To: The Cybersecurity and Infrastructure Security Agency & The Federal Emergency Management Agency
From: State Associations Coalition
RE: Questions for Consideration in Development of Guidance for the State & Local Cybersecurity Grant Program

On November 15, 2021, President Biden signed into law the Infrastructure Investment and Jobs Act (IIJA). The measure includes a critical priority for states and territories, a $1 billion cybersecurity grant program designed to help state, local, tribal and territorial entities improve their cyber posture as well as address cybersecurity threats and risks to their IT systems.

In order to effectively inform the guidance development process at the federal level, our collective associations solicited our memberships for both questions and recommendations for implementing the grant program. This information can be found starting on the next page of this memo.

Bottom Line: We believe that FEMA and CISA should provide as much flexibility as possible in implementing this new grant program. States have taken significant strides to leverage existing federal funding to enhance and secure their cyber postures. This established grant program should avoid constraints and new requirements that would hinder existing programs and initiatives as well as new innovated approaches

We also encourage CISA and FEMA to continue routine consultation process through the guidance formulation and implementation to ensure that stakeholder perspectives are accounted for.

We look forward to working with you in partnership to effectively utilize this new grant program to further these important efforts across the country.

RECOMMENDATIONS

Who will manage the funds at the state level?

- Given the existing infrastructure, expertise available, and ability to complement existing federal grant programs, the funds should be managed by the current State Administrative Agency (SAA) with programmatic direction given to the State CIO.

What items can the funding be used for – equipment, software, training? CISA/FEMA should consider the following as potential allowable uses of funds. Recommended List Generated by States

- Protection: Email security; network security (LAN/WAN/Internet/Remote Access, IPS, IDs, and web application security); identity (MFA and Access Control); EDR; data security/backup/encryption; security education; vulnerability management (system updates and patching); DotGov
- Identification: Assessments
- Detection and response: recovery; statewide SOC; incident response; and security monitoring
- Other Items: cooperative contracts; governance and oversight; project management; and workforce

Will the Homeland Security Grant Program cyber carve out still exist?

- With the newfound directed funding on cybersecurity, FEMA should consider the phase out of existing carve-outs for State Homeland Security Grant Program (SHSGP) but allow the flexibility to use this program for cybersecurity initiatives. The two programs should continue to work in harmony with one another to demonstrate effectiveness and results-based outcomes.

Does a planning committee need to be created specifically for the purpose of developing the cybersecurity plan?

- The program should afford flexibility in interpreting this requirement and should expressly state that a separate committee and cybersecurity plan need not be created where a state has already created a committee and/or has an existing cybersecurity plan.

Will there be any training or additional funding for compliance and grant management?

- CISA/FEMA should work to utilize existing cyber-learning capabilities such as those in the National Domestic Preparedness Consortium, the convening power of the Center for Homeland Defense and Security, or other federal assets such as the United States Secret Service and the Hoover Center to integrate state and local training and executive education opportunities and diversify opportunities wherever possible. These federal assets must be combined with a dedicated, recurring, and substantial federal outreach effort to stakeholders through their national associations to ensure receipt of these training and funding resources.

STATE QUESTIONS FOR CONSIDERATION

Interpretation of Statute

- Will the SAA provide financial management as with other FEMA grants or would CIO/CISO offices now be managing these funds separately?
- With the federal share of funds being reduced by 10% each year, is attainment of other funding mechanisms a requirement for grant approval?
- Does state-level management of grant funds that benefit a local entity preclude that entity from seeking grant funds directly?
- Is there any intention to continue this program past 2025?
- Has the allocation formula been determined? If not, what is the timeline for this? And will it be publicly available to affected stakeholders?
    - Will FEMA decide? Baseline amount is .25% of such amounts to each of the territories.
- Please clarify how funds can and should be passed through from state to local entities and who will be ultimately responsible for management of local funds, the federal government, states, or locals?
- Will Environmental and Historical Preservation (EHP) requirements be applicable for this award?
- For state-level management of grant funds, do funding allocations need to be specified in the Cybersecurity Plan?
- How much is allocated to state government for internal state projects and how much for local entities within the state? Is that 20/80?
- How does the funding flow from federal to state to local/tribal?
    - Does the state administer individual grants to local entities?
    - Is tribal allocation separate from state?
- How is "rural" defined? County level? Municipality level? Regional?
- Are municipal owned utilities in scope as a local government entity?
- Are K-12 school districts in scope for the funding?
- Are state and local government entities required to adopt the NIST Framework? (vs. adopting other frameworks like the CIS Controls Framework).
- Can states create rules for the funds that are more directive or restrictive than the federal guidelines?
- If funds are distributed through State Administering Agencies, but state CIOs/CISOs are directing funding, and there is a 5% cap on administrative funds – is that limit applied to the combined efforts of CIOs/SAAs? This leads to potentially even less administrative costs for each entity, particularly when 80 percent of funds must be sent outside of state government.
- Can the 80 percent passthrough be in the form of services/solutions procured, managed, and deployed by the state in coordination with the local government benefited?
- Can expenses be planned for forward years or is the annual application process run a risk of reduces competitive allocation in future years?

- Can private businesses such as nuclear power companies that provide funding to the state contribute the required cash match? In general, the number of grants with required matches continues to grow. What can be done to increase the number of funding sources that might be used as a match?
- We need specific categories of eligible expenses (assume will be issued with grant guidance as it is for HSGP/UASI). For instance, we have already shared cyber navigator program operating centrally for the benefit of locals. But what about replacing unsupported servers or operating systems, for instance? Those create significant vulnerability, would that qualify? Are salaries eligible; training costs, travel, etc.?
- The Act says CIOs and CISOs must be consulted, but it would be helpful to get a more concrete description of what that means (appears the application for grant funds may be submitted separate and prior to a plan being submitted – i.e., funds can be used to develop the plan)
- Could federal guidance allow for the grant to flow through the state's main federal funds recipient, specifically in states with a federated structure?
- Could federal guidance reduce the number of requirements and restrictions required in the plan and implementation to allow states, and the subsequent local governments, the freedom to tailor the proposals to their needs? Also, are the requirements only imposed on the state funds, or also on local funds?
- Are local grants competitive?
- Who will manage and award local grants – CISA or the state?
- If the state is to award local grant dollars, it is imperative that states have the flexibility to craft local grant requirements to ensure proper use of funds and capabilities.
- How will the rural grant dollars be allocated? By the state or by CISA and will this be a competitive process?

Applicability of Funds and Timing of the Notice of Funding Opportunity

- Can we hire qualified IT/cybersecurity personnel and purchase equipment, software, and training?
- Can the funding be used to supplement staffing costs? As required in § 14.106. Division of Cybersecurity and Critical Infrastructure?
- How will this grant work alongside the Homeland Security Grant Program cyber funds? Will both be run concurrently, or will they be staggered timing wise? Can HSGP funds be used to extend an effort or program funded through IIJA cyber grants?
- Local jurisdictions commonly lack the personnel resources to operationalize security measures. Could the 80 percent passthrough to locals be used to sustain personnel, or professional services to operationalize security defenses? If localities use state personnel and resources, can part of their 80 percent be charged back to the state?
- Can the 80 percent allocation intended to benefit local jurisdictions be used to build centralized security services at the State level with the sole intended purpose to serve local jurisdictions? (For example, Vulnerability Assessments

provided by the State, or Security Operations Services/Tools/Processes operated at the State for the benefit of the local jurisdiction networks).

- Other than the 25 percent allocation to rural areas, are there any minimum funding requirements (e.g., HSGP has a minimum 25 percent allocation towards law enforcement terrorism prevention activities)?
- Confirm that the limitation on construction does not include installation of equipment (e.g., installation of fiber optics in a wall or ground).
- Can grant funds be applied to existing state-level projects, such as the California Cybersecurity Integration Center?
- Are funds used to "develop or revise the Cybersecurity Plan" considered "expenses directly relating to the administration of the grant" and thus subject to the 5 percent limit?
- Can funds be applied to existing state-level programs that directly benefit local entities and be counted in the local allocation, or must those funds go directly to local entities?
- Can the funding be used for consulting engagements?
- Can the funding be used for professional services?
- Can the state contract for services on behalf of local entities? For example, the state pays a vendor to provide assessment and planning services and then make those services available directly to local entities.
- Does this grant expect the state to provide the cash match on behalf of local jurisdictions or can the state choose to require local jurisdictions to provide their own cash match?
- The statute authorizing the grant says the Secretary can waive or modify the match requirement for any entity or multi-entity group that can demonstrate economic hardship. Why is the potential match waiver only being offered to multi-entity groups, based on information on the grant provided so far?
- What items can the funding be used for – equipment, software, training?
- Can grant funding be used to develop the State Cybersecurity Plan, and be considered as pre-award costs?
- If there are unspent dollars at the end of the annual cycle, due to unforeseen delays, can the money be rolled over and combined with the following year grant, but still target initial spend items?
- Do partnerships arrangements need to be at the state level, or can tribal regions, for example, across state boundaries build partnership to qualify?
- Can the funds be used to procure subscriptions or services that are provided to local governments in scope? Is there any restriction on the subscription terms (e.g. do they have to be fully consumed within the grant year, or can software be licensed for longer terms within a single grant term)?
- Can funds be used to stand up a service at the state level that serves all local/tribal entities, such as a statewide SOC?
- If statewide services are a permissible use of funds available to locals, is there a threshold or quota of consuming customers that must be met (i.e. 50 percent of customers must be locals? 30%?)
- For the share of money which is made available to states under this program, are there any restrictions on the types of goods/services that can be procured using these funds? Or do they just need to be included in the approved cybersecurity plan?

- Can the funding be used for staff for local government relationships/support?
- Can these funds be used to replace a stand-along EDR solution with a managed EDR solution (e.g., local instances of Crowdstrike that are managed by local staff with MS-ISAC Crowdstrike offering)?
- If so, can the state require visibility into solution findings (e.g., scans, alerts) as a condition of providing services to locals?
- Can CISA provide states with a sample plan that would meet their requirements?
- Will CISA provide the states with the actual amounts to be allocated to local governments and rural areas?
- What is the process if a state's plan is not approved?
- Do state(s) receive 100 percent of the grant funds 45 days after enactment of the IIJA (which would be Dec. 30, 2021), or do states get all of this funding earlier or later, such as when the planning committee is established or when the cybersecurity plan(s) are ultimately approved?
    - If this date is correct, that would mean that the state(s) would be required to make available 80% of these funds to locals by Dec. 30, 2021, as well – is this correct?
- What percentage of grant funds will be made available to the state(s) before or after the planning committees in each state(s) are established – is it 100 percent, 20 percent, nothing?
    - Is there a deadline on when these new planning committees in each state(s) need to be established by?
- Does the 45-day clock for disbursement of grant funds by the state(s) to locals happen only <u>after</u> their cybersecurity plan(s), which will be put together by the new planning committees, are approved by the federal government?

    - Is there a deadline in terms of when planning committees in each state(s) have to finalize their cybersecurity plan(s) by and turned in to be looked at for federal approval?

<u>Guidance and Grant Performance Evaluation</u>

- Is there guidance for the potential on multi-state grant projects?
- Any special guidance for combining grants?
- Will CISA/FEMA grant guidance timing align with the Homeland Security Grant Program (HGSP) timeline? If not, please clarify what the separate timeline will be.
- Will there be more guidance provided for states entering into partnering arrangements with local / tribal governments and/or multi-state groups? When will such guidance be available?
- Will there be federal personnel assigned to assist recipients with federal guidance for the program? If so, when can we expect the assignment to take place?

- Has FEMA considered using local or statewide NSCR results for guidance and progress measurement? Can this data be made available to states for planning and evaluation purposes?
- Will the grant include a requirement for all recipients and subrecipients to complete the annual NCSR, similar to the HSGP?
- Will the grant-funded projects be required to be tied to the THIRA/SPR?
- Will there be additional reporting requirements beside the annual report? If so, at what frequency and in which federal system(s)?
- Will in-person or virtual meetings be required for grantees?
- Can pre-existing state/local arrangements such as multi-jurisdictional working groups or committees be enhanced to include enhanced cyber security initiatives?
- Will CISA provide more guidance on development of the cybersecurity plan - e.g., required vs. recommended elements/templates.
- When are the funds expected to be made available and how long will we have to spend them?

Cybersecurity Plan & Planning Committees

- What are the explicit membership requirements from the planning committee? How will we ensure a variety of representation from IT, security, public safety, and emergency management?
- Does the planning committee play any role in subject matter expert (SME) reviews for the grants, or will that be a part of the process at all? Will the state offices for CIO's/CISO's be the sole advisors for determining allocation of funds?
- The requirement for submission of a cybersecurity plan only rests upon the state, but why not the localities as well?
- If a state already has an effective and robust cyber plan in place, what additional purpose does the plan committee serve other than determination of funding priorities?
- Can it be utilized to upgrade an existing plan?
- Planning committees will assist with the determination of effective funding priorities. Are there any required national level priority requirements?
- Will use of existing state-level organizations as the planning committee commit that state-level organization to any other obligations beside administration of grant funds in accordance with the Cybersecurity Plan?
- How do state CIO/CISOs formally designate planning committees for purposes of developing the Cybersecurity Plan?
- How is "professional experience relating to cybersecurity or information technology" defined for the purposes of committee membership qualification? Can the same planning committee designated for state-level awards be used for multi-state grants?
- Can 5 percent overhead funds be used to support plan development and planning committee?
- Will additional guidance be provided on plan development?
- When does the planning committee need to be established by?

- What is the deadline for submitting the plan?
- Will FEMA or CISA provide a template, or at a minimum a planning checklist, to ensure plans contain all required elements?
- Are planning committees expected to identify local, county, and tribal distribution of state allocated funds to meet grant requirements?
- What flexibility will there be in interpreting this requirement when a state has a long-standing cybersecurity committee and existing cyber security plans? Will it be sufficient for that committee to review the existing plan and make any revisions necessary to meet the grant requirements?
- Inevitably many people will find after the first year that items that were proposed are not working out, or other things have changed that would require plans to be updated. What's the process to change or update plans and have these reviewed and approved?
- How large does local/county/tribal government participation on the planning committee need to be? WA has a Technology Services Board which has one local government representative on it (we likely won't be able to leverage this for other reasons) but curious how much representation these groups need on the planning committee since the lion's share of funding goes to locals.
- In a similar vein, how large does the planning committee need to be?
- Is there guidance as to specific elements or time periods the cybersecurity plan must cover?
- Is there a preferred format for the cybersecurity plan?

Annual Reports

- Will potential applicants be provided with examples of "good" grant submissions or showcases of previously successful grants efforts after the first year?
- What post-award analysis on use and effectiveness of grant awards will be conducted, if any?
- Are there any prohibited vendors or services in this grant performance series, such as software/services from foreign telecommunications companies that are banned or sanctioned by the FCC?
- Are report management and requirements the same as other DHS/FEMA grants?
- Will templates and/or format be made available to develop the annual reports?
- What is the requirement and process to submit the reports?
- Is there any expectation of confidentiality on the annual reports to manage sensitive data regarding maturity and inherent risks?
- Will there be any requirements to access federal databases or systems for reporting (e.g., ND Grants, Grants Reporting Tool, etc)?
- Annual reports must be publicly available. Which public medium will be used for this requirement (e.g., Cal OES website, DHS website, etc)
- Will there be any training or additional funding for compliance and grant management?