IIJA Cybersecurity Grant Committee

September 28, 2022

State and Local Cybersecurity Grant Program – Funding overview

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

State and Local Cybersecurity Grant Program

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

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

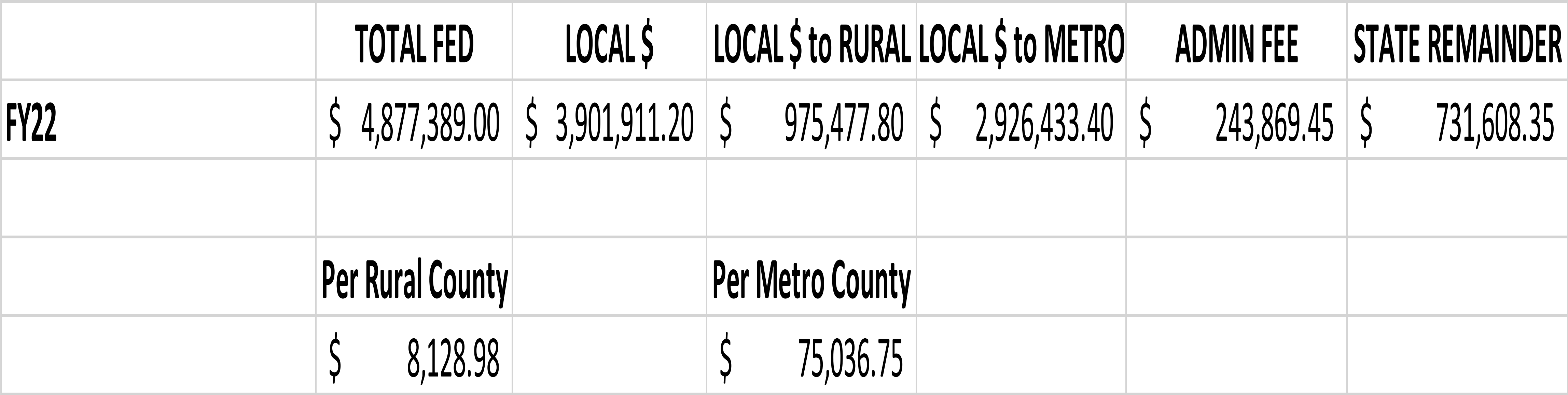
This can be accomplished as a direct passthrough of funds and/or, with their consent, <u>spent on cyber capabilities provided on behalf of local governments</u>

“Whole-of-State”

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

For a single entity (1 State)	For a combined ‘multi-entity group’ (at least 2 States)
90% for FY22	100% for FY22
80% for FY23	90% for FY23
70% for FY24	80% for FY24
60% for FY25	70% for FY25

Georgia Funding Allocation



	TOTAL FED	LOCAL $	LOCAL $ to RURAL	LOCAL $ to METRO	ADMIN FEE	STATE REMAINDER
FY22	$ 4,877,389.00	$ 3,901,911.20	$ 975,477.80	$ 2,926,433.40	$ 243,869.45	$ 731,608.35
	Per Rural County		**Per Metro County**			
	$ 8,128.98		$ 75,036.75			

Match Requirements

Eligible entities, if applying as a single applicant, must meet a **10% cost share requirement** for the FY 2022 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants shall agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 10% of activities under the award.

DHS/FEMA administers cost-matching requirements in accordance with 2 C.F.R. § 200.306.To meet matching requirements, the recipient contributions must be verifiable, reasonable, allocable and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds.

For example, if the federal award were at a 90% cost share and the total approved budget costwas $100,000, then:

•Federal share is 90% of $100,000 = $90,000

•Recipient share is 10% of $100,000 = $10,000

However, with this example, if the total cost ended up being $120,000, the federal share would remain at $90,000 due to the statutory formula even if it means the federal share ends up being lower than 90%. Any cost overruns will not be matched by this grant program and will be incurred by the recipient.

Objectives

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

- **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.

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 grant 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 grant 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** ✓

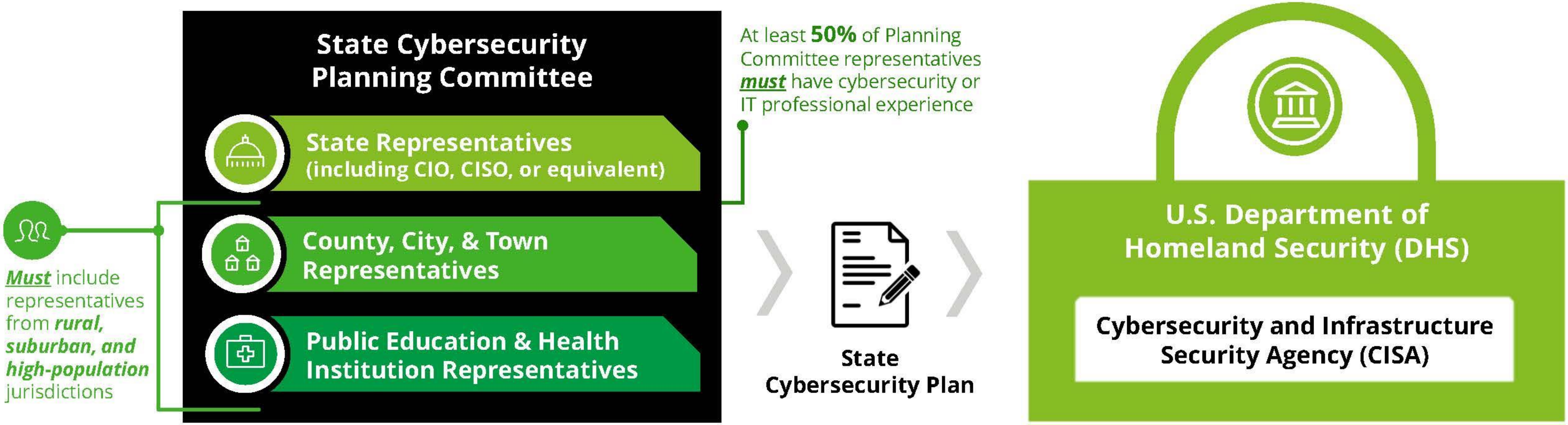
- **Any purpose that does *not* address cybersecurity risks and threats to an information system owned or operated by, or on behalf of, a state government that receives a grant or a local government within the State's jurisdiction** ✓

✓ **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 Grant Funding – Establish a State Cybersecurity Planning Committee



State Cybersecurity Planning Committee

State Representatives (including CIO, CISO, or equivalent)

County, City, & Town Representatives

Public Education & Health Institution Representatives

Must include representatives from ***rural, suburban, and high-population*** jurisdictions

At least **50%** of Planning Committee representatives ***must*** have cybersecurity or IT professional experience

State Cybersecurity Plan

U.S. Department of Homeland Security (DHS)

Cybersecurity and Infrastructure Security Agency (CISA)

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 Grant 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 **individual responsibilities** of State ***and*** local governments in implementing Cybersecurity Plan

Outline necessary **resources and timeline** for implementing Cybersecurity Plan

Describe ***metrics*** **for measuring progress towards**:

- Implementing Cybersecurity Plan
- Reducing cyber risks and identifying, responding to, and recovering from cyber threats

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.**

Path Forward

30 SEP: Finalize committee membership / charter

21 OCT: Submission of agency/local plans (Cybersecurity Plan Template Appendix B) gacyber@gta.ga.gov

04 NOV: Committee completes plan reviews and draft grant submission

11 NOV: Final State Cyber Board approval

15 NOV: Submission deadline

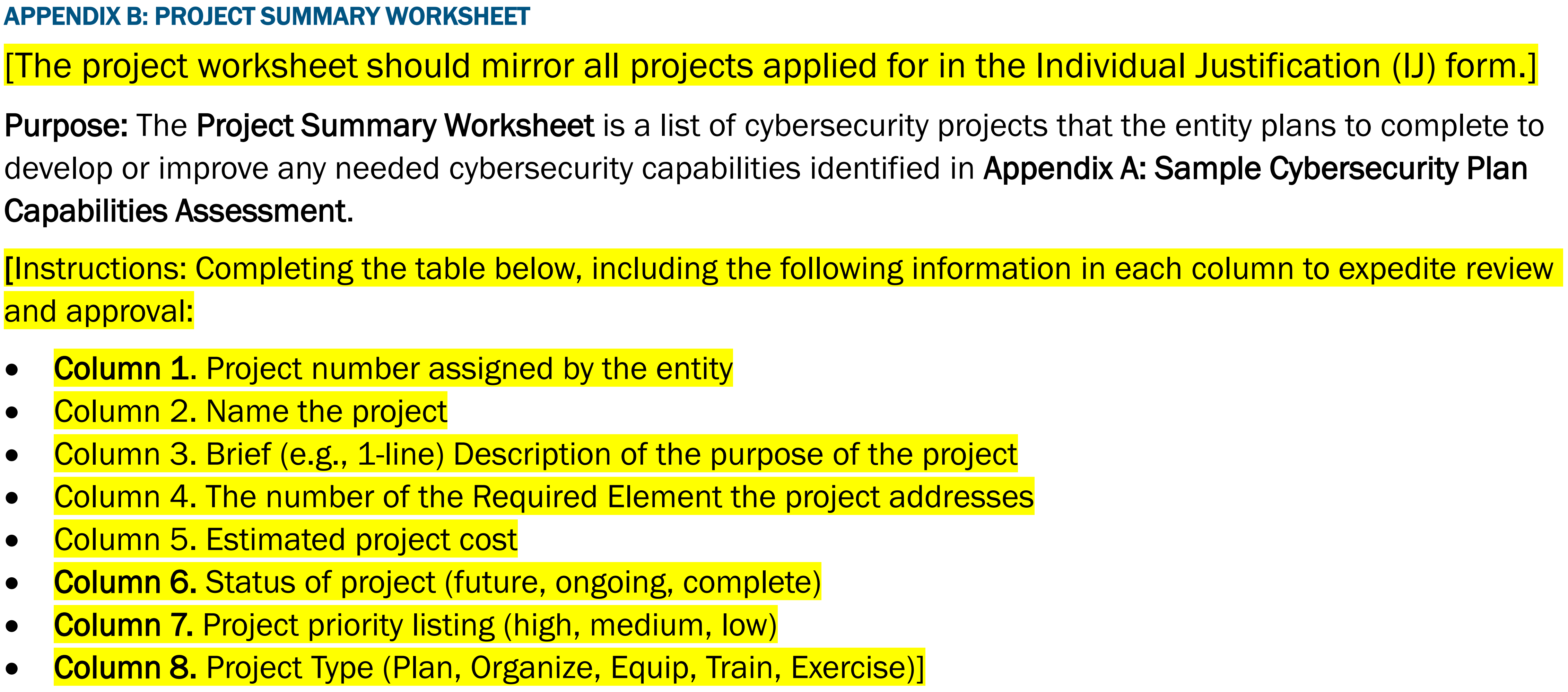
30 NOV: Est. Funding Selection Date

31 DEC: Anticipated Award Date

Priorities

- Multifactor Authentication
- Endpoint Detection and Response
- Web presence protection
- Backup and recover solutions
- Threat intelligence and brand management
- Enhanced Monitoring
- Cyber Maturity Assessments
- Training

Project Submission



APPENDIX B: PROJECT SUMMARY WORKSHEET

[The project worksheet should mirror all projects applied for in the Individual Justification (IJ) form.]

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment.**

[Instructions: Completing the table below, including the following information in each column to expedite review and approval:

- **Column 1.** Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Element the project addresses
- Column 5. Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

POC

David Allen – State CISO and Committee Chair

CISO@gta.ga.gov

470-270-3218