7&mc=true&n=pt2.1.200&r=PART&ty=HTML)
Financial and program management standards in 2 CFR include but ARE NOT limited to requirements of jurisdictional financial management systems, established internal controls, procurement standards procedures for determining costs, property management standards, acceptance of audit applicability, programmatic and financial reporting requirements, and record-keeping requirements.

Eligible Applicants:

- Town/Cities/Municipality
- Borough
- Tribes
- Public Educational Institutions

Ineligible Applicants:

- Non-profit organizations
- For-profit organizations

If, in review with successful applicants, it is determined that a jurisdiction may have difficulty meeting the subrecipient requirements of 2 CFR Part 200, a state-managed award may be available. This will be determined through discussion with jurisdictions after award notifications are made.

If you feel your jurisdiction needs help meeting any of the grant requirements, please get in touch with DHS&EM for state-managed grant options.

Funding Priorities

For the FY2022/2023 SLCGP, the State of Alaska has established the following priorities:

1. Cybersecurity Risk Assessment
2. Enhancing cybersecurity resilience and interoperability.
3. Foster a cybersecurity culture.
4. Enhance cybersecurity collaboration and partnerships.
5. Improve cybersecurity incident management and response capabilities.

Requested projects must align with at least one of the above-listed priorities.

NOTE: If you intend to apply for this funding opportunity and **still need to register** in the System for Award Management (SAM), please take immediate action to register in SAM. It may take four (4) weeks or more after you submit your SAM registration before your registration is active in SAM.

Project Eligibility

No more than four (4) projects will be allowed. Project applications can contain planning, equipment, training, or exercise activity based on gaps, capability targets, and improvement areas identified through the applicant's cybersecurity risk assessment. Approved projects will be expected to begin within 90 days of the grant award date.

Other Eligibility Requirements:

Cybersecurity Risk Assessment: Applicant must have a completed cybersecurity risk assessment or request funds to do an assessment. The requested projects must align with closing gaps and/or strengthening capabilities in the agency's cybersecurity risk assessment.

Management and Administration (M&A): The state prohibits jurisdictions from using funds for M&A.

SLCGP Objectives:
The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. This goal can be achieved over the four years of SLCGP funding as applicants focus their Cybersecurity Plans, priorities, projects, and implementation toward addressing the SLCGP objectives. Once CISA confirms that a recipient has met their objective requirements for each fiscal year, the recipient moves to the next set of program objective(s).

In FY 2022, applicants are required to focus on addressing the following program objectives in their applications:

- Objective 1: Develop and establish appropriate governance structures, including by developing, implementing, or revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

In FY 2023, applicants are required to focus on addressing the following program objectives in their applications:

• Objective 1 can still be funded under FY2023. The applicant must meet Objective 1 before they can be awarded funds for Objectives 2-4.

• Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

• Objective 3: Implement security protections commensurate with risk.

• Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Allowable Costs and Activities

Requested projects must strengthen state and local cybersecurity preparedness by focusing on cybersecurity measures to help manage state and local risk and enhance Alaska's cybersecurity position.

The requested project **MUST:**

- Close gaps and strengthen capabilities identified in the applicants' cybersecurity risk assessment.
- Align with the Alaska Cybersecurity Plan
- Align with at least one FY2022 SLCGP the State of Alaska priorities.

Below is not an all-inclusive list. Please review the FY2023 SLCGP Notice of Funding Opportunity for additional information.

Planning:

Planning costs are allowable under this grant. Funds may be used to plan activities supporting the SLCGP priorities, Alaska Cybersecurity Plan, closing gaps and strengthening capabilities in the applicant's cybersecurity risk assessment.

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).

Training:

Training costs are allowable under this grant. 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 eligible entity's 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 that may be more impacted by disasters, including 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, should be identified in an assessment and addressed in the eligible entity's training cycle. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

Recipients are also encouraged to utilize FEMA's National Preparedness Course Catalog. Training includes programs or courses developed for and delivered by institutions and organizations funded by FEMA. This consists of the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners.
The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope and the increasing training needs of federal, state, local, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov.
Some training activities require an Environmental and Historic Preservation (EHP) Review, including exercises, drills, or training that require any land, water, vegetation disturbance, or building of temporary structures or not located at facilities designed to conduct training and exercises. Additional training requirements and EHP review information can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Exercise:

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and run consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Some exercise activities require EHP review, including exercises, drills, or training that require any land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional training requirements and EHP review information can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Equipment:

Equipment costs are allowable under this grant. 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 SLT governments.

Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List | FEMA.gov. In addition, recipients 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 (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

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 also extends to licenses and user fees.

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

Prohibitions on Expending 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 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. 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:

a. 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.

b. 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

c. 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.

Replacement Equipment and Services

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the NOFO and the Preparedness Grants Manual requirements.

DEFINITIONS

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:
i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
iii. Telecommunications or video surveillance services provided by such entities or using such equipment or
iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.
Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." *See* 2 C.F.R. § 200.471.

Unallowable Costs and Activities

Below is not an all-inclusive list. Please review the FY2023 SLCGP Notice of Funding Opportunity for additional information.

Grant and match funds cannot be used for:

- Spyware
- Microsoft Office
- Construction/Renovation
- To meet a cost-sharing contribution
- To pay a ransom
- For recreational or social purposes
- To pay for cybersecurity insurance premiums

- To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities or
- 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.
- Salaries and personnel costs of planners, equipment managers, exercise coordinators, and/or training coordinators
- Supplanting any expense already budgeted
- Reimbursable training and related travel costs not pre-approved by DHS&EM
- Contracts and procurements over $10,000.01 not pre-approved by DHS&EM
- Sole source contracts and procurements not pre-approved by DHS&EM
- Stand-alone working meals
- Expenditures not supported with appropriate documentation when submitted for reimbursement. Only properly documented expenditures will be processed for payment. Unsupported expenditures will be returned for resubmission by the jurisdiction.
- Drawdown of funds prior to expenditure*

*Reimbursement advances with strict guidelines can be requested from DHS&EM

Application and Submission Information:

1. Dates

Application Open date: February 13, 2024

Application Submission date and time: March 29, 2024, at 11:59 pm

2. Agreeing to the Program Terms and Conditions of the Award

By submitting an application, the applicant agrees to comply with the requirements of the SLCGP NOFO and the program's terms and conditions of the award, should the applicant receive an award.

Applications will only be accepted by emailing them to mva.grants@alaska.gov

3. Application Forms and Required Documents

As part of the FY2022/2023 SLCGP application, each eligible applicant must complete all application forms and provide all required documents:

1) Application Coversheet
2) Project Application Form
3) Signatory Authority Form
    a. A signature is required for the Primary Project Manager, Primary Chief Financial Officer, and Primary Signatory Official. We highly recommend that
4) Print-out of jurisdiction's www.SAM.gov Entity Overview record displaying the jurisdiction's UEI Number
5) If applicable, any Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) related to inter-agency projects.

Four (4) project applications are allowed. **There may only be a single project per application form.** To qualify as a single project, the pieces of the project must be integral toward achieving one objective.

Some examples of one project include:

- Requesting a Cybersecurity Assessment
- Creating or revising Cybersecurity Plan
- Creating or revising IT & Cybersecurity Policies
- Creating or revising the cyber portion of the Disaster Recovery Plan

Combining any of the above projects into one cybersecurity project application is considered a multi-project and will be disqualified.

The SLCGP Application Form, Application Coversheet, and Signatory Authority Form can be found at DHS&EM | State and Local Cybersecurity Grant Program (SLCGP) (alaska.gov)

Applicants must familiarize themselves with the requirements and restrictions of the FY2022 and 2023 SLCGP Notice of Funding Opportunity, when available, the FY2022 and 2023 SLCGP Notice of Funding Opportunity, 2 CFR Part 200, which governs this 2022and 2023 award.

All successful grant subrecipients are assumed to have read, understood, have accepted, and will comply with this State Overview, the SLCGP Program Guidance, 2 CFR Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, and the jurisdiction's Obligating Award terms.

SUBMITTING THE SLCGP PROGRAM APPLICATION PACKAGE

DHS&EM must receive applications
by 11:59 p.m., Friday, March 29, 2024.

Applications must be submitted electronically in PDF format with complete signatures to the DHS&EM grants email at
mva.grants@alaska.gov

Project Review and Selection Process

DHS&EM will review application submissions to determine application completeness and eligibility based on adherence to the state and federal program guidance. If applicable, DHS&EM will also review a jurisdiction's previous performance history (risk assessment).

The project applications will be reviewed for project relevance to the jurisdiction's Cybersecurity Risk Assessment, adherence to state and federal program guidance, feasibility, how well the proposed project is outlined, sustainability, impact, and demonstration of ready-to-go projects.

Project comprehensiveness is based on the following:
Eligibility for the award is dependent upon accuracy and completeness. Incomplete applications and/or individual projects will be disqualified.

- Project descriptions supporting the project need
- Project descriptions addressing the need/gap for the applicant
- Project descriptions describing how it has a multi-jurisdictional or statewide benefit
- Budget justification, AEL #'s, and/or budget categories
- Demonstration of projects "ready-to-go" and begin implementation within 90 days of the grant award date

Jurisdiction performance history is based on the following:

- Prior project initiation per Grant Agreements
- Any prior project cancellation due to inability to complete without justification
- On-time Quarterly Reporting
- Activity towards project completion being shown on each Quarterly Report
- Ability to meet any prior Award Grant Requirements, Assurances, and Agreements or Special Conditions
- Timeliness of award extension requests
- Timeliness of de-obligation requests
- Results of on-site monitoring reviews
- Compliance with procurement and contracting requirements
- Compliance with property management system and reporting requirements
- Prior audit findings

Eligible project(s) are then forwarded to the Cybersecurity Planning Committee—representatives knowledgeable in the field who are independent of the DHS&EM review applications so that objectivity is maintained. Members of the committee are professional equals of applicants, and their evaluation results in a credible and independent assessment and informed judgment of project feasibility, capability, and need while considering local, regional, and State assets and resources. This committee recommends the final project approvals and funding allocations.

Additional Award and Program Information

If you feel your jurisdiction needs help meeting any of the requirements below, please contact DHS&EM for state-managed grant options.

If your jurisdiction is successful in receiving an award, the following are required:

- Subrecipients must be registered with www.SAM.gov and have a UEI number. If you have questions regarding this requirement, contact the Grants Section.
- Subrecipients must ensure and maintain the adoption and implementation of the National Incident Management System (NIMS). Subrecipients will certify NIMS compliance through the Alaska Assessment
- Subrecipients must complete an Environmental and Historic Preservation (EHP) review on any ground-disturbing activities, communication towers, or modification/renovation of existing buildings or structures. Additional information on EHP Reviews can be found below.
- Subrecipients must have a fiscal and programmatic jurisdictional representative attend the 2022/2023 SLCGP Grant Award Kick-off meeting in Summer 2024.
- Subrecipients must follow procurement processes and documentation requirements
- Subrecipients must complete an annual inventory review of grant-funded equipment, if applicable.

All recipients and subrecipients of the Statewide Alaska Cybersecurity Grant Program (SLCGP) are required to participate in the following free services provided by the Cybersecurity and Infrastructure Security Agency (CISA). Please note that participation in these services is not mandatory for grant submission and approval but is a post-award requirement.

REQUIRED SERVICES AND MEMBERSHIPS

Cyber Hygiene Services:

- **Web Application Scanning:** A service that assesses the health of publicly accessible web applications, identifies vulnerabilities, and recommends security enhancements.
- **Vulnerability Scanning:** Continuous scanning of public, static IPs for accessible services and vulnerabilities, providing weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP." In the body of your email, mention that you are requesting these services as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR):
The NCSR is an annual self-assessment that measures the gaps and capabilities of cybersecurity programs of state, local, and tribal (SLT) entities. It is based on the National Institute of Standards and Technology Cybersecurity Framework and sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Entities and subrecipients should complete the NCSR annually.
For more information, visit the Nationwide Cybersecurity Review (NCSR) website (cisecurity.org).

Reporting: Each subrecipient must report quarterly progress in Performance Progress Reports on the timelines, milestones, and related project activities. This information is captured

as a statewide report used to assess overall program effectiveness and impact and to report results to Congress.

Quarterly Performance and Financial Progress Reports are required by the 20th of the month following each calendar quarter. Narrative Reports must describe, clarify, and support the expenditures submitted in the Financial Report for reimbursement. SLCGP Report forms are available on the DHS&EM website at DHS&EM | State and Local Cybersecurity Grant Program (SLCGP) (alaska.gov) and are updated as needed or required. Instructions and compliance information are included on the back of both report forms. Jurisdictions are encouraged to use the updated forms from the website each quarter to ensure the most updated information is used. Use of incorrect or outdated forms will be returned and cause payment reimbursement delays.

Each quarterly report should show activity toward the completion of grant-funded projects. Failure to do so may result in the de-obligation of funds. A Final Performance Progress Report is required within 45 days after the end of the performance period. It summarizes all project accomplishments, achievements, impacts, challenges, unmet goals, and the reasons why, etc., throughout the entire grant award period. The Final Performance Progress Report does not replace the last Quarterly Performance Progress Report. More information on final reporting can be found on the DHS&EM website.

Environmental and Historic Preservation Compliance: All SLCGP projects that may have a potential impact on the environment require a FEMA Environmental and Historic Preservation (EHP) review per the Grant Programs Directorate (GPD) Programmatic Environmental Assessment (PEA). Ground-disturbing activities, new construction, including communication towers, or modification/renovation of existing buildings or structures must undergo a FEMA EHP review. For more information on the PEA, see FEMA Information Bulletin (IB) 345 www.fema.gov/grants/preparedness/about/informational-bulletins and www.fema.gov/pdf/government/grant/bulletins/fonsi.pdf

Furthermore, for those proposed construction or renovation projects that are part of larger projects funded from a non-FEMA source (such as an Emergency Operations Center that is part of a larger proposed public safety complex), a FEMA EHP review must be completed before the larger project is initiated. For these types of projects, recipients must complete the FEMA EHP Screening Form (Office and Management and Budget (OMB) Number 1660-0115/FEMA Form 024-0-1) and submit it, with all supporting documentation, to DHS&EM for review. Recipients should submit each project's FEMA EHP Screening Form as soon as possible upon receiving the grant award. If a jurisdiction is aware a project will require an EHP review, they may submit the Screening Form at the time of application.

The following activities would not require the submission of the FEMA EHP Screening Form: planning and development of policies or processes; management, administrative, or personnel actions; classroom-based training; tabletop exercises; and acquisition of mobile and portable equipment (not involving installation). While an EHP Screening Form may not be required, an EHP Statement of Work may be required for the items above, especially training, exercise, and mobile/portable equipment. The state reserves the authority to request a review on any approved projects that could potentially fall closely out of these areas.

For more information on FEMA's EHP requirements, grant recipients should refer to DHS&EM's webpage at DHS&EM | Grants Section Documents (alaska.gov). Additional information and resources can also be found in FEMA Policy 108-023-1, located at https://www.fema.gov/grants/tools/environmental-historic/preparation-resources.

Subrecipient Monitoring: Jurisdictions will be monitored by DHS&EM to ensure that project goals, objectives, timeliness, budgets, and other related program criteria are being met. Monitoring will be accomplished through a combination of office-based and on-site monitoring visits. DHS&EM is responsible for providing assurance to FEMA that awards are compliant with federal and state requirements, including but not limited to the accomplishment of project goals, accounting of receipts and expenditures, cash management, maintenance of adequate financial records, and the refunding of expenditures disallowed by audits.

Pass-Through Requirements: The state shall pass-through 80 percent of the total SLCGP funding available to local units of government within 45 days of the receipt of its state award.

Memorandum of Understanding Requirements/State-Managed Awards: The State may retain part of the pass-through funding for expenditures made by the State on behalf of the jurisdiction or for a statewide benefit. The state and jurisdiction must enter into a formal Memorandum of Understanding (MOU) specifying the amount of funds to be retained by the state and the intended use of funds. The amount will be considered as part of the 80 percent pass-through requirement.

For example, through an MOU, a jurisdiction's specified funds for equipment could remain with the state. The state would purchase equipment through the state procurement process on behalf of the jurisdiction, pay for the equipment, and turn over the equipment to the jurisdiction upon receipt. This is often helpful if local procurement policies prevent the use of a state procurement contract or if state assistance is needed to comply with timelines or award deadlines. This would be a state-managed award.