

CYBERSECURITY ADVISORY COMMITTEE

Hybrid Meeting

In-Person, NM Gaming Control Board
4900 Alameda Blvd, Albuquerque, NM 87113
Virtual via Microsoft Teams

Thursday, April 3, 2025, 2:00 p.m. MDT

1. WELCOME AND CALL TO ORDER

Ms. Gutierrez called the meeting to order at 2:05 p.m. and welcomed everyone to the meeting.

ROLL CALL

MEMBERS PRESENT

Raja Sambandam, Chair
Logan Fernandez
Jason Johnson
Dr. Lorie Liebrock
Sueanne Athens

Charli Hannoona
Josette Monett
Todd Ulses
Cecilia Mavrommatis

MEMBERS ABSENT

Robert Benavidez
Kenneth Abeyta
Clinton Nicely

Seth Morris
Danielle Gilliam

OTHERS PRESENT

Melissa Gutierrez, Cybersecurity Project Mgr.
Todd Baran, DoIT General Counsel
Bryan Brock, DoIT Counsel
Dan Garcia (OCS), Flori Martinez, (DoIT), Heather Sandoval (DoIT), Todd Glanzer (Deloitte),
Joshua Yadao (Deloitte), Cassandra Lynn Brown, Gavin Lujan (DGF)

2. APPROVAL OF AGENDA

MOTION Ms. Gutierrez called for a motion to approve the Agenda. Dr. Liebrock so moved, seconded by Ms. Mavrommatis. There being no opposition, the Agenda was approved.

3. APPROVAL OF MEETING MINUTES

MOTION Ms. Gutierrez called for a motion to approve the minutes from the October 3, 2024 meeting. Ms. Athens so moved, seconded by Ms. Mavrommatis. There being no opposition these minutes were approved.

MOTION Ms. Gutierrez called for a motion to approve the minutes from the October 22, 2024 meeting. Ms. Athens so moved, seconded by Mr. Ulses. There being no opposition these minutes were approved.

MOTION Ms. Gutierrez called for a motion to approve the minutes from the October 28, 2024 meeting. Ms. Athens so moved, seconded by Ms. Mavrommatis. There being no opposition these minutes were approved.

4. Action Items - None

5. Updates from State CISO – Raja Sambandam

a. Legislative Update

SB254 did make it through due process. There was no opposition on the Senate side with completion of two Senate committee sessions and one Senate floor session. It was then assigned to the House Judiciary Committee, which did not have time to hear it, so it died in this Committee. Chair Sambandam stated that he is unsure if this will be brought forth in the event of a special session, but preparations will be made in anticipation of this, however, these changes will definitely be addressed in the next regular session if not considered in a special session.

Multiple other bills were introduced touching on cybersecurity for funding, as well as multiple memorials and bills considered related to artificial intelligence. The process regarding which ones have passed and will be signed by the Governor is still underway. Once these bills are signed he hopes that a summary can be provided with respect to those activities at the next Committee meeting.

b. Federal Policy Changes

Chair Sambandam stated that there are multiple federal policy changes taking place but those most closely related to cybersecurity are:

i). MS-ISAC services have been cut. This means potential impact to FEMA, DHS through CISA, etc. Any offensive posturing or even defensive posturing in terms of threat alerts and things of that nature are going to have some impact. Efforts are being made in coordination with CISA and Homeland Security to determine what these impacts would be, however, at this time it is known that MS-ISAC and the work they have been doing with all 50 states and the territories has been impacted.

Chair Sambandam asked if there were any questions regarding his report thus far. There were none.

ii). There is also the possibility that other similar ISACs which provide some cyber related functions, such as election ISACs, could also be impacted, but nothing has been determined at this time.

Chair Sambandam added that these policy changes are being closely monitored and he will keep the Committee advised.

Chair Sambandam again asked if there were any questions. There were none.

6. Engagement Subcommittee Updates & Recommendations – Robert Benavidez

Ms. Gutierrez noted that Mr. Benavidez is not in the meeting today and that the next active member of the Subcommittee present is Dr. Liebrock. Ms. Gutierrez stated that she did not believe Dr. Liebrock was prepared to describe the Subcommittee's activities and therefore asked that she be allowed to address this item by permission of the Chair and Dr. Liebrock. Chair Sambandam and Dr. Liebrock agreed that Ms. Gutierrez should give the Subcommittee updates.

a. Project 1 – Governance and Planning (Policy Development)

The Subcommittee has been working to determine priorities and has partnered with the Office of Cybersecurity to develop a larger library and has joined that office in their

initiative for state agencies to build on this to bring policy updates for local entities, higher education, etc. This is still in early development but is going very well. Ms. Gutierrez asked if Mr. Baran had anything to add.

Mr. Baran stated that the goal of the project is to create a policy library which for this Committee will provide a foundation for selecting policies that the Committee would want to establish as the minimum standards or controls for local governments. The first set of template policies to be developed will be for use by executive agencies and once those are in place this library will be modified in order to tailor it for local governments. A contract for this will soon be in place and the hope is to see significant progress by the end of the fiscal year.

b. Project 2 – NCSR Completion – Deloitte

Ms. Gutierrez asked Mr. Glanzer from Deloitte to provide this update.

Mr. Glanzer gave an outbrief of the NCSR, reviewing a presentation of the project which he screen-shared. He noted that the input into the system is sponsored by CISA and CIS, but the completion of the project is up to the participating entities. This project was to facilitate 22 entities across the state in completion of this within the open period, which is November to February; however, the project here was not begun until January. He reviewed the project timeline, which is normally November to February, noting that all entities were able to complete the project by the end of February. He stated that some of the information obtained through this project revealed that a majority of the entities are looking for more standardized approaches through policies and procedures regarding cybersecurity, across different control families, so they can effectively provide this governance to their organizations and other parts of their entity structure, as well as being able to use this to promote compliance, awareness and support from their structures. This will also help inform the work being done through this Committee toward the annual cybersecurity report, as well as providing information for the Plan updates moving forward and, through the Engagement Subcommittee, how to continue providing information with respect to improvement areas that will make the most impact across the state.

Mr. Glanzer shared the following project recommendations: 1) start the project or pre-work in November and 2) determine how to formalize capture of the information being submitted by individual entities in a reporting format that will better effect the statewide planning process, i.e. collection of survey results, proper controls in place to prevent unintended release of information, etc.

Mr. Glanzer concluded by reporting that the project was completed on time, and that it favorably impacted the entities involved and will inform future processes. Mr. Glanzer then asked if there were any questions or comments.

Chair Sambandam asked for clarification of the five areas Mr. Glanzer referred to in his report and whether these were the five areas of CSF; identify, protect, defend, respond and recover. Mr. Glanzer confirmed that this was correct and this coordinated with being able to extract standardized questionnaires and other resources.

Ms. Gutierrez recognized the amount of work and success of this project, noting that the Planning Committee was able to turn this around in “about a short month”, from issuing

the RFQ to identify a vendor for this project, which began in October with closure of the RFQ in the middle of November, with vendor selection occurring at the end of November/first week of December. She added that state procurement is not easy, especially during the holiday season, however, this was contracted and completed for Deloitte to start in January and they were able to get all 22 entities completed by February 28th. She stated that this was also the first project for the Planning Committee, which was very successful, with completion on time and under budget, and offered her congratulations to the Planning Committee and all the individuals involved in this project.

Ms. Gutierrez gave a reminder that all of these projects are funded through the State and Local Grant Program, the SLCGP, and these first projects are being funded with Year-1 funding, with much to look forward to with Year-2 and Year-3 funding. These projects have been a great start.

c. Project 3 – Vulnerability and Attack Surface Management

Ms. Gutierrez explained that this is the scanning project, with 25 entities currently onboarded, with two still pending due to local technology and infrastructure upgrades needed. The Securin team is providing services to those entities to get them onboarded. With the savings realized in Project 2 the amount for Project 3 has been increased, so for entities covered in Project 3, services for VMaas and ASM are being extended through June 30, 2026. She asked if there were any questions. There were none.

d. Project 4 – Cybersecurity Training

Ms. Gutierrez reported that licenses for KnowBe4 were procured for entities applying for this service. She added that there were a few entities already receiving services through their county affiliations and these opted out and are not using these licenses. This has resulted in there being a balance of remaining licenses available. She noted that she has sent out an email to all members of this Committee as well as the Planning Committee regarding a short window of opportunity for this project, which will end on April 30th, for entities to apply. These applicants will be onboarded as quickly as possible to start using the previously procured licenses. She estimated that there are 1,500 licenses available. There is a remaining balance under this project which will enable funding of additional licenses, if more than 1,500 applications are received. She asked if there were any questions. There were none.

e. Project 5 – Cybersecurity Workforce Development Planning

Ms. Gutierrez stated that the Procurement Subcommittee developed an RFQ which was issued in mid-February and closed on March 12th. This Subcommittee is currently reviewing all of the RFQ responses to determine their recommendation to the full Planning Committee.

Ms. Gutierrez commented that all of these projects are moving forward, and that the Engagement Subcommittee and Planning Committee are doing great work getting these projects moving.

Ms. Gutierrez asked if there were any questions related to Agenda Item 6.

Chair Sambandam asked if the announcement had been sent out about the additional

application period for the training licenses. Ms. Gutierrez stated that yes, the email had been sent out and those receiving the email are encouraged to share the information, however, applicants must be a local government or county government, those types of government entities. Unfortunately, this does not cover private entities. She noted that there is an initiative to get water systems onboarded, so if there are local entities with a water or wastewater system, those are being accepted as well. Chair Sambandam thanked Ms. Gutierrez for the clarification.

Mr. Johnson thanked the Engagement Subcommittee and Ms. Gutierrez for all these updates. Lots of good work. Ms. Gutierrez thanked Mr. Johnson.

7. Discussion – Meeting cadence & attendance requirements for committee members

Ms. Gutierrez asked Mr. Baran to describe this in more detail.

Mr. Baran explained that this concerns the functioning of the Committee and its ability to assemble and maintain quorum, noting the challenges that have occurred in this respect. He has been asked to bring in some perspective from the NMDOJ. One of the things that many boards and commissions do is establish requirements for member attendance, and if members do not meet these requirements there can be consequences. For boards and commissions which have some control over appointing members, as in filling empty seats, some of these have elected to have a requirement that if a stated number of meetings are missed the member loses their seat. However, this particular Committee has statutory positions, certain wild-card/flexible positions, some positions that are allowed to have designees and some that are not, so a “one size fits all” kind of rule will not work, but there could be some type of resolution to set attendance expectations and consequences. For example, a provision that states if two meetings are missed in a row, or two out of three meetings, the Committee will send a notification to whoever the appointing authority is for that member, and request a new appointee or a designee; something to ensure that the appointing entity is aware of potential problems with attendance. Mr. Baran opened this up for discussion to see if existing Committee members shared these same concerns and to see if Committee members had experience with this from other boards and commissions. If this discussion begins to coalesce around a particular approach to this, then work could begin toward developing a written policy for future discussion and potential action. He then opened the discussion to the Committee members.

Chair Sambandam asked if this is to discuss continued participation. Mr. Baran replied that this is correct.

Ms. Athens stated that she would support placement of some sort of policy for understood accountability. She also agreed that there are different requirements for some positions, which would have to be considered, such as notification to the agency Secretary, etc., depending on the status of the position.

Mr. Johnson agreed with the idea of a policy which elevates and raises awareness of the criticality of Committee membership and meeting attendance, and would support such a policy.

Mr. Baran asked what a reasonable policy would entail.

Chair Sambandam recognized the requirements for some members to be from a particular agency. In light of this, would it be possible for the Committee member to delegate a “stand-in”

for a particular meeting, such as in the instance of last minute unavailability, i.e., medical situation, etc.

Mr. Baran stated that this should certainly be explored, as in many instances the authority to appoint a designee is situational, so if it is a last minute thing you can generally select someone else to act in your place, but for some Committees, particularly ones that have a lot of appointees from the Governor's office, the Governor's office likes to vet the designees. If this is something the Committee would like to explore they can work with the Governor's office to see how they would like to approach it for this particular Committee. They may be fine with having a situational designee on a sporadic basis, but if this becomes more than two or three meetings a year, then they may want to have a voice in selecting the designee. This is definitely a conversation that can be pursued.

Chair Sambandam asked Mr. Baran to verify that the meeting frequency for this Committee is every two months. Mr. Baran stated that this is correct. Chair Sambandam stated that this would mean approximately six meetings per year. Mr. Baran stated that this is the minimum, but as things move forward in the policy development process more meetings may be necessary. Chair Sambandam asked if today the concept is just being introduced. Mr. Baran replied that this is correct.

Chair Sambandam asked if the approach is for Committee members to consider all these things and bring their ideas to the next Committee meeting. Mr. Baran replied that this is correct.

Ms. Athens agreed that it would be important to consult the Governor's office as mentioned by Mr. Baran. She stated that in a situation such as hers, where she has been designated by the agency Secretary, if she could not attend she would expect and would arrange with her agency Secretary to attend, and this kind of approach would seem to make sense for other agencies as well. Mr. Baran agreed.

Chair Sambandam asked if the concept could be to have a primary and a secondary designee, which would both be vetted. Mr. Baran agreed that this is a good proposal and perhaps this would alleviate pressures with Committee members knowing they have a vetted designee that they can access, which should help with maintaining quorum, and should prevent absences from accumulating. Chair Sambandam commented that this could be a good approach, having a primary and secondary designee, at least to begin with, having a structure, a level of awareness, support and engagement.

Mr. Baran asked Ms. Athens how this concept resonated with her. She responded that this sounds good.

Mr. Ulses asked how appointed positions would be handled, such as his position, being appointed by the New Mexico Counties. He asked if the appointing bodies should be informed that their appointee is not participating so they can re-appoint the position. Chair Sambandam replied that this probably would not be best, but his recommendation would be to have a secondary appointee in case the primary is not available.

Mr. Baran stated that there could be two approaches running concurrently. There could be the option to have a standing designee, as well as a process in the case of continued absences, despite having the back-up designee, that this is brought to the attention of the appointing

authority.

Chair Sambandam stated that he would be in agreement with whatever the Committee recommends.

Mr. Ulises stated that the appointing authority should be notified, but he was unsure if this was an action item or just discussion today.

Chair Sambandam replied that this is just discussion today, no action required. He then asked if there was further discussion of this item.

Mr. Baran stated he would start the conversation with the Governor's Boards and Commissions team about having the standing designees and once feedback is received from that office he can put together a proposed policy which incorporates that option and the notification option for continued absences for further discussion and potential action in future meetings. He then asked if this was an acceptable path forward.

Chair Sambandam stated that from the Executive side of the house this is a workable approach. He then asked if other Committee members had further input.

Mr. Ulises stated that he was agreeable with this approach.

Dr. Liebrock stated that this is a good starting point.

Chair Sambandam asked Mr. Baran to move forward with gathering the necessary information for possible policy formation to be presented at the next meeting. Mr. Baran replied that he will do so. Chair Sambandam also asked Mr. Baran to consider the impact of the legislative session calendar on Committee meeting schedules during the January to March interval. Mr. Baran agreed to do so.

Mr. Johnson also mentioned being aware of other sensitive times during the year, such as September/October when annual reports are due in the Governor's Office, in addition to the legislative sessions. Chair Sambandam responded that this is a good point to consider. Mr. Baran agreed that awareness of these situations and planning around these will alleviate obstacles moving forward.

Mr. Baran stated again that he will pursue the work on this and report back to the Committee.

8. Discussion – Committee/OCS Policy Promulgation Processes

Mr. Baran explained that the law states the CISO can issue orders to enforce the Committee's policies. This discussion is for how this will be operationalized. He asked Mr. Brock to present this item as he has been working more closely on this issue.

Mr. Brock thanked Mr. Baran for his explanation and agreed with this. He stated that the Cybersecurity Act contains language describing the CISO's authority and the Committee's authority, however, it is not very clear. Because of this there has been discussion amongst legal counsel concerning the extent of this authority and how it should be applied. He reiterated that this is a discussion item, not an action item, and is intended to raise the Committee's awareness of appropriate background activity. The authority of the CISO seems relatively clear with regard to certain parts of the Cybersecurity Act, with certain duties and

powers, the strongest being, in his opinion, the ability and authority to engage in rulemaking, to set certain minimum security standards and other protocols which the persons and entities over which he has jurisdiction must follow. There are other powers and authorities which are not written as a model of clarity, but can be easily interpreted as the CISO's authority to develop cybersecurity controls, certain IT security standards and perform certain monitoring and detecting activities, those sorts of powers. The more complicated areas, as alluded to by Mr. Baran, involve the ability to enforcement of these orders and policies. He noted that generally in state government, when an agency is given certain powers and duties, the language used is always the same, very consistent, coming out of the Legislature, which gives the power and authority to conduct rulemaking and to issue orders, and also very clearly give the authority to enforce the rules, orders and policies that usually a cabinet secretary is authorized to develop. This same language does not currently exist in the Cybersecurity Act. An argument is that the Cybersecurity Advisory Committee actually has the authority to voice its opinion on enforcement matters and then, arguably only then, does the CISO have the authority to issue an order to enforce the thoughts of the Advisory Committee. He stated that a good outcome of these discussions would be to do more work toward developing a policy regarding the CISO's authority to issue rules, orders, and policies, and an agreement on the enforcement authority of the CISO regarding these elements. Mr. Brock then asked Mr. Baran if he had anything more to add.

Mr. Baran gave an example of what this might involve. Say that a new type of control is identified for managing a particular risk and the CISO believes that this control should become a minimum standard for definitely the executive agencies, and preferably statewide, and in the best interest of these agencies. What would the process be for getting some type of directive out to impose this policy, or mandate the implementation of this control? Would this need to go through the Committee for their approval of the policy and then would the CISO have any unilateral authority to mandate the implementation? What should this process look like? These are the kinds of questions that need to be answered and the Committee is being asked for their input.

Ms. Athens stated that she believed the intention of the Advisory Committee was to perform this function. If certain controls or requirements are to be imposed at the state level this Committee would be in the position to advise, suggest and provide feedback regarding potential impacts to the state agencies or local public bodies. She believed that the imposition of additional controls statewide might conflict with other functions or have a cost involved that would be prohibitive for some organizations.

Mr. Baran asked if having an issue brought to the Committee and having the Committee promulgate a policy, even if it is a simple resolution, should this be implemented on a statewide basis, which would empower the CISO to enforce this policy? Is that what Ms. Athens is suggesting?

Ms. Athens stated she believed so, however, she has not been on the Committee very long, but this was her understanding of the original intentions.

Mr. Baran then asked if the CISO would have the ability to act unilaterally as the policy maker for executive agencies and mandate the implementation?

Ms. Athens asked if this would be after discussion or simply a unilateral authority at some level.

Mr. Baran stated he was suggesting this as one option, which may not be how the Committee envisions this working, restating that the goal of this discussion is to figure out where the boundaries are and get everyone on the same page in order to build a process around the requirements for acting.

Ms. Athens stated that if there would be a critical or high issue, which needs to be addressed immediately, there should be unilateral authority to act, however, if an issue were not in this realm then discussion and evaluation should occur.

Dr. Liebrock asked if Ms. Athens was referring to issues involving the Executive Branch only, not the entire state.

Ms. Athens asked Mr. Baran if he was referring to just the Executive Branch or the whole state.

Mr. Baran replied that his last hypothetical reference was referring to just the Executive Branch, but the discussion ended up referring to whole of state.

Dr. Liebrock noted that even when there is some urgent incident anticipated there could still be major negative consequences statewide from an immediate order which cannot be complied with, which is a concern. However, the CISO is far more integrated and tied into the Executive Branch, and if the Executive Branch gives them that authority then the Committee may not have standing to interfere with an emergency response within the Executive Branch, but with respect to a statewide situation this would be a concern.

Mr. Baran asked Dr. Liebrock if she would prefer to see these issues brought to the Committee before directives are issued, even in a fairly emergent situation.

Dr. Liebrock replied that yes, in part, because the Advisory Committee should be helping get the response out to non-state agencies concerned, having this executive order coming down, which is potentially a very large impact, especially in the case of schools for example, having to implement something in an urgent situation.

Mr. Baran then re-stated that the process would be the same for all types of directives for local entities and there may be a different process and the CISO may have different authorities with respect to executive agencies, but the Committee should be in the loop with respect to decisions that will impact local governments.

Dr. Liebrock stated that she is just asking questions at this point.

Mr. Baran restated the purpose of this discussion and the perspectives that have been articulated are those that need to be examined.

Mr. Johnson noted that the previous agenda item could influence these situations, that is meeting cadence and attendance, where if there were a critical event the Committee would need to convene quickly, probably go into closed session, and formulate recommendations to be issued in a timely fashion. He agreed that the CISO has a closer relationship to the Executive Branch, at the executive agency level. He stated that this should be discussed, vetted and published as there have been issues in the past with a critical alert, and having the proper policy(ies) in place could prevent untoward or unnecessary disruptions to state

functions and state business, however, these actions should be communicated first, unless the event is exceedingly critical.

Mr. Baran stated that in the event of an emergency the constraints of the Open Meeting Act do not apply. A quorum is still needed before any action could be taken by the Committee, but notice is not required, etc., so there is much more flexibility in an emergency situation.

Mr. Fernandez noted that in his role as CISO for the judiciary his concern is how the term “statewide” is being defined. He shared that the stance of the judiciary has usually been that there should be a separation of powers, what one side can dictate to another side and what they are able to do in the event of emergencies. He suggested that there be a definition of what “statewide” refers to and also that “emergency” should be defined to better refine the processes related to the powers designated to the CISO.

Mr. Baran stated that the purpose for today’s discussion was to begin the conversation and this will probably have to be revisited a couple of times before any “pen to paper kind of policy is promulgated”. He thanked everyone for their input and stated again that this will be revisited at a future meeting.

Ms. Gutierrez asked if Mr. Baran would welcome any correspondence from Committee members for review on this subject. Mr. Baran stated he would absolutely welcome this. Ms. Gutierrez asked members to send emails to her and she will make sure these are examined and as Mr. Baran has suggested there will be an opportunity for further discussion and review.

Chair Sambandam offered an explanation of “change management” in other types of business, such as banking, wherein emergency action has to be taken for the survivability of the operational process, the decision is made “on the fly” and is then reported back to the change board or change management committee, so those type of practices currently exist and are considered best practices.

Mr. Baran suggested that a policy addressing the decision making process can include the “circuit breakers and contingencies” necessary to ensure as much consistency is maintained as possible while recognizing that certain emergencies require immediate action. Chair Sambandam agreed.

Chair Sambandam stated that he believes the federal government intends to “ramp down” their involvement in offensive and defensive cyber postures and will let the states assume responsibility for these areas. Because of this there should be efforts to have structures in place to enable timely reaction to major situations. This should also include reporting as a standardized practice. Mr. Baran agreed with Chair Sambandam, and that this was part of the impetus for this discussion, the concern or recognition that this responsibility will be moving to the states.

Ms. Gutierrez stated that this item will also be included as an Agenda item for the next meeting. If Committee members will be emailing ideas or thoughts to her, she reminded them to make sure the message is sent only to her and not to all Committee members, as a precaution against a rolling quorum issue.

9. Public Comment

Mr. Ulises asked if there were any concerns or any information about SLCGP funds being

clawed back due to the change in federal leadership. He noted that he had received information from NACo Tech Xchange about a committee that would be meeting regarding that grant.

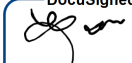
Ms. Gutierrez responded that she has not received any correspondence regarding claw back of any of these funds or anything related and they are operating with status quo for now. She stated that there will be a meeting with CISA and FEMA in May and hopes to learn or know more at that point. She added the state received the third year award in mid-January, and actually more funding was received as there are fewer states participating, approximately \$20,000.00 more. She noted that they are receiving some correspondence and having good communication, but nothing about no future SLCGP grant dollars.

Chair Sambandam reported that NASCIO has made a concerted effort, along with state CISOs and the Secretary/Treasurer of NASCIO, from Utah, and met with one of the congressional subcommittees and provided the evidence for this funding to be continued, which was a huge success. He shared that NASCIO is fully in support of all the legislative “pushes” to have this process continue. He noted that the federal fiscal year does not begin until October 1st, so he does not anticipate any major action regarding this, unless there is a specific claw back through some other legislative action in the interim. After October 1st another budget cycle will begin and at that point there could be some impact to future year funding, so the potential does exist. He reported that all parties are working toward the rationale and justification that more funding actually needs to be added to this program.

Ms. Gutierrez thanked Chair Sambandam for this information. She then asked if there was any further public comment. There were none.

10. ADJOURNMENT:

MOTION Ms. Gutierrez called for a motion to adjourn. Mr. Johnson so moved, seconded by Dr. Liebrock. There being no objection and no further business before the Committee the motion passed and the meeting adjourned at 3:25 p.m.

DocuSigned by:

437214FBE82C453...

Raja Sambandam, Committee Chair, State CISO