Deloitte.

State & Local Cybersecurity Grant Program (SLCGP)

Overview and Key Considerations

August 2022

Contents

State & Local Cybersecurity Grant Program (SLCGP) – Funding overview

State and Local Cybersecurity Grant Program

Appropriates $1 billion over next 4 years:

- $200 million for FY22
- $400 million for FY23
- $300 million for FY24
- $100 million for FY25

'Eligible entity':

- State
- Tribal government

Funding for each State is calculated by *formula*:

- 0.25% to each of the territories
- 1% to each of the remaining states
- 3% to tribal governments

***Remainder* will be apportioned by:**

- 50% – population of each State divided by the total population of all States
- 50% – population of each State residing in rural areas divided by the total population of all States residing in rural areas

For States, a majority of grant funding is focused on local government cybersecurity:

- At least **80%** of grant funds ***must*** benefit **local governments**
- Of that 80% share, at least **25% *must*** benefit **rural areas**

This can be accomplished as a direct passthrough of funds and/or, with their consent, spent on cyber capabilities provided on behalf of local governments

"**Whole-of-State**"

Federal share of the cost of an activity may not exceed:

- 90% for FY22
- 80% for FY23
- 70% for FY24
- 60% for FY25

For a single entity (1 State)

- 100% for FY22
- 90% for FY23
- 80% for FY24
- 70% for FY25

For a combined 'multi-entity group' (at least 2 States)

Activities for which grant funding *can* be used

- **Develop or revise Cybersecurity Plan of the "eligible entity"**
  - ✓ A State ***must*** submit its Cybersecurity Plan to DHS/CISA for review by ***no later than*** **9/30/2023**
  - ✓ Grant funding which a State dedicates to *developing or revising* a Cybersecurity Plan is ***not*** subject to the required 80% local govt. (and 25% rural govt.) passthrough or benefit
- **Implement Cybersecurity Plan**
  - ✓ But a State ***cannot*** allocate grant funding towards **implementing** its Cybersecurity Plan *until* the Plan has been **approved** by:
    - *State's Cybersecurity Planning Committee;*
    - *State CIO, CISO, or equivalent official;* ***and***
    - *DHS/CISA (i.e., determines Plan meets program requirements)*
- **Assist with *activities addressing imminent cybersecurity threats*, as confirmed by U.S. Dept. of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), to the information systems *owned or operated by, or on behalf of, a State or local governments* within a State**
  - ✓ In addition to developing or revising a Cybersecurity Plan, grant funds can also be spent on *"addressing imminent cybersecurity threats"* prior to Plan submission and approval by DHS/CISA
  - ✓ Anticipate additional information/clarification on *"addressing imminent cybersecurity threats"* in FY22 SLCGP Notice of Funding Opportunity (NOFO) announcement/guidance
- **Pay expenses directly related to administration of grant, ✓ which must not exceed 5% of total grant amount**
- **Fund any other appropriate activities determined by DHS/CISA**
  - ✓ Also anticipate additional information/clarification on *"other appropriate activities"* determined by DHS/CISA in FY22 SLCGP NOFO announcement or other DHS grant guidance

Activities for which grant funding ***cannot*** be used

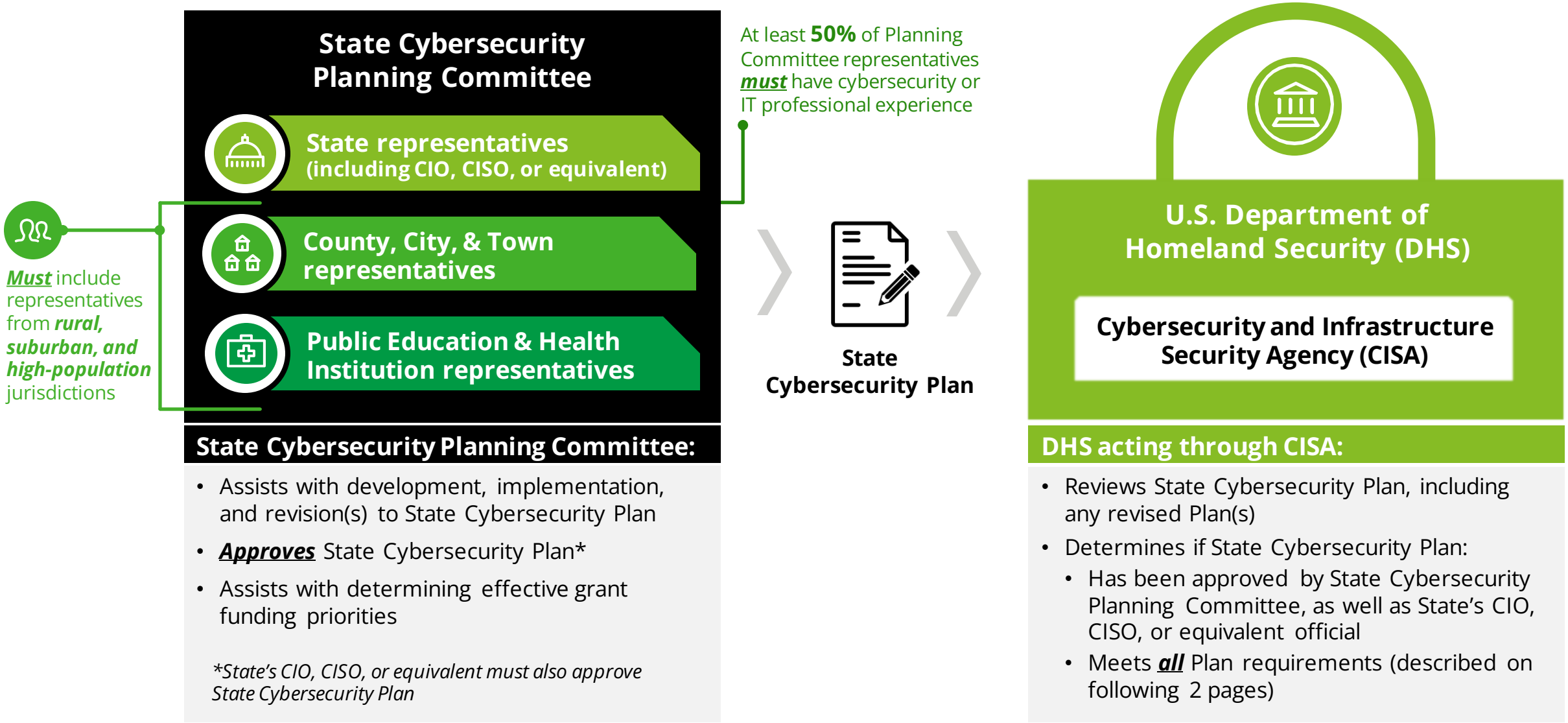
- **Supplanting State, local, or territorial funds**
- **Recipient cost-sharing contribution** ✓
- **Ransomware attack payments** ✓
- **Any purpose that does *not* address cybersecurity risks and threats to an information system owned or operated by, or on behalf of, a state government that receives a grant or a local government within the State's jurisdiction** ✓

✓ **Supplanting:** *when a State or unit of local govt. reduces State or local funds for an activity specifically because federal funds are available (or expected to be available) to fund that same activity*

✓ When supplanting is not permitted, federal funds ***must*** be used to **supplement** existing State or local funds for program activities and ***may not replace*** state or local funds appropriated or allocated for the same purpose

✓ If a question regarding supplanting arises, applicant or grantee will be required to substantiate that the reduction in non-federal resources occurred ***for reasons other than*** the receipt or expected receipt of federal funds

To Receive SLCGP Funding – Establish a State Cybersecurity Planning Committee



State Cybersecurity Planning Committee:

- Assists with development, implementation, and revision(s) to State Cybersecurity Plan
- ***Approves*** State Cybersecurity Plan*
- Assists with determining effective grant funding priorities

**State's CIO, CISO, or equivalent must also approve State Cybersecurity Plan*

DHS acting through CISA:

- Reviews State Cybersecurity Plan, including any revised Plan(s)
- Determines if State Cybersecurity Plan:
  - Has been approved by State Cybersecurity Planning Committee, as well as State's CIO, CISO, or equivalent official
  - Meets ***all*** Plan requirements (described on following 2 pages)

To Receive SLCGP Funding – Create, approve and submit a State Cybersecurity Plan

Cybersecurity Plan submission for DHS/CISA review:

An **"eligible entity"** (e.g., a State) applying for a cyber grant under the State & Local Cybersecurity Grant Program ***must*** submit to the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) a Cybersecurity Plan for review

DHS/CISA review:

In reviewing a State Cybersecurity Plan, DHS/CISA will ensure the Plan has been ***approved*** **by the State's Cybersecurity Planning Committee, as well as the State's CIO, CISO, or equivalent official**, ***and*** meets the following requirements

REQUIREMENTS:

A State's Cybersecurity Plan *must* incorporate, as applicable:

Any existing plans to protect against cyber risks and threats to information systems owned or operated by, or on behalf of the State and local govts. within State	**Consultation and feedback from local governments and associations of local govts.** within State

A State's Cybersecurity Plan *must*:

Assess capabilities to perform the actions & activities described in Cybersecurity Plan	Describe ***metrics*** **for measuring progress towards**: • Implementing Cybersecurity Plan • Reducing cyber risks and identifying, responding to, and recovering from cyber threats
Describe **individual responsibilities** of State ***and*** local governments in implementing Cybersecurity Plan	
Outline necessary **resources and timeline** for implementing Cybersecurity Plan	Specify how **rural areas will receive sufficient access and benefit** from cyber services and items funded by the grant
	Describe how services, items, capabilities, etc. will **benefit local govts.** (**80%** of award) **and rural areas** (**25%** of award)

State Cybersecurity Plan – Required actions and activities in Plan

REQUIREMENTS (cont'd):

Cybersecurity Plan *must describe* how the following will be performed for a State and its local govts.:

Manage, monitor, and track **information systems, applications, and user accounts**	*Monitor, audit, and track* **network traffic and activity**	*Enhance preparation, response, and resilience* of **info. systems, apps, & user accounts** against cyber risks/threats
Implement *continuous cybersecurity vulnerability assessments and threat mitigations* prioritized by risk severity	*Adopt and use best practices & methodologies* to enhance cybersecurity, such as: • **NIST Cybersecurity Framework (CSF)** • NIST cyber supply chain risk mgmt. guidance • Knowledge bases of adversary **tools & tactics**	Promote delivery of *safe, recognizable, and trusted online services*, including through use of the **.gov internet domain**
Ensure *continuity of operations*, including by **conducting exercises** to practice responding to a cyber incident	*Identify and mitigate cyber workforce gaps*, *enhance cyber recruitment & retention*, and *improve knowledge, skills, & abilities* through **cybersecurity training** (using the NIST National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity)	Ensure *continuity of communications and data networks* in the event of an incident involving those communications and data networks
Assess and mitigate, as much as possible, *cyber risks & threats* to **critical infrastructure**, which if degraded may also impact info. systems within a State	Enhance capabilities to *share cyber threat indicators* and related info. between a State and its local govts., including by expanding **info. sharing agreements with DHS/CISA**	*Leverage cybersecurity services* offered by **DHS/CISA**
Implement an **IT and operational technology (OT)** *modernization cybersecurity review process* to ensure alignment of IT & OT cyber objectives	*Develop and coordinate strategies to address cyber risks and threats* **in consultation with local govts.**, *any* **neighboring states or countries**, and **members of an info. sharing & analysis org.**	

State Cybersecurity Plan – Discretionary elements

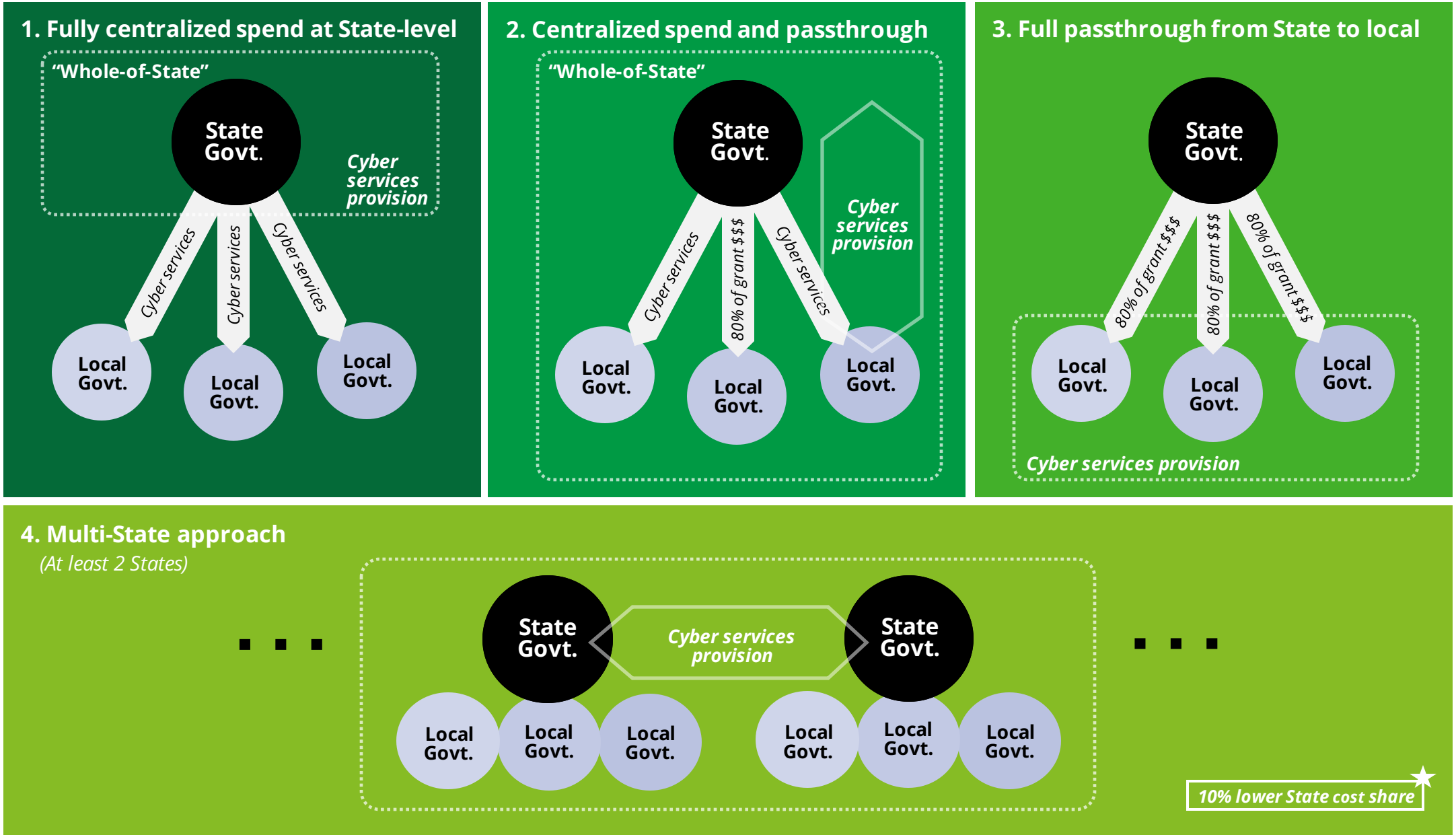
In drafting a Cybersecurity Plan, a State *may*:

Consult with **the Multi-State Information Sharing and Analysis Center (MS-ISAC)**

Include a description of **cooperative programs developed by groups of local governments** within the State for addressing cyber risks and threats

Include a description of **programs provided by the State for supporting local govts. and critical infrastructure owners & operators** to address cyber risks and threats

Cyber services provision model correlates with State funding allocation method



After Receiving Grant Funding – Plan resubmission and annual reporting

Resubmission of Cybersecurity Plan for DHS/CISA review:

Upon *determination by DHS/CISA* that a State's Cybersecurity Plan *meets **all** requirements* of grant program:

- Effective period of initial determination will be **two years**
- DHS/CISA *will review Plan or revision(s) to Plan* **annually** thereafter to determine if Plan continues to meet all program requirements ("annual renewal" of positive determination)

*Note: Within one year (and annually thereafter) of a State receiving funds under this program which has **not** submitted a Plan for review, it **must** report to DHS/CISA on how those funds were spent to develop or revise its Plan or assist with "activities to address imminent cybersecurity threats."*

Annual reporting:

Within **one year** (and **annually** thereafter) of a State receiving grant funding for ***implementing*** its Cybersecurity Plan, it ***must*** submit to DHS/CISA a report, ***using the metrics described in its Plan***, which describes progress towards:

- *Implementing its Cybersecurity Plan*; and
- *Reducing cybersecurity risks, and identifying, responding to, and recovering from cybersecurity threats*, to information systems owned or operated by, or on behalf of the State and the local governments within its jurisdiction

DHS must annually report to Congress on various aspects of the SLCGP, including:

- Use of grants awarded under the program
- Effectiveness of the grant program
- Any required modifications to the program
- Proportion of grants supporting rural areas
- Progress towards:
  - Developing, implementing, or revising Cybersecurity Plans; and
  - Reducing cyber risks, and identifying, responding to, and recovering from cyber threats, to information systems owned or operated by, or on behalf of, State, local, or Tribal govts. as a result of grant funds awarded

SLCGP – Key events roadmap and estimated timeline

Year 1:
(FY 2022)

Infrastructure Investment and Jobs Act (IIJA) – *Section 70612*

Enacted on 11/15/2021 ✓

NOTIONAL AND FOR INFORMATION PURPOSES ONLY

10/1/2021
(FY22 Begins)

01

Funding for the State and Local Cybersecurity Grant Program (SLCGP), as for all new spending in the IIJA (i.e., Bipartisan Infrastructure Law) are "guaranteed appropriations."

*This means all funding authorized to be appropriated for the 4 years of the grant program does **not** require any additional legislative action to be made available for each fiscal year.*

We are here

FY22 SLCGP Notice of Funding Opportunity (NOFO) announcement

Estimated:
Aug. - Sep. 2022

02

For grant applications made prior to submission of a Cybersecurity Plan for DHS/CISA review, a State must certify to DHS/CISA that:

- *The activities supported by the grant are integral to development of the Plan, etc.*
- *The State will submit to DHS/CISA a Plan for review by **9/30/2023***

Grant application submission

Estimated:
Oct. - Nov. 2022

03

Grant awards

Estimated:
Nov. - Dec. 2022*

04

10/1/2022
(FY23 Begins)

What each State (CIO & CISO, etc.) *should do NOW*:

- Begin forming a **State Cybersecurity Planning Committee** *(minimally meeting the requirements prescribed in the SLCGP legislation, pgs. 849-850 of IIJA)*
  - Reach out to & build or enhance relationships with local govt. associations, including:
    - State's Association of County Executives/Commissioners
    - State's City/Municipal League or Association
    - State's Association of Towns/Townships
    - State's Association of School Administrators (Superintendents)
    - State's Association of County and/or City Health Officials
- Work with Planning Committee, once formed, to begin developing outline of a **Cybersecurity Plan** *(minimally meeting the requirements prescribed in the SLCGP legislation, pgs. 846-849 of IIJA)*
- Reach out and build or enhance relationship with State Administrative Agency (SAA)

**Original goal for grant awards was prior to the end of FY22 (9/30/22), but continued delays in initial NOFO release will likely cause awards for Yr. 1 of grant program to slip to Q1 of FY23*

Notes:

- *The key events roadmap and estimated timeline above is based on publicly available information; discussions with relevant organizations, such as U.S. DHS's Cybersecurity and Infrastructure Security Agency (CISA), and a comprehensive review of the State and Local Cybersecurity Grant Program (SLCGP), which is included in Section 70612 of the IIJA, and existing U.S. DHS preparedness assistance grant programs for State, Local, Tribal & Territorial govts., notably the Homeland Security Grant Program (HSGP).*
- *The Period of Performance for each year of grant funding is likely to be at least 36 months based on the PoP for the HSGP, etc. Additionally, the IIJA states that the amounts authorized for appropriation each year for the SLCGP are to "remain available until expended." Therefore, there may not be a PoP end date at all but rather the grant funds will remain available to be obligated until exhausted (i.e., "no-year appropriations"). Ultimately, DHS/CISA will determine the PoP.*
- *The SLCGP's funding through "no-year appropriations" also enables funds that are allocated for a particular fiscal year to be obligated in another fiscal year, thus enabling Yr. 1 SLCGP grant awards to be made after the end of FY22 (9/30/22).*

Appendix

State Cybersecurity Plan – Required Capabilities *(Mapped to NIST CSF Functions)*

Identify	Protect	Detect	Respond	Recover
Manage, monitor, and track information systems, applications, and user accounts		Implement continuous cybersecurity vulnerability assessments and threat mitigations prioritized by risk severity		
Adopt and use best practices and methodologies to enhance cybersecurity		Monitor, audit, and track network traffic and activity		
Develop and coordinate strategies to address cyber risks and threats	Identify and mitigate cyber workforce gaps, enhance cyber recruitment and retention, and improve knowledge, skills, & abilities through cyber training		Ensure continuity of operations, including by conducting exercises to practice responding to a cyber incident	
	Enhance preparation, response, and resilience of info. systems, applications, and user accounts against cyber risks/threats		Ensure continuity of communications and data networks in the event of an incident involving those communications and data networks	
Assess and mitigate cyber risks & threats to critical infrastructure				
Enhance capabilities to share cyber threat indicators and related information	Promote delivery of safe, recognizable, and trusted online services, including through use of the .gov internet domain			
Implement an IT & OT modernization cyber review process to ensure alignment of IT & OT cyber objectives				
Leverage cybersecurity services offered by U.S. DHS's Cybersecurity and Infrastructure Security Agency (CISA)				
Specify how rural areas will receive sufficient access and benefit from cyber services and items funded by the grant				
Describe how services, items, capabilities, etc. will benefit local govts. (80% of award) and rural areas (25% of award)				

Deloitte.