CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
August 30, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was to review the draft recommendations for the CSAC September Quarterly Meeting and map communications channels for election officials.

Discussion

- Ms. Kirsten Heidelberg, Alternate Designated Federal Officer (ADFO) for the MDM Subcommittee, brought the meeting to order, reviewed the agenda, reminded Subcommittee members of the upcoming CSAC September Quarterly Meeting on September 13, and turned the call over to Dr. Starbird.

- Dr. Kate Starbird, Associate Professor, Human Centered Design & Engineering, University of Washington, MDM Subcommittee Chair, reviewed the agenda to include a discussion on the draft recommendations for the CSAC September Quarterly Meeting, the Homeland Security Advisory Council (HSAC) recommendations concerning mis- and dis-information, and beginning to map communications channels for election officials. Subcommittee members did not provide any additional feedback concerning the CSAC September Quarterly Meeting.

- The group discussed the HSAC recommendations concerning mis- and dis-information. Mr. Geoff Hale, CISA, added context to the HSAC's work and noted that the group assembled in the wake of the DHS Disinformation Governance Board (DGB). He offered that the HSAC's work solidified DHS and CISA's role in the mission space to protect critical infrastructure from mis- and dis-information, but the recommendations did not determine what agencies have the ability to surface reports of mis- and dis-information outside the Intelligence Community.

- Subcommittee members discussed the HSAC recommendation to "bolster the role of DHS Office of Intelligence and Analysis to identify high-volume disinformation purveyors and emerging focal points of disinformation such as dangerously inaccurate health advice."[1] Dr. Starbird cautioned it might not be helpful for DHS to participate in identifying domestic actors. The group noted the difficulty in determining the government's involvement in combatting high-volume disinformation purveyors before the purveyor is attributed to a domestic or foreign threat. The group suggested making recommendations during the pre-attribution phase.
    - Ms. Suzanne Spaulding, Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies, clarified that the Federal Bureau of Investigation (FBI) would not engage during the pre-attribution phase due to First Amendment concerns if the purveyors were later identified as a domestic threat. Mr. Hale noted the FBI can get involved in domestic issues if there is explicit indication of a crime present. Mr. Hale reflected that these discussions of scoping authority relate to the Subcommittee's initial deliberations urging CISA to be actor-agnostic in their work combating mis- and dis-information.

[1] https://www.dhs.gov/publication/homeland-security-advisory-council-disinformation-subcommittee-final-report

  - Dr. Starbird noted that the HSAC recommendations do not change the Subcommittee's work. She reviewed the statements CISA Director Jen Easterly has made publicly in appearances such as DEF CON expressing her support of this mission and work.

- Ms. Spaulding urged Dr. Starbird not to solely focus on addressing foreign threats during the CSAC September Quarterly Meeting. Ms. Spaulding observed a shift in narrative to combatting foreign threats. She encouraged Dr. Starbird to emphasize that domestic threats remain and while attribution is sometimes unclear, CISA should be sensitive to domestic distinctions, but cannot focus too heavily on such limitations.

- Subcommittee members began to map communications channels to election officials to help identify gaps in CISA's communication and resource delivery. Dr. Starbird noted that the Elections Information Sharing and Analysis Center (E-ISAC) maintains regular outreach to many jurisdictions but does not know the gaps in the jurisdictions missed.
  - Mr. Hale identified the most effective form of outreach as one-on-one relationships with local clerks, but acknowledged these relationships are difficult to maintain. The largest gap in communication is reaching the smallest organizations who lack adequate and enduring staff or have staff who serve other roles outside managing elections.
  - Dr. Starbird questioned whether the hard-to-reach jurisdictions know how to find CISA resources or get connected with CISA staff. Mr. Hale noted that CISA has over 130 Protective Security Advisors to its field staff who help tie election jurisdictions into broader cybersecurity service models. The group discussed the difficulties that exist within these relationships, as election jurisdictions lack adequate staffing and do not have the time to dedicate to cyber awareness. Mr. Hale described CISA's enhanced efforts deploying subject matter experts to conferences across the country to talk to election clerks, facilitate state-level election exercises, promote CISA services, and more. He described the complexities of how to engage with certain jurisdictions.
  - Dr. Starbird asked whether smaller jurisdictions face relative need or if CISA is finding that jurisdictions only require surge support in certain incidents. Mr. Hale affirmed the latter and noted that this is why CISA directs their attention to planning and resilience work before an incident strikes.

- Subcommittee members discussed factors for mis- and dis-information attacks to amplify. Based on her research, Dr. Starbird reviewed four key reasons why election-related mis- and dis-information spreads:
  1. Uncertainty – e.g., if states have laws that delayed the processing of mail-in ballots which extended the vote count and therefore the uncertainty,
  2. Anxiety – e.g., if individuals place a high degree of care in the outcome, or if one state or locality was critical in the outcome,
  3. Sensationalism – e.g., if the particular news is interesting and could draw more attention,
  4. Contagion – e.g., if information is contained to a small, tightknit community that passes information amongst each other.

- Ms. Kim Wyman, CISA, thanked Dr. Starbird for the helpful guidance. She added that hard to reach jurisdictions are not only smaller in size and have less resources, but also lack the bandwidth to remain informed of cyber threats. She detailed that CISA has made resources available for jurisdictions to use as a resource. Dr. Starbird reflected on a past brief with the National Association of Secretaries of State and the National Association of State Election Directors who identified the main need for people hours. She asked if CISA could provide grant funding for jurisdictions to hire additional support.

  - Mr. Hale commented that CISA has limited experience with grant funding in this space, but suggested the group explore new state, local, territorial, and tribal (SLTT) cyber grants. He encouraged the Subcommittee to explore CISA's role in providing grant funding if the Subcommittee deems this a potential recommendation.
  - Dr. Starbird reflected the complexities on the need for jurisdictions to operate independently when delivering crisis communications, but that many lack the resources to do this. Mr. Hale offered that many jurisdictions point to the guidance coming from their state.
  - Subcommittee members discussed the difficulties where the communicator is no longer a trusted voice, or if the communicator is a private organization. Ms. Spaulding cautioned the group that the current state of the nation's readiness for cyber threats in the elections space is not equal across the board, so a crisis communications team or other advanced ideas do not solve the gaps in existing communication.

- Subcommittee members continued to discuss the spread of mis- and dis-information. Mr. Hale noted that a majority of states have myth busting websites that also outline audit expectations to help preempt any interference by pointing individuals to these resources.
  - To combat the resources problem, Ms. Spaulding suggested that CISA reach out to local colleges and universities, especially Cyber Centers of Excellence, to help election jurisdictions. She suggested leveraging students studying cybersecurity, communications, and journalism.
  - Ms. Spaulding recommended Mr. Craig Neumark as a potential point of contact to request funding for such initiatives.

- Dr. Starbird thanked attendees for their participation. She suggested that the group focus the next meeting on the tasking questions related to surveillance and monitoring. Ms. Heidelberg reminded the group that the next meeting is scheduled for September 20 and adjourned the meeting.

Action Items

1. Subcommittee members will send Dr. Starbird any feedback on discussion points for the CSAC September Quarterly Meeting.

Attendees*

Participants

Name	Organization
Dr. Kate Starbird, Chair	University of Washington
Mr. Geoff Hale	CISA
Ms. Suzanne Spaulding	CSIS
Ms. Kim Wyman	CISA

Other Meeting Attendees

Name	Organization
Ms. Devi Nair	CSIS
Ms. Claire Teitelman	JPMorgan Chase

Government and Contractor Support

Name	Organization
Ms. Kirsten Heidelberg, ADFO	CISA
Ms. Mariefred Evans	TekSynap

**Meeting was held via Teams/teleconference*