CYBERSECURITY ADVISORY COMMITTEE
Hybrid Meeting
Thursday, August 7, 2025, 2:00 p.m., MST

1. **Welcome, Call to Order and Roll Call – Renee Narvaiz**

Ms. Narvaiz called the meeting to order at 2:04 p.m. and introduced herself. She welcomed everyone to the meeting and reviewed general procedures for the online portion of the meeting.

MEMBERS PRESENT

Raja Sambandam, Chair
Jason Johnson
Logan Fernandez
Seth Morris
Charli Hannoona
Dr. Lorie Liebrock
Sueann Athens (Sarita Nair)
Danielle Gilliam
Cecilia Mavrommantis/Brian Salter

MEMBERS ABSENT

Josette Monette
Kenneth Abeyta
Todd Ulses
Robert Benavidez
Clinton Nicely

OTHERS PRESENT

Manny Barreras, DoIT Cabinet Secretary
Renee Narvaiz, DoIT PIO
Melissa Gutierrez, Cybersecurity Project Mgr.
Todd Baran, OCS General Counsel
Dan Garcia (OCS), Flori Martinez (OCS), Bryan Brock (OCS), William Campos (Deloitte), Joshua Yadao

2. **Approval of the Agenda**

MOTION: Ms. Narvaiz called for a motion to approve the Agenda. Mr. Johnson so moved, seconded by Mr. Morris. There being no opposition, the Agenda was approved.

3. **Approval of June 5, 2025 Meeting Minutes**

MOTION: Ms. Narvaiz called for a motion to approve these minutes. Mr. Hannoona so moved, seconded by Mr. Johnson. There being no opposition these minutes were approved.

4. **Action Items: None**

5. **Updates from State CISO – Raja Sambandam**

a. Order from State CISO

Mr. Sambandam stated this order was issued to identify a liaison for reporting any breeches or incidents to the Office of Cybersecurity. He reported that some feedback has been received and the office is currently working through those. He asked Mr. Baran if he had any additional comment regarding this.

Mr. Baran explained, for context, that this is the order which implements the statute requiring the CISO to establish a statewide cybersecurity incident notification process, so this order is applicable to all political subdivisions and all public bodies in the State of New Mexico, requiring notification of any incident with the threshold of any entity accessing data which they should not have acces to, or if anyone has a permission that they should not have within any state system. In addition to notification OCS will triage with the reporting entity and will provide support if possible. If OCS does not have the resources or jurisdiction to provide support the office will stay involved to maintain situational awareness, as well as keep the rest of the State informed and aware of risks. Mr. Baran added that one report has been received and the process went very well.

b. MS-ISAC
Mr. Sambandam reported that this was federally funded in the past using a Homeland Security grant and managed by federal Homeland Security and then later by CISA when that was created. However, the federal government has stopped funding this program, so it is becoming a member paid service. This situation has been examined in the process of scaling up the State's attack surface management, which provides many services, such as MDBR, and while these features are currently built into the program and they have onboarded all entities who are complying as voluntarily as possible, there are many entities yet to be onboarded onto this program, so there is a need to provide continuity to MS-ISAC at least until all entities can be onboarded onto the State ASM program. The cost of this service for New Mexico, based on the population formula provided, will be approximately $150,000.00. OCS will pay for this, as this will provide services not only to the State IT ecosystem but will also provide election security, updates to the Secretary of State and many of the County Clerks. OCS made this decision due to the critical nature of this situation, and the purchase request is in process. This will be valid for one year. He added that it appears that the federal government is shifting more of the responsibilities for these types of programs to the states, and more of these processes are becoming member paid services. He again stated that OCS will pay for this service for one year until all entities can be onboarded to the State platform for ASM and threat intelligence.

Mr. Sambandam asked if there were any questions or comments and there were none.

c. 2025 Federal Grant NOFO
Mr. Sambandam reported that the NOFO for the SLCGP grant has been issued and the criteria is being examined, stating that there is a less than two week response period, with the deadline being 08/15/2025. He added that similarly the NOFO for the Homeland Security Grant Program was issued, also due by 08/15/2025, which included many terms and conditions. He asked Mr. Baran or Ms. Gutierrez if they would like to address the details of this.

Mr. Baran stated that all federal grants now have a standing set of conditions which obligate the State to cooperate with federal immigration enforcement initiatives, including housing detainees and participating in sweeps. This is awaiting a response from the Office of the Governor regarding how to proceed with respect to these conditions and issues. The early indications are that OCS will continue to apply for these funds and accept these funds under protest, but exactly what this will look like is yet to be determined.

Ms. Gutierrez stated that this is the last year of the 2025 federal grant, which is approximately $2 million with a cost share of 40% from the state. She noted that the requirement for the grantee and the local entity that will apply for services or anything else from that grant is that they participate in the vulnerability scanning from CISA, which will require entities to onboard and have CISA scanning all of their vulnerabilities. She added that this is a free federally funded program, which means since it is included in the federal grant NOFO it is not an area that they will be making cuts to, such as MS-ISAC and NCSR which have had funding stopped.

Mr. Sambandam added that none of these grant programs can be used to subscribe for MS-ISAC, which was a condition updated in both the Homeland Security Grant program and the SLCGP, and so the reason for OCS deciding to pay for MS-ISAC.

Mr. Sambandam asked if there were any other questions or comments. There were none.

6. Annual Advisory Report – Deloitte – William Campos
Mr. Campos stated that Deloitte started work on the Annual Advisory Committee Report a little early this year in an effort to capture some of the initiatives that the Office of Cybersecurity has been doing. He reviewed that the original report in 2023 was more of a strategy and in 2024 there was more definition regarding what the initiatives would be for support of that strategy. This year's report will show that OCS has started to make progress on their own and will continue to support some of these services and initiatives with SLCGP funding, extending the outreach to entities which would not have

normally been able to participate. They have been communicating with various stakeholders to better understand how these initiatives have evolved over the last year and where they may be by the time the report is submitted in late October. He stated that this report is still in the very early stages, having completed about two weeks' worth of interviews and discussions with various stakeholders and OCS. A draft of the report will be prepared for sign-off and verification before proceeding to other high-level and executive portions of the report. This initial phase is so these items and initiatives will be included that provide continuity within the report from year two.

Ms. Gutierrez reminded the Committee that this report is due October 30th of each year and there is a report Subcommittee which will review and finalize the report before it comes to the full Committee. The hope is to have the draft of the report available to all Committee members by the beginning of October. She stated that the Report Subcommittee members are Jason Johnson, Clinton Nicely, Kenneth Abeyta, Todd Ulses and Robert Benavidez. They will be contacted for their input and the information they would like to see in this report. She noted that she had shared last year's report with the Agenda and other documents for today's meeting. If Committee members have questions or other items of discussion about the report she asked that they e-mail those to her.

Ms. Gutierrez asked if there were any other questions regarding the report at this time. There were none.

7. SLCGP Project Updates -

a. Project 1 – Policy Development – Todd Baran

Mr. Baran stated that work has been progressing with the vendor, Datapoint, over the last couple of months, on the set of template policies which will be put in place for use by executive agencies. These policies are intended to help entities satisfy the requirement of the CSF, which states the need for policies to be in place for certain cybersecurity controls. He noted that these policies are not the controls, but are the policies which will drive the development and implementation of those controls. He reported that there are currently 20 policies in the queue and drafts of those should be available within the next couple of weeks. At that point a fairly aggressive series of stakeholder engagements will be undertaken to provide feedback to Datapoint on these policies, which will be followed by another round of drafting and then a final review. He stated that, as had been discussed at a prior meeting, the concept is to go into a phase 2 after those policies are adopted for executive agencies, and then have this Committee review and modify these policies for the purpose of standing them up for the rest of New Mexico public bodies, as an advisory function. He explained the main substance of these policies will be fairly well established by the conclusion of the initial phase, so Advisory Committee members are encouraged to participate in the stakeholder groups and provide comments, with the idea that these may be adopted in whole or in part later on for use by other local governments, etc. He advised Committee members to watch for an invitation from Ms. Gutierrez to the stakeholder meetings, and encouraged any other interested parties to contact Ms. Gutierrez so they can be put on the invitation list as well as the list to receive the drafts.

Mr. Sambandam commented that this is in alignment with the cybersecurity strategy document outlines and that members of both the Advisory Committee and the Planning Committee will be working on this. He added that this is also in strategic alignment with what the Cybersecurity Act requires in order to meet minimum cybersecurity standards. He stated that he was happy to see this all coming together so well.

Mr. Sambandam asked if there were any questions. There were none.

b. Project 2 – NCSR – project closed (no updates)

c. Project 3 – ASM and VMASS – project ongoing (no updates)

d. Project 4 – Cybersecurity Training – project ongoing (no updates)

e. Project 5 – Cybersecurity Workforce Development Planning – Bryan Brock
Mr. Brock stated that the quotes received from various vendors far exceeded the budget for this project so OCS met with members of the Planning Committee and the decision was made to prepare a new RFQ, which was more focused and limited in its scope of work, and that OCS has prepared a draft which is almost ready for release. This draft is asking for a needs assessment, a statewide capabilities assessment, which is new, as well as a gap analysis with some high level remediation recommendations for the 19 public entities who have signed up to receive services. This draft will be issued as quickly as possible and will provide vendors approximately one month to review it and respond with new quotes. The RFQ will be published just as the previous one was, with the anticipation of receiving another good group of quotes.

In a related update Mr. Brock stated that internally OCS is very aware of the potential good results with a good workforce development plan, so the office is working independently to compose perhaps another RFQ for someone to provide those services for state government, which would be a much larger undertaking, and that the office does not intend to use SLCGP funds for this. He added that he felt this was worthy of an update as it will ultimately be a result of Project 5.

Mr. Brock asked if there were any questions or if there were any Planning Committee members who would like to comment.

Dr. Liebrock noted that the discussion at the last Planning Committee meeting revolved primarily around the existing capabilities around the state which need to be leveraged and it was felt the original RFQ did not address this, so the current approach will be a more targeted and efficacious way to use these funds and the Committee is excited about this.

Mr. Sambandam thanked Dr. Liebrock for her comments and added that the meeting she mentioned was a very productive session, looking forward to selecting the ideal vendor partner. He noted that some of this relates to policy decisions and these necessary data points can be provided to the appropriate policy makers in order to make cybersecurity a key piece of the workforce development through other state policy initiatives. He asked for confirmation of his observation from Dr. Liebrock, who responded in the affirmative.

8. **Member Comment(s) – None.**

9. **Public Comment(s) - None**

10. **Adjournment:**
MOTION: Ms. Narvaiz called for a motion to adjourn. Dr. Liebrock so moved, seconded by Mr. Johnson. There being no objections and no further business before the Committee the meeting adjourned at 2:32 p.m.

DocuSigned by:
437214FBE82C453...

Raja Sambandam, Committee Chair, State CISO