CYBERSECURITY ADVISORY COMMITTEE
Hybrid Meeting
Thursday, October 5, 2023, 2:00 PM

In-Person at the NM Gaming Control Board
4900 Alameda Blvd, NE, Albuquerque, NM 87113

1. Welcome and Call to Order

Ms. Narvaiz called the meeting to order at 2:03 p.m. and welcomed everyone to the meeting. She reviewed general procedures for the Zoom participants.

2. Roll Call

MEMBERS PRESENT

Raja Sambandam, Chair
Seth Morris for Raul Burciaga
Todd Ulses
Jason Johnson
Logan Fernandez for Cassandra Hayne
Kenneth Abeyta
Robert Benavidez
Josh Rubin
Phil Zamora for Sarita Nair

Danielle Gilliam for James Kenny (joined after roll call)
Cecilia Mavrommantis for Wayne Propst (joined after roll call)

MEMBERS ABSENT

James Mountain (IAD)
Clinton Nicely
Suzanne Begay

OTHERS PRESENT

Renee Narvaiz, PIO-DoIT
Melissa Gutierrez, DoIT Project Mgr.
Todd Baran, Office of State Atty. Gen.
Peter Mantos, DoIT Special Projects Mgr., Todd Glanzer (Deloitte), Rick Comeau (Deloitte), William Campos (Deloitte), Andrew Buschbom, Flori Martinez, Jeff Roth, Dan Garcia, Joshua Yadao, Jacci Gruninger

3. Approval of Agenda

Ms. Narvaiz called for a motion to approve the Agenda for today's meeting.

MOTION Mr. Benavidez so moved, seconded by Mr. Johnson.
There being no opposition, the Agenda was approved.

4. Approval of September 7, 2023 meeting minutes.

Ms. Narvaiz called for a motion to approve these minutes.

MOTION Mr. Johnson so moved, seconded by Mr. Benavidez.
There being no opposition the minutes were approved.

5. Updates from Committee Chair – Raja Sambandam

Thanked Committee members for their attendance today.

The Plan has been submitted, was accepted and approved. The NOFO requirements for Year-Two of the SLCGP were published and the application has been submitted for this.

Reviewed the joint session of the Cybersecurity Advisory Committee and the Cybersecurity Planning Committee held last week, which included how the existing organization would continue to function, as well as the process for some legislative bill clean-up, working with Senator Padilla.

Mr. Sambandam asked Ms. Gutierrez if there was anything else that has occurred in the interim since the last meeting which should be mentioned.

Gutierrez – Nothing else. Asked Mr. Mantos if he had a comment or question.

Mantos – Heard his name mentioned as he walked by meeting room. Is there anything he can help with?

Sambandam – Was giving update to the Committee regarding the joint meeting last week, had mentioned Mr. Mantos by name with respect to the continuing function of the Cybersecurity Planning Committee, with the response being to go through the legislative process of fine tuning the existing law.

Mantos – Will be happy to join the meeting.

Sambandam – Year-Two application will be for approximately $4.1 million. Were able to leverage and scale the enterprise contracts and now ready to service K-12 schools, higher educational institutions and the counties. Asked Ms. Gutierrez for confirmation on this.

Gutierrez – Correct.

Sambandam – Paused for questions. There were none at this time.
Shared that there were a number of items in the news this past week regarding security breaches, i.e. Johnson Controls, etc., which all point to not having good cybersecurity or good cyber hygiene practices in place. October is Cybersecurity Awareness Month. Reminded everyone of the need to share the importance of good cybersecurity practices and cyber hygiene, both in the workplace and in personal practices. Noted that October is also a month where heightened activity from attackers is often seen. Paused for any questions.

Asked Deloitte representatives if any further responses to the Capabilities Assessment have been received since last week.

Campos – No further responses since last week.

Sambandam – Was +/- 150 last week, correct?

Campos – It was 130.

Sambandam – Asked members to encourage their respective groups/organizations to complete the Capabilities Assessment. Need more participation to gather contacts in order to start scheduling penetration testing, the vulnerabilities assessment, etc. Need to know where "holes" are in order to fix these as well as identify the necessary resources to take a risk based approach. Once this can be accomplished will have more meaningful, reliable information to help provide a level of assurance and gain a better understanding of the current status. Paused for questions. There were none.

6. Update from Report Subcommittee – Jason Johnson

This subcommittee met with the Plan Subcommittee from the Cybersecurity Planning Committee and had a good conversation about some of the work already done. Agreed to have them plug in some of the overarching pieces of their report, which were discussed. They will be going over the particulars of this, in their weekly meetings on Wednesdays, upcoming on the 11th, the 18th and the 25th, with the intent of meeting before this whole Committee meets again in order to present the work from the Subcommittee to the entire Committee.

Mr. Johnson asked Ms. Gutierrez to screen share the information received, which she did.

Mr. Johnson asked Mr. Benavidez or Mr. Glanzer to review the presentation.

Glanzer – Reviewed the presentation which included the Table of Contents layout and outline of the Approach, which was presented to the Subcommittee and approval was given to move ahead with the draft. Reviewed the schedule to complete the five items identified by October 25th for final edits in preparation for final draft review by the full Committee. No blockers identified to completion of the draft in this timeline.

Johnson – Clarified meeting date in the timeline as November 2nd.

Sambandam – Asked for clarification of "next steps" in this presentation. Are these next steps as part of the Cybersecurity Plan or next steps related to the report process.

Johnson – Replied that it would be the latter (the report process).

Sambandam – Any other recommendations or additions evolving for the Report Subcommittee to consider with respect to the Table of Contents?

Johnson – Agreed. Asked if there were any questions or additions for the Subcommittee. There were none.

Sambandam – Should recommendations be grouped by category or across the ecosystem; e.g., recommendation to define a better data classification policy or to have data privacy and loss established.

Johnson – This is next steps for the Subcommittee just to develop the report due in November. Information already gathered being synthesized into the report. Work listed as accomplishments and next steps specifically for being able to deliver report in November.

Sambandam – Thanked Mr. Johnson for his comment. Definition of what should be included in the report seems to be lacking or was unclear. Will this report be used to measure the effectiveness of the Committee? Would projected accomplishments be used a measurement of the Committee's work, either as part of the Cybersecurity Plan or part of the commitment made in the Report?

Johnson – Asked Mr. Glanzer from Deloitte to review what will be included in the Report. His understanding is that the purpose of this Report is to review the current status of the State, not setting future expectations within the Report, only reporting what is known, but he is not entirely sure about this.

Sambandam – Asked for additional comments from Deloitte or others.

Glanzer – Can do a little bit of both. Legislative language is broad enough as it asks to address the preparedness of the State with regard to cyber and there is some measure of that included through the self-assessment and other programs at the state level. Thinks qualified reports of the status can be made based on this information along with recommendations that tie to the priorities identified or gaps identified at this point in order to raise the cybersecurity baseline and overall preparedness. This would give the Office and the Committee a chance to measure some of these things in conjunction with the Plan moving forward through the year, some tied to grant projects or other initiatives, knowing that in October 2024 the Committee will be required to produce another Report and annually thereafter.

Comeau – Agreed with Mr. Glanzer's explanation. Gave example of mapping the metrics within the plan to the objectives.

Sambandam – Thanked Mr. Comeau for his comment.

Abeyta – Agrees with comments from Deloitte. Information from surveys discussed in the Subcommittee meeting. Also discussed broad stroke information to help outreach to rural communities with no IT infrastructure to

engage them and help them understand where they are. Nothing binding, but will enable a full understanding of the entire state, not just the entities who have responded to the surveys. Want to actively engage rural communities to include these as part of the Report. Use the metric of what is known and can be reported on, but continue efforts to engage and gather additional information moving forward. Regional meetings have been discussed.

Sambandam – Had a question about section 5, subset G, page 8, refers to status of cybersecurity preparedness within agencies and elsewhere in the state. Section G reads, “Cybersecurity Advisory Committee shall present a report to the Legislative Finance Committee and appropriate interim committee concerned with information technical (dates) regarding the status of cybersecurity preparedness within the agencies and elsewhere in the state”. Elsewhere in the state could be anywhere, such as higher education institutions and public schools, counties, municipalities, etc. Referring to this earlier level, should things be kept at a grouping level or segments in terms of where things stand in the process. This could be based on the 130 Capabilities Assessments received. Not sure how this could be uniquely quantified. An agreeable solution needs to be ascertained for both the Legislature and the Executive Branch, which will be easy to read and understand.

Johnson – There are a lot of entities/agencies that just do not know how to respond. This void also needs to be addressed, having adequate IT and cybersecurity technology resources at these levels.

Ulses – Regional meetings discussed previously. He, Mr. Benavidez and Mr. Abeyta have discussed how to do regional divisions to help with this and improve the response rate, at least with respect to the counties. Schools and municipalities could also be included.

Abeyta – OBAE has done some regional meetings, inviting everyone in each area and had a lot of response. This would make for easier access by outlying communities, who might not make it to Santa Fe. In some villages emails of this nature are often just sent to their IT contractor. Having regional meetings could help close the gap for smaller counties, communities, school districts, etc. Addressing this, to say that this gap and disparity in the rural areas of the state are being addressed, would be a good blanket statement to include, which could be quantified later with the outreach provided and the number of responses received by category. No way to understand the status of the whole state at this time due to lack of information from certain areas.

Sambandam – Would another communication push through the Association of Counties, the Municipal League and higher education institutions be helpful? Could a dedicated time slot be made available for call-in through teams or via Zoom, to walk them through completion of the Assessment? Do not have good contact information in areas where responses have not been received.

Abeyta – Agrees that as a group this is lacking. Mr. Benavidez's idea to regionalize this is good because he (Mr. Abeyta) knows quite a few of the IT professionals in the northeastern part of the state, including medical, higher education, K-12, municipalities, counties, and it is easier to have those conversations in a more "boots on the ground" approach than inviting to a Zoom meeting. Personal contact may be more successful.

Ulses – What areas or different types of agencies/sectors are the most lacking? Would these be the areas to focus efforts? Are counties and municipalities the areas of least response?

Sambandam – Good question. Asked Deloitte to provide this information.

Abeyta – Can we also look at locations? Direction for where to go.

Sambandam – Reviewed screen share by Deloitte. Asked Mr. Fernandez to comment on response from Courts.

Fernandez – There are approximately 74 courts. Three do their own IT, their own infrastructure. The rest go through the Administrative Office of the Courts. Questionnaires are generally centralized through the Admin. office. Depends on what courts things are being sent to. They recommend sending directly to the Administrative Office of the Courts. Two courts in Albuquerque are fairly independent with regard to IT infrastructure.

Sambandam – Can Capabilities Assessment be sent to Mr. Fernandez for completion to increase the number or court responses?

Fernandez – Would prefer this. Will answer what they can at the Admin. Level.

Ulses – If everything is sent through Mr. Fernandez's office this will only be recorded as one response for the entire Administrative Office of the Courts statewide, correct?

Fernandez – Yes, that is correct.

Ulses – Noted that county responses are 18, which is barely over half the total counties, and local municipalities are at 9 out of several hundred. Need to be mindful of this when examining these numbers.

Benavidez – Suggested that Mr. Fernandez discuss this with Ms. Hayne as he has had a conversation with her about this and she was concerned that responses from the courts could be used in a negative way.

Fernandez – Will look at the survey and if there are concerns will reach out and

mark as something they are not comfortable sharing.

Sambandam – Thought the sensitivity concern had been addressed.

Abeyta – Noted that many of the healthcare institutions/hospitals in rural areas are managed by out of state entities. If one entity has several hospitals within the state would these fall under one reply or would there be instructions for how to reply individually. This could be interesting.

Sambandam – Not sure which three healthcare entities completed the Capabilities Assessment. Mr. Abeyta is correct. Has access to Presbyterian CISO and will ask them to complete the Assessment, but this would be for all Presbyterian facilities, would be the same for Lovelace, which is based out of state. Can reach out. Has question about whether healthcare is actually part of infrastructure focus area.

Benavidez – Recognized that healthcare and critical infrastructure are not really part of the scope for the Executive Order and the Office of Cybersecurity per se, but there are some tie-ins, critical infrastructure being, for example, a water authority such as Albuquerque/Bernalillo County Water Authority, which would be one of those not completely within the scope of this, but is a critical part of understanding cybersecurity in New Mexico. The same applies to healthcare. Dr. Liebrock and Ms. Lopez led the team with respect to healthcare and this sector got the poorest response. These are heavily regulated industries so they do tend to already have a pretty good cybersecurity program as a requirement on the funding they receive. May not need to focus on these as hard as education, tribal, etc.

Sambandam – Primary intent of the NOFO was to address local governments and schools, correct?

Comeau – Definition of local governments provided in the NOFO includes K-12 schools, but also includes counties, cities, towns, public health at the local level. The main focus though is on local governments in rural areas.

Sambandam – Thanked Mr. Comeau for the clarification.

Johnson – In the process of creating the framework for the Report would it be beneficial to reach out to the Engagement Subcommittee of the Planning Committee to gather contact information for the regional areas mentioned by Mr. Abeyta and Mr. Ulses.

Sambandam – Asked Deloitte if it is possible to identify what zip code the responses came from to identify which areas of the state had the lowest response rate.

Glanzer – Can look at this to see if it will be of value in terms of representation. Can make general comments about agencies and different levels, municipalities, counties, state agencies or others, and present at the next Report Subcommittee meeting.

Sambandam – What is the data saying based on what has been collected so far? This would be a good starting point and can acknowledge that there is more work to do in the report.

Glanzer – Can have qualifiers. Certainly should take every opportunity to get more input moving forward, particularly in areas like localities and municipalities, where the responses did seem low, maybe there is an opportunity to ask for more input while completing the report.

Sambandam – Perhaps coordinate with respective organizations as they are going through their budget cycles. Try to identify location of the chokepoint to get entities to complete the assessment.

Abeyta – Agrees with the need to stand on true data points currently available, but add that work is ongoing to engage these different entities to help gain a better understanding because the digital gap is so vast within the state. Nothing specific, but that engagement efforts will continue in the rural areas that did not respond to help them better understand or become better educated with respect to the process.

Sambandam – Good discussion and input which can be incorporated into a reporting mechanism which will be more acceptable to the Legislature and the Executive Branch for them to make policy decisions, in terms of funding or workforce development plan to address this.

Johnson – Will make sure this is addressed in the Report. Would be smart to continue to work with the Engagement Subcommittee of the Planning Committee to continue gathering information.

7. Options for Cybersecurity Planning Committee – Todd Baran

Baran - Believes the objective for this discussion would be to ruminate on the options presented at the joint meeting and return with a recommendation. Those options being:

a). A legislative fix.

b). Some type of alignment between the two Committees moving forward, in which the roles and responsibilities with respect to preparing the Cybersecurity Plan are somewhat shared.

If there are any questions about this he is available. Believes information

presented at joint meeting is sufficient to begin this discussion.

Sambandam – Asked if there were any questions or comments from anyone.

Gutierrez – Not seeing any hands on Zoom, however, Mr. Mantos is present at the in-person and he does have questions or comments. Let Mr. Mantos know that Mr. Baran is available for questions.

Mantos – His impression was that the intent had been for the work of the Planning Committee to be complete with submission/acceptance of the Cybersecurity Plan, which it appears now may not be the case due to terms in the NOFO, which seem to indicate that a Planning Subcommittee is required in order to participate in certain events, in which case the Cybersecurity Planning Committee may need to continue. Would like to see the work of the Planning Committee transition to the Office of Cybersecurity, to whatever extent possible, and the Planning Committee standing down if possible. Perhaps the Plan Subcommittee of the Cybersecurity Planning Committee would become that entity and transfers to be a Subcommittee of the Office of Cybersecurity. Very unsure how this could be accomplished. Asked Mr. Baran to explain what the constraints are and if he had any suggestion as to what the correct course might be.

Baran – Recognizes that the resources available to staff these Committees and do this work are scarce. Having two committees with such substantial overlap in one area does not seem to be a wise use of those resources. A legislative fix that would ensure that the Cybersecurity Advisory Committee has the membership that aligns with the NOFO is probably the most efficient process. However, there may be a desire amongst the members of the Planning Committee to continue to have a voice and participation in this process, which is for them to discuss internally and bring forward. From a pragmatic perspective a legislative fix is probably the best.

Mantos – Understands that Report Subcommittee of the Advisory Committee will invite some members of the Cybersecurity Planning Committee to join them. Two are already part of both and some other names have been suggested such as Dr. Liebrock. With appropriate representation in this Report Subcommittee then they could decide how to proceed. Stated he suspects it may be as Mr. Baran has suggested, a legislative fix so that the Advisory Committee picks up the responsibility of the Cybersecurity Planning Committee, which then would disband.

Baran – If even that fix is implemented there would be nothing to prevent this Committee from inviting current members of the Cybersecurity Planning Committee as advisory members to this Committee.

Mantos – Could be an issue with the bill which specifically states membership

requirements, how they are appointed, etc. Could join as non-voting members which may solve the issue.

Baran – This is what he was suggesting, that they would be non-voting advisory members, which is allowed by the current statute.

Johnson – This is what is happening with the Report Subcommittee. These individuals are being invited as non-voting members.

Mantos – Agrees this is the way to proceed. Let them come to a consensus and make recommendations for any legislative changes and let the Cybersecurity Planning Committee stand down. Asked Mr. Sambandam if this sounds agreeable.

Sambandam – Agrees. Will yield to the legislative experts in providing the necessary consult for the Committee and to him in order to navigate through this and come to a conclusion.

Mantos – Thank you. This was all he had for comment/discussion.

8. Public Comment

Ms. Jacci Gruninger, the Executive Director of the Los Alamos Senior Centers, is attending the meeting today because they experienced a security breach recently which resulted in wire fraud and cybercrime, which they are currently addressing. In light of this it had been suggested to her that she seek out this Committee to inquire about grant application for funding to improve the security of their system. Her organization's situation is unique as they are a non-profit funded by state grant funds as well as county funding, but not directly funded by the county or the state. Not seeing nonprofits in the list of entities included in this work. Will there be a place for nonprofits to receive funding to boost their cybersecurity?

Comeau – Nonprofits and private sector entities are not eligible recipients or sub-recipients. However, there is an annual grant program called the Non-Profit Security Grant Program, and he put a link to this in the Zoom chat. He also put his email address in the chat as he may be able to provide Ms. Gruninger with some additional information. Noted that one of the steps is for non-profits to reach out to the state administrative agency, noting that Ms. Gutierrez would be the point of contact for that and would be able to provide more information about this grant program. The link he provided will give more information and he offered to help with some of the details. He stated that the program for the current year has closed, however, there will be another one opening in the Spring of 2024.

Gruninger – Thanked Mr. Comeau.

Sambandam – As an abundance of caution asked if law enforcement had been

contacted and if not information on this can be provided. This should also be reported to the State Attorney General.

Gruninger – This was reported to the FBI and is trying to connect with the Secret Service.

Sambandam – Thanked her. If this is wire fraud the Secret Service should be able to handle this.

Offered help with creation of policies, where to obtain cybersecurity awareness training, things of that nature, resources which would be available at no cost.

Gruninger – That would be very helpful for her staff and the board of directors.

Gutierrez – Added her email to the chat in Zoom for Ms. Gruninger. Happy to coordinate anything she might need.

Not seeing any further hands up for Public Comment.

9. Adjournment

MOTION Mr. Johnson moved to adjourn, seconded by Mr. Ulses. There being no objection and there being no further business before the Committee the meeting adjourned at 3:13 p.m.

DocuSigned by:
437214FBE82C453...

Raja Sambandam, Committee Chair, State CISO