**QUESTIONS ON STATE & LOCAL CYBERSECURITY GRANT PROGRAM:**

Q: Where a state wishes to pass through items, services, capabilities, or activities to local governments in lieu of funding in order to meet part or all of its 80% pass-through requirement, how may a state go about obtaining consent from the local government as required by the SLCGP NOFO?
A: Local governments can either consent or opt out of the "in lieu of" services. How consent is obtained is up to the state or territory, but consent must be obtained in writing for all entities in which the state will provide an item, service, capability and/or activity in lieu of direct funding. Additional information on this process can be found in Section F, Federal Award Administration of the SLCGP Notice of Funding Opportunity.

Q: Must **all** local governments provide consent for the state to provide items, services, products, capabilities or activities in lieu of funding?
A: No. It is not a requirement for all local units governments to provide consent. The state can still provide that item/service/capability/activity in lieu of funding to those local units of government that do consent. It is not an all-or-nothing requirement.

Q: Can the Cybersecurity Planning Committee be used as the sole source of consent on behalf of local governments to accept "in lieu of" services?
A: No. While an association or council of local governments can provide consent on behalf of its members (if the local government has specifically authorized the association or council to do so in writing), consent must still be obtained from the appropriate local governments. Permitting a council or association of local governments to act in this role is at the discretion of the state.

Q: The SLCGP NOFO has several references to the Chief Information Officer (CIO), Chief Information Security Office (CISO), or an "equivalent" official. What is meant by "equivalent?" Who else might be that equivalent official?
A: An equivalent official is the executive responsible for the state or territory's information technology and information/data security. The term "equivalent" allows for flexibility so that states or territories may use individuals that have different titles or have broader responsibilities (e.g., a Chief Risk Officer or a Chief Technology Officer).

Q: Do states or territories have to use the template provided for the Cybersecurity Plan in the SLSGP NOFO or can states or territories use their own template if the elements are covered?
A: The template is not required, but **strongly** recommended. If a state or territory uses its own format, the Cybersecurity Plan must include all the required elements. CISA will work with states and territories to ensure inclusion of all required elements in their plans.

Q: Will there be an extension process available for states or territories that will not be able to meet the November 15, 2022, application submission deadline?
A: As stated in the SLCGP funding notice, DHS will generally not review applications that are received after the deadline. However, DHS may extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause

for an extension may include technical problems outside of the applicant's control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for DHS to make an award. See Section D of the funding notice for more information.

Q: Can states/territories require that local governments complete a cybersecurity risk self-assessment to get a better understanding of the risks throughout the state?
A: An assessment of the current capabilities of state, local and territorial entities is a required component of the Cybersecurity Plan and should serve as the justification for individual projects. Regular assessments, testing and evaluation to understand risks are an objective of the grant program. Planning committees are encouraged to consider existing assessments and evaluations conducted by SLT governments and any planning gaps that require additional assessments and/or evaluations as they create their plans. As a post-award requirement, states/territories and their subrecipients must complete the Nationwide Cybersecurity Review, administered by the Multi-State Information Sharing and Analysis Center, during the first year of the award/subaward period of performance and annually.

Q: The SLCGP funding notice requires the submission of an "initial application" and then a "final application." What's the difference?
A: All FEMA preparedness grant applications must be initially submitted in Grants.gov, and then migrated to FEMA's Non-Disaster (ND Grants) system for final submission. The initial application is submitted by the State Administrative Agency (SAA) through Grants.gov. After processing, the initial application is automatically transferred to FEMA's ND Grants System. The SAA does not need to re-apply in ND Grants. Once complete, FEMA will notify the SAA that the application is ready for final submission in ND Grants (the second portion of the application process).

Q: Are the funding amounts listed in the funding notice the amount we should expect for the entirety of the grant?
A: The funding amounts in the NOFO are for FY 2022 only, with a 48-month period of performance ("Year 1"). Updated allocation amounts can be found in Information Bulletin (IB) 479. Funding will be available in FY 2023, FY 2024 and FY 2025. Each FY will have its own funding notice, allocation amounts, and application period.

Q: If local governments are not required to participate in the Cybersecurity Planning Committee, can they still receive SLCGP funding?
A: Yes. Appendix B of the FY 2022 SLCGP NOFO outlines the entities that are required or encouraged to be members of the Cybersecurity Planning Committee. As not every local government is required to be a member, the Committee develops the Cybersecurity Plan, which would drive the investment decisions across the state including at the local levels in terms of projects and priorities.

Q: Do states or territories have to receive all local government requests for funding by the application deadline of November 15, 2022?
A: No. Any projects at the local level that will be funded out of FY 2022 SLCGP funds would have to be a part of the Cybersecurity Plan, which does not have to be final by November 15. For those states or territories that do not submit a Cybersecurity Plan with their application, they will need to

submit it no later than September 30, 2023, and it should also include all relevant local government projects that are prioritized for funding under the FY 2022 SLCGP award.

Q: Is there a deadline for a state or territory's Cybersecurity Plan? Or can the whole first year be used to write the plan, including conducting evaluations and assessments to help support Plan development?
A: States and territories must submit Cybersecurity Plans for review and approval as part of the grant application. If the state or territory is applying for grant funds to develop a Cybersecurity Plan, the plan is not required to be submitted as part of the FY 2022 application. The deadline for Cybersecurity Plan submission is September 30, 2023.

Q: If states or territories submit their Cybersecurity Plan before September 30, 2023, will CISA and FEMA review it and approve it before the deadline, or will it not be reviewed until after the deadline?
A: Plans will be reviewed and approved as they are received, and before the deadline if received before the deadline. The goal is to review and approve Cybersecurity Plans as soon as practical after submission so that the recipients can begin implementing approved projects as soon as possible at the time they are submitted.

Q: Are public school districts and local government public health agencies restricted to Cybersecurity Planning Committee roles only, or can they also be subrecipients of SLCGP funding?
A: Yes, public school districts and public health agencies are local governments under the definition. Page 10 of the funding notice provides a definition of a local government, which includes school districts and agencies or instrumentalities of a local government.

Q: Is there a form to request a waiver for entities that are unable to meet the cost share requirement?
A: Appendix H of the SLCGP funding notice defines the criteria, requirements and process for the Economic Hardship Cost Share Waiver. Waiver requests should be submitted in the form of a written narrative and other supporting documents, as outlined in Appendix H of the funding notice.

Q: Is the 5% of the funding that states/territories are allowed to retain for management and administration (M&A) activities calculated against the total federal grant award, or the 20% portion the state is permitted to retain?
A: The state/territory may retain 5% of the *total federal grant award* for M&A activities. However, it also counts as part of the 20% they may retain and is not in addition to the 20%.

Q: Can the state or territory's non-federal cost share be fulfilled by leveraging ***already budgeted*** state cybersecurity funding vs. the state or territory being required to budget for ***new*** cybersecurity funding, which may not be possible for states on a multi-year budget cycle?
A: In general, previously budgeted-for funding can be used if:

1. The funds were expended within the grant period of performance;
2. They are for allowable uses of funds under the grant program;

3. Federal dollars are not used as a source of the matching funds (unless authorized by the source of the other federal funding); and
4. The expenditures comply with the applicable terms and conditions of the grant award, including that the expenditures do not violate state procurement policies.

States or territories may request a waiver of the cost share requirement where they can demonstrate economic hardship. Please see Appendix H of the funding notice for more information.

Q: Can the state or territory provide the funding for the non-federal cost share for the entire grant award?
A: The federal share of each "activity" carried out with an SLCGP grant award cannot exceed the percentage identified in the grant award, which will be 90% in FY 2022. Where the activity is carried out by a local government subrecipient, the non-federal cost share can be met by the local government expending its own funds to carry out at least 10% of the amount of the grant-funded activity, or the non-federal cost match share could be met by the state contributing its own funds to carry out at least 10% of the amount of the grant-funded activity.

Q: If an activity or project is performed by the state or territory but for the benefit of the local governments (i.e., a whole of state solution) can the state or territory pay for the entire non-federal cost share of that activity or project?
A: Yes.

Q: Can a state/territory place additional requirements on local units of government as a condition of receiving pass-through funds (e.g., require that a local government share alerts with the state/territory if grant funding is used to provide that alert function)?
A: Per the funding notice, the eligible entity's pass-through commitment must be unconditional (i.e., no contingencies for the availability of state funds). As such, requiring a local unit of government to share alerts could be viewed as a "contingency." However, if the state uses its 20% on this, then it could put those contingencies on as that funding is not part of the required pass-through funds.

Q: Is it possible to have a multi-entity project using a mix of SLCGP and Tribal CGP (TCGP) monies?
A: In theory, portions of a large project could be funded with both SLCGP and TCGP funding. However, because the TCGP funding notice has not yet been announced, a SLCGP recipient's cybersecurity plan and proposed FY 22 budget cannot presume it would receive TCGP funding, and thus the plan and budget must be complete without including TCGP funding. However, the TCGP NOFO has not been issued, and SLCGP awards will be made before TCGP awards are made so there is no guarantee for the FY 2022 cycle that a certain Tribe would receive TCGP funding for a certain project.

Q: Do states/territories have to use the existing SAAs or can they establish a new SAA for purposes of this grant program?
A: The state's governor designates the SAA. The governors have already identified SAAs for the Homeland Security Grant Program which can be used as the SAAs for the SLCGP. However, if a state or territory wishes to change who the SAA is for the purpose of the SLCGP, they would need a letter from

the governor (letter should contain the state seal) which designates the new agent/agency. That letter would have to be uploaded into ND Grants.