State and Local Cybersecurity Grant Program (SLCGP) 5th Cyber Planning Committee Meeting Minutes

May 18th, 2023

Agenda Items		
Roll Call		Netta Squires
Review and approval of last meeting's minutes	April 13th, 2023 Minutes	Netta Squires
General Updates	SLCGP Cybersecurity Plan Update	Taylor Munir
Cybersecurity Plan Investments Justifications Discussion	Survey Results Investment Justifications Examples & Development of Maryland Investment Justifications	Markus Rauschecker Taylor Munir
Adjournment		Netta Squires
Next Meeting	Jun 15, 2023 2:00 PM - 3:30 PM EST	
Action Items	See action items here.	

Attendance

Committee Members in Attendance:

Marcia Deppen (Co-Chair), Netta Squire (Acting Co-Chair)

- David Lewis
- Valerie Hawkins
- Nathaniel Watkins
- Kathryn Poff
- Keith Young
- John Bruns
- Matt Otwell
- Mark Cather
- Jon Caudle
- Edward Gardner
- Justin Fiore

Guests and non-voting members:

- Sabrina Chase
- Taylor Munir
- Jason Schaum
- Markus Rauschecker
- Patrick Mulford

Absent: Kevin Kinnally, Katie Savage, Russell Strickland, Susan Killian, Scoot Boone

---

Meeting Called to Order at 2:02 PM EST by Netta Squires.

I. **Roll Call:** Netta Squires facilitated roll call to the committee.

II. **Minutes: Motion #1:** A motion was made by Taylor Munir to approve the April 13th, 2023 minutes as written.

Motion #1: The motion passed without objection.

III. **General Updates**

MD Cybersecurity Plan update presented by Taylor Munir

The MD Cybersecurity feedback submitted by the committee has been added into the plan. We will be making final updates based on the Investment Justifications (IJs) that are discussed later today. You should have received the most recent copy of the draft plan on **MAY 16th.** Please connect with Taylor Munir (taylor.munir@maryland.gov), if you have any final plan feedback.

Additional General Updates presented by Marcia Deppen

Compliance Requirement for Open Meetings: For the open meeting act to be in compliance the meeting needs to have somebody who's serving as the open meeting officer. Marcia Deppen volunteered for that position until someone else would like to volunteer.

Process for moving to a closed meeting: The committee can go into closed session specifically when they will be discussing jurisdictional projects that might contain information that is sensitive in nature. This is done by committee vote at the beginning of the meeting that requires a closed session. In addition, the intention for part of the meeting to be a closed session must be posted on the agenda beforehand.

Netta Squires opened the meeting for discussion.

Keith Young: Should we vote on a closed session for the next session, if we will be having this discussion at the next meeting?

Netta Squires: We should discuss this as part of our IJ discussion today.

Committee agreed with that assessment.

IV. Survey Results & Cybersecurity Plan Investments Justifications Discussion - Presented by Markus Rauschecker, Taylor Munir, & Jon Caudle.

A. Survey completion update presented by Markus Rauschecker.

There was a survey that was sent out to all the jurisdictions that asked a lot of questions about demographics and what type of jurisdiction is responding. The survey was a self assessment on their capabilities, and their gaps, and then lastly asked about what kind of issues the jurisdiction would like to address with any potential funding and what kind of projects they might have in mind that they would like to find.

There were a total of 37 responses submitted. 5.4% of respondents were from a higher education institution, 37.8% were from a county, 40.5% were representing a public school, and 16.2% were from a municipality.

One of the first questions we asked was how many people are actually in your jurisdiction to understand how big the jurisdictions are that we're responding to. We can see that the majority of respondents have fewer than twenty thousand people within their jurisdictions. So what that means is that actually the majority of our respondents fall within the rural definition of the Homeland Security Act definition that we're using for our plan.

Trying to get a little bit more information about the makeup of jurisdiction, to understand how many users these jurisdictions have and how many active accounts they were responsible for. Most of the respondents were smaller jurisdictions and had smaller numbers of total users within jurisdictions, and also between zero and one hundred active service accounts.

Next, we wanted to find out some information about what kind of cyber security resources these jurisdictions currently have. One of the primary

questions the survey asked was how many dedicated cyber security employees do you actually have within your jurisdiction. Forty percent of jurisdictions that responded said that they have zero dedicated cyber security personnel.

Then the survey moved into budget related questions. First, what is your overall budget? Respondents have an overall budget, between zero and two hundred million dollars. Of that we ask what is your annual IT budget?

Most jurisdictions have a relatively small IT budget between zero and one million. Some had a budget of one to five million. In terms of a cyber budget, most respondents are on the very low end in terms of how much they're spending on cyber security relative to their overall budget.

Given that forty percent of jurisdictions don't even have a cybersecurity dedicated cyber person. It's no surprise that we're seeing zero dollars spent on cybersecurity employees, and not very much money spent on contractors either. Where we're seeing jurisdictions spending money is on services.

Next, we wanted to get a sense of the overall cybersecurity posture of Maryland jurisdiction.

Markus paused to discuss the separate NPSR survey first that had thirty- three local jurisdictions, forty county's that participated in that process and the assessment results indicated that the average scores of all of the participants in that assessment was hovering around four for most of the functions. In the activity performance summary section there was lower adoption.

Moving back to the SLCGP Survey, the biggest gap for jurisdictions is related to managing monitoring and tracking information system applications for users accounts, which was true for almost seventy- two percent of respondents. Markus noted that this capability is one of the

required elements for the cyber plan that Maryland must be capable of doing.

Fifty percent of the respondents said that they have gaps, with respect to identifying, and the resiliency of their system. There were gaps identified with relation to multi- factor authentication which is a required best practice in the cyber plan. We had almost sixty percent saying they have a gap related to recruitment of cybersecurity workforce retaining cybersecurity workforce, finding the skill Cybersecurity workforce. That was noted by sixty- two and a half percent of respondents.

Next, we asked respondents to estimate the funds needed to complete their proposed solutions and identify specific projects through a ranking system of their 1st, 2nd, and 3rd choice projects.

For the 1st choice projects, a lot of jurisdictions said they would like to enhance managing, monitoring and tracking. Next, was adoption of multi- factor authentication,and also things like training and exercising. 2nd choice projects for some jurisdictions also included enhancing managing, monitoring and tracking. 3rd choice projects contributed largely to operational planning.

The project costs estimates provided by jurisdictions ranged from a couple thousand dollars to about a couple of million dollars to complete the 1st choice project. For the most part, responses indicated that they could partially pay for some of these projects, but there would be additional support needed to fund the project that they would like to do. We also ask if these projects were a recurring or one-time expense. This had mixed answers. Some projects were recurring expenses while others were one-time expenses. The recurring expenses dealt mainly with salaries for employees. The cost range for 2nd choice projects ranged from seven thousand and a million dollars.

Some interesting finds in the survey included:

1. Almost 90% of respondents said that their jurisdiction had cyber insurance.
2. 35% of jurisdictions were not responsible for any critical infrastructure, and if they were it was related to water and water systems.
3. 65% of respondents said that there was some type of cyber hygiene training available in their jurisdiction, and 35% said no.
4. The survey also asked if there was a formal cybersecurity policy in your jurisdiction for employees and contractors. The results determined that most policies were related to acceptable use, password management, and breaking technology.

Markus opened for discussion.

John Bruns: It is interesting that many jurisdictions' main need is to understand what they have and not having cyber staff.

David Lewis: Agreed with John's assessment.

Mark Cather: Do we have a question around non-dedicated security staff? Do they have no staff or does the survey represent that they have no cybersecurity staff.

Netta Squires: We asked how many other IT staff in other departments, but not a phrased question on "non-dedicated staff".

Markus added, there were some respondents that said they had a half of a person dedicated to cybersecurity.

Edward Gardner: There are some dedicated staff for Frederick County. To add some context, most of the zeros from public schools are likely because there is a collaborative effort between non-dedicated cyber professionals. There is the issue of staff to support cybersecurity efforts because these are non-dedicated staff. They are doing what

they can with the resources they have, so resources in that area are welcome.

Mark Cather: This is a key point to think about: How will we support projects with limited internal resources to help get the project off the ground?

Johns Bruns: There are multiple areas of attack. How we identified these different areas and prioritized. If we look at what counties have, we might need to look outside and then internally.

B. **Funding Process Review presented by Taylor Munir.**

The total grant award is $3,214,088.00 of this amount a 80% local pass through is required which amounts to $2,571,470.40. The 80% local passthrough must support local entities. Additionally, a 25% rural carve out must support rural entities totalling $642,617.60. These may overlap.

The state share amount is $428,447.43. The M&A amount is $214,170.17. There is a required match for Maryland which will be shared amongst all entities who receive monies. Maryland's required match is $357,009.78 (which will be waived in year one). **Reminder: we will be expected to match year two monies and we are anticipating double the funds in year two. This means an expected match of about $700,000.**

The period of performance is September 1, 2022 to August 31, 2026.

Next slide: In regards to investment justifications, there must be at least four IJs, one for each of the four FEMA objectives. Each IJ must describe how the project aligns to our plan and how success will be measured.

Allowable Investment Justifications fall into one of six categories: Planning, Organization, Equipment, Exercises, Training, and Management and Administration (M&A). The grant cannot be used for: Cost share, Ransom, Insurance Premiums, Acquire Land or Construct Buildings.

Next slide: Descriptions of the allowable IJs are:

Planning - Development, review and revision of cyber plans, and Other planning activities

Organization - Program Management, Development of whole community partnerships that support the Cyber Planning Committee, Structures and mechanisms for information sharing between the public and private sectors, Operational Support, and Hiring of personnel (training and exercise coordinators, program managers, planners).

Equipment includes: Maintenance contracts/agreements, Warranty coverage, Licenses and user fees, Repair or replacement of equipment, and Equipment upgrades. All equipment purchases must be coordinated with the Statewide Interoperability Coordinator (SWIC).

Exercises - must be HSEEP concept

Training

M&A

C. **Investment Justifications Examples presented by Taylor Munir.**

As mentioned above, the 80% local passthrough must support local entities while the 25% rural carve out must support rural entities. There is a required match for Maryland which will be shared amongst all entities who receive monies. The period of performance: September 1, 2022 to August 31, 2026.

The plan must include at least four IJs, one for each of the 4 FEMA objectives. Each IJ must describe how the project aligns to our plan and how success will be measured.

The **4 FEMA objectives** are folded into the 16 Elements, and serve as a part of the guidance for creating the Cybersecurity Plan and will be fulfilled by meeting the 16 Elements. These objectives are:

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.
2. Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
3. Implement security protections commensurate with risk (implementation of best practices).
4. Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

We reviewed the projects from other approved state plans and have identified 4 different common project types. These are:

1. **Individual Project Funding:** Some States provided information on the pass through funding projects as a project type. They included this

information under their own projects IJs as a "General Funds" project, which detailed how much money was earmarked as pass through funds for local and rural communities. (Note: Any approved local and rural community projects using the SLCGP FY22 funds must be included in the Maryland Cybersecurity Plan IJs section.)

2. **Funding New Statewide Services:** Some states intend to use funding for launching wholly new projects that provide statewide capabilities that have not existed before. For example, establishing an ISAC, staff augmentation, and/or adding professional services to implement security protections for state and/or local entities.
3. **Expanding Current Statewide Services:** Some states are intending to use funding to support or expand existing state projects and capabilities, such as .gov domain expansion.
4. **Training:** States are intending to use a portion of their funds for cybersecurity training for government employees or IT professionals, specifically.

Committee members received a document that includes a list of project examples that they can reference during the subsequent discussion. Taylor did a brief review of the example types.

Taylor Munir opened up the meeting to questions on the IJ examples.

D. **Investment Justifications Discussion presented by Netta Squires & Taylor Munir.**

Taylor Munir: We will now open up the meeting to discussion on the IJs for Maryland. We will also determine metrics by which to measure success of projects.

Netta Squires opened up the meeting to discuss the IJs for Maryland.

Discussion:

- John Bruns: Network discovery & mapping
- Matt Otwell: Tool recommendations
- David Lewis: Bringing in a third party to assist with network discovery and Training for jurisdictions so they understand how to determine what they don't know about their systems and networks (both for users and leadership)
- Edward Gardner: Do we make .gov migration required, and if so that is a heavy lift; how can we support that?
- David Lewis: Looking at the issue of IT staff, or lack thereof.
- Valerie Hawkins: How can we be a force multiplier to make better use of existing staff.
- Mark Carter: Can we provide training on how do you implement
    - John Bruns: suggested a training "discovery day", to allow cyber staff to ask questions and learn about things they would need to know during day 1 of a cyber attack.
    - Edward gardner: Can we create a training or exercise bank provided by the State that jurisdictions can use internally & also a privacy lawyer that can help jurisdictions create governance policy on records management.
- David Lewis: Providing initial guidance and boots on the ground for phase 1 to help understand and implement initial cyber needs.
- Jon Caudle: Should we include priorities on the applications so we can steer applicants to resources. Example would be making asset discovery a priority. Then in the following years they build cybersecurity posture.
- Nathaniel Watkins: Can we allow the State to use network maryland to look at jurisdictions networks to help with mapping, if they want that.
- Johns Bruns:
    - NJ is looking at EDR or other large programs. Some states are using state funding or using the SLCGP to help with that.

    - Is there a tiered approach that we can use that's more collective.
- Mark Cather: Year 1 could be discovery and planning to understand what to dedicate investments to moving forward. Year 2 is investment from what is learned in year 1. Year 3 is filling in the gaps from year 2.
- John Bruns: There is a need for an incident response retainer. They may go through their cyber insurance but it is still a need.
    - David Lewis, will this fall under planning or organization and not be considered an unallowable expense.
    - Edward Gardner: I would like the idea of people on retainer to help with these aspects.
- Committee Question: How many counties meet the rural definition?
    - Answer from Anna Sierra: 18 counties.
- John Bruns: Every county should have someone to provide guidance on how to implement protections, MFA etc.
- David Lewis: Rather than have a CISO, have an ISM or ISO on the ground to help complete these gap projects.
- Netta Squires: Do we consider assessments as a good initial need?
    - Mark Cather: I think it will be a blend of some jurisdictions that already know what an assessment will provide and others that need the next step up.
    - Edward Gardner: From a school district perspective, this would be helpful.
    - Matt Otwell: This is also a culture shift within organizations. An assessment may seem daunting to some. We need to consider how to eliminate the fear factor and create a culture of security.
    - Edward Gardner: seconded the need for a culture shift.
    - David Lewis: Looped in the ISM and how this can help with this and creating a more individual customer approach and help plan for remediation.
- Jon Caudle: Assessments are a priority for this grant program and something we can stress within the application process.

- Keith Young: We should focus on IR, MFA, Asset discovery, security awareness training. Also, someone that can help jurisdictions complete these (outsourcing some assistance for those who don't have the funds for dedicated professionals)
- Netta Squires: We should look at assessment as a prompting for baseline cybersecurity.

Netta Squires provided a quick summary of what was discussed by the committee. The committee focused on a hybrid approach looking at governance, implementation of best practices, and ISM guidance based on individual jurisdictional needs, and also provided money to those who would not like to join a multi-jurisdiction project.

Year 1: The committee discussed focusing funds in two different ways:

1. 1st on assisting jurisdictions with governance and implementing baseline standard best practices. Baseline standard best practices would be defined using the requirements guidance outlined in the Maryland Cybersecurity Plan and approved by the committee. The committee discussed hiring a ISO/ISM that could provide individual assistance to interested jurisdictions with these priorities in mind.
2. 2nd for jurisdictions that do not want to follow this model or have more laid out individual projects, they could submit an application for funding for priorities set by the committee, e.g. MFA, EDR, Security Awareness, and Firewalls. .

Year 2: The committee discussed focusing funds on:

1. Finalizing the 1st priority area in year 1 and starting to look at the next level after baseline best practices have been implemented.
2. Individual project applications for jurisdictions not utilizing priority 1.

The planning team will review the approach discussed above and cross check it with the SLCGP requirements to make sure it is in compliance with these requirements. They will review this with the committee at the next meeting.

VI. Questions/ Open Forum

Netta Squires: There will be an MML meeting coming up on June 2nd and also a MaCo meeting is being scheduled. Please encourage your colleagues to join us in the discussions for MD's jurisdictions cybersecurity needs.

Netta Squires asked the committee should have part of the next meeting have a closed session.

Sabrina Chase mentioned that we will have to provide a note on our future agenda that part of the meeting will be closed, and that Marcia and Sabrina will provide a process for that.

VII. Action Items - presented by Netta Squires

We will send the committee the summary documents that contain the results of the survey. However, the document will be scrubbed of all jurisdictions identifiable information.

VIII. Adjournment

Recorded vote to close the meeting:

Date: 04/13/2023; Time: 4:09 PM EST ; Location: In- person & Teleconference

Meeting Slides are attached.