CYBERSECURITY ADVISORY COMMITTEE
Virtually Only Meeting
Thursday, October 2, 2025, 2:00 PM

1. **Welcome, Call to Order and Roll Call -** Renee Narvaiz
Ms. Narvaiz called the meeting to order at 2:12 p.m. and welcomed everyone to the meeting. She reviewed general procedures for the meeting and using the Teams platform.

Members Present

Raja Sambandam, Chair	Kenneth Abeyta
Jason Johnson	Charli Hannoona
Logan Fernandez	Dr. Lorie Liebrock
Seth Morris	Sueann Athens for Sarita Nair
Josett Monette	Cecilia Mavrommantis (Brian Salter)

Members Absent

Todd Ulses	Clinton Nicely
Robert Benavidez	Danielle Gilliam

Others Present

Renee Narvaiz, DoIT PIO
Melissa Gutierrez, Cybersecurity Project Mgr.
Todd Baran, OCS General Counsel
Manny Barreras, DoIT Cabinet Secretary
Bryan Brock (OCS), Flori Martinez (OCS), Dan Garcia (OCS), William Campos (Deloitte), Todd Glanzer (Deloitte), Patrick Torres (DOT), Shannen Barela (DOT), Jefferson Woodman (DOT)

2. **Approval of Agenda –** Renee Narvaiz
MOTION – Ms. Narvaiz called for a motion to approve the Agenda as presented. Ms. Athens so moved, seconded by Mr. Hannoona. There being no opposition, the Agenda was approved.

3. **Approval of Meeting Minutes -** Renee Narvaiz
MOTION – Ms. Narvaiz called for a motion to approve the minutes of the previous meeting. Ms. Athens so moved, seconded by Mr. Abeyta. There being no opposition these minutes were approved.

4. **Action Items – None.**

5. **Updates from State CISO –** Raja Sambandam
a. MS-ISAC
Chair Sambandam described how this was previously a federally funded project made available to states, local governments, K-12 and higher education, however, due to federal funding cuts to CISA and Homeland Security this service is now being evaluated to move to a paid funding model. This will mean that states and other users of the system will be contributing to replace the lack of federal funding. He added that the State of New Mexico made a state wide agreement in the past, which all parties participated in and became acclimated to it. Predominantly the malicious and domain blocking services were those which the State leveraged to be informed of any malicious domain which might be hitting state web sites or traffic from those domains which could be problematic. He stated that these services are outsourced to The Center for Internet Security, which primarily acts as the first line of defense for all incoming traffic, once the operable domains are added to their platform. This has been a very valuable service for local communities and especially the K-12 school districts. Given the fact that this is changing to a paid model the State of New Mexico will provide continuity, with the Office of Cybersecurity taking responsibility for this enterprise agreement. He added that this service is critical as it is used by counties, specifically pertaining to elections. Providing this continuity will eliminate individual agencies signing up for services. He stated that OCS has gone through the procurement process and is awaiting some clarity. Once this is obtained, which is expected in the next couple of

days, the agreement will be signed and the Office will move forward with this.

Chair Sambandam asked if there were any questions regarding this service. There were none.

b. STTC Meeting
Chair Sambandam noted that participation in the first meeting was not possible due to scheduling conflicts, however, he was able to attend the August and September meetings. The purpose for attending these meeting was to bring awareness about the Office of Cybersecurity, its personnel and its current and future functions. He added that the plan is to address funding requests, etc., at the next meeting. During the August and September meetings there was a request from one of the committee members regarding information about entities impacted, the reasoning behind an incident or breach, associated fiscal impacts, etc. The Office is now in the process of gathering as much information as possible regarding this request. He added that there was discussion about the participation of various entities into the program, how to better utilize funding and what is happening at the federal level regarding federal funding cuts and the potential government shutdown.

Chair Sambandam asked if there were any questions or comments.

Patrick Torres asked if an entity already has an MS-ISAC member account would they need to create a new member account. Chair Sambandam replied that he did not believe so, however, there is some account “clean-up” to do with respect to top level domains being monitored that are not current, such as state entities still listed under “nm.us” which need to be moved to “nm.gov”, etc., and other updates needed. This is part of the clarification being sought, but the current indication is that there will be no disruption in the existing service.

6. **Incident Response Plan – Status/Engagement –** Todd Baran
Included in item 7.

7. **Policy Development Project – Status/Engagement -** Todd Baran
Mr. Baran reminded the Committee that OCS is working on a Cybersecurity/Information Security Policy template library project with the goal to develop templates which agencies can use as a resource, customized to having a compliant set of policies that will reflect their IP environment. He stated that at this time they are engaging with stakeholders to review these policies, which will help the drafters of the templates understand if the policies are feasible, reasonable and pertinent to the state of IT in New Mexico in order to deliver an end product which will not require extensive customization or editing for agencies to put into use.

Mr. Baran noted that the second phase of the project will be taking the agency adopted templates and amending these for political subdivisions, which would be schools, HEIs, counties, municipalities and tribal governments. He added that, according to the vendor for this project, the more input received from these political subdivision sectors the less revision will be needed later on. He stated that they still have not received permission from the Cybersecurity Planning Committee to use SLCGP funding for this second phase, but he is confident this will occur, however, these funds can be used for other initiatives if the amount of work for phase two can be minimized. The vendor is also asking for more engagement from this Committee in the stakeholder meetings to increase input into the policy drafts, as agency engagement so far has been a little disappointing. He encouraged Committee members to review these policies and add their feedback by contacting Ms. Gutierrez, who will provide invitations to the meetings and a link to the documents.

Dr. Liebrock asked if the MS-ISAC funding being provided by OCS will cover universities. Chair Sambandam responded that yes, it will. He added that the SLCGP funding criteria was revised due to funding cuts, so the NOFO now clearly states that SLCGP funding cannot be used for that subscription service, so the necessary funding was provided by the State to keep the service going.

Mr. Torres asked if the project presented by Mr. Baran is related to the Trust Cloud process previously done. Chair Sambandam stated that it is not, this is a separate exercise. Mr. Baran stated that the Trust Cloud Risk Assessments identified gaps within the policies of the executive agencies. He added that a lot of the political subdivisions mentioned above are in the same position and that even though this initiative is not directly linked to the Trust Cloud initiative there is a relationship in that as agencies/entities adopt these new policies these gaps will be filled, improving their risk assessment scores and their security posture.

Mr. Torres asked if agencies will be required to follow these templates in the future. Mr. Baran stated that the policies will be offered on a voluntary basis for agencies to adopt, with encouragement for agencies that do not have policies to adopt them. He added that for agencies with their own policies these templates should be used as reference to ensure that their existing policies are NIST compliant. He also stated that within the Trust Cloud platform policies uploaded by agencies will be validated to ensure NIST compliance.

Chair Sambandam added that having a standardized, scalable template is a very valuable option, which helps identify and address gaps in order to meet standards, as well as improve the effectiveness of plans such as the Incident Response Plan, Continuity Plan, etc. He also noted that testing these plans and training employees will help makes these plans much more effective.

Mr. Baran stated that the development of the Incident Response Policy is occurring simultaneously with development of the Incident Response Plan template and playbook, which will also be available as part of this template library. He added that the vendor working on this secondary set of documentation would also appreciate stakeholder engagement, particularly from this group as the target audience is the whole of the state, and understanding the challenges of IP environments of smaller political subdivisions will be critical to these templates. He again encouraged members to watch for invitations to those meetings and stakeholder discussions and plan to participate.

Ms. Athens asked if an inventory of agency policies had been done. Chair Sambandam stated that the information currently available is what has been submitted as part of the Risk Assessment Questionnaire. Ms. Athens stated she believed actual policies were not submitted, just questions answered on the questionnaire. Chair Sambandam said he did not have that information readily available, but he will investigate this and respond to Ms. Athens about her agency's status later. Ms. Athens stated that some type of inventory could be helpful as a starting point.

Mr. Abeyta noted that having these policies or a "playbook" available to smaller entities, with limited staff and resources, will be very beneficial.

Mr. Baran stated that one of the projects for SLCGP funding in the future will be to provide support to those political subdivisions which need help taking these policies out of the library and customizing them, so providing this type of support is being considered.

8. **Discuss Cybersecurity Report –** Melissa Gutierrez
Motion to close the meeting pursuant to Section 9-27A-5(D) NMSA 1978
Mr. Johnson so moved, seconded by Dr. Liebrock. There being no opposition the meeting moved into closed session at 2:42 p.m.

The meeting returned to open session at 3:28 p.m. with Chair Sambandam stating no action was taken during the closed portion of the meeting and the meeting will now proceed with the remaining items on the Agenda.

9. **Member Comment(s)**
None.

10. **Public Comment(s)**
None.

11. Future meeting cadence and agenda – Melissa Gutierrez

Ms. Gutierrez stated a meeting needs to be scheduled to adopt the report discussed in Item 8, preferably in a couple of weeks. Chair Sambandam asked for suggestions. Mr. Johnson suggested meeting on October 16th which would give another two weeks, if needed, to meet again on the 30th to meet the deadline. Chair Sambandam stated that would work for him and asked if that was agreeable with the rest of the Committee. Consensus was positive so Chair Sambandam asked Ms. Gutierrez to schedule a meeting for the 16th, with the 30th as a possibility if anything further is needed. Ms. Gutierrez responded that she will do so.

12. ADJOURNMENT:

MOTION: Mr. Johnson moved to adjourn the meeting seconded by Mr. Abeyta. There being no further business before the Committee and no objection to the motion the meeting was adjourned at 3:31 p.m.

DocuSigned by:

437214FBE82C453...

Raja Sambandam, Committee Chair, State CISO