CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation

The core of CISA's mission is to safeguard American's critical infrastructure. The nation has seen the corrosive effects of mis-, dis-, and mal-information (MDM) across a host of our critical infrastructure in recent years, impacting our election systems, telecommunications infrastructure, and our public health infrastructure. As there is no shortage of entities working on MDM issues, CISA is evaluating how to best engage in the space in an additive way, while safeguarding our credibility as an independent agency ahead of the next election cycle.

- **Where We Are.** CISA has a burgeoning MDM effort that focuses on building national resilience through public awareness. CISA engages with subject matter experts—researchers, think tanks, and public relations experts—to understand the threat of MDM, develop strategies to message to the public, and amplify trusted voices. These actions include directly engaging with social media companies to flag MDM, and creating a repository of factual guides and toolkits.
- **New Initiatives.** CISA is bringing on staff to address MDM related to the pandemic and incorporate lessons learned into longer-term strategies, as well as improving our ability to do analytics on narrative intervention. We are also working with federal partners to mature a whole-of-government approach to mitigating risks of MDM, framing which tools, authorities, and interventions are appropriate to the threats impacting the information environment.
- **Where We Want to Go in 2022.** Ahead of midterm elections in 2022, it will be critical to evaluate CISA's role in this space and ensure that the agency is providing additive value that fits within its unique capabilities and mission. One approach is to recognize CISA's responsibility for securing our election infrastructure – and ensuring CISA is a trusted resource in providing education on election processes and procedures to minimize misunderstanding and opportunities for MDM. CISA also wants to ensure it is set up to extract lessons learned from 2022 and apply them to the agency's work in the 2024.

Questions for the Committee

1. What should CISA's role be in the MDM space? How should it leverage its unique capabilities and mission to contribute to this space, without becoming duplicative of other efforts and remaining focused on its mission?
2. How would the Committee balance CISA's efforts between the need to build resilience to MDM, broadly, versus activities to address to MDM narratives, specifically? This distinction can be understood as broad public education and awareness campaigns versus rumor control, amplifying credible information, type efforts.
3. How can CISA inspire innovators to partner with the government in a way that catalyzes availability of trusted information without being seen as government "propaganda"?
4. What is the right model for CISA engagement with social media and other media entities?
5. How should CISA and the USG maintain situational awareness of MDM and detect efforts to manipulate the information environment? What is the balance between social listening, privacy, and protected speech?

EXHIBIT
Q

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
April 12, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was to de-brief the March 29 presentation from [redacted] to inform the subcommittee's draft recommendations to CISA leadership.

Discussion

- [redacted] Designated Federal Officer (DFO) for the CSAC and the MDM Subcommittee brought the meeting to order and turned the meeting over to MDM Chair, [redacted]

- [redacted] University of Washington, MDM Subcommittee Chair, asked subcommittee members to reflect on their conversation with [redacted] Subcommittee members expressed concern regarding the demands on elections officials to respond to MDM in addition to their primary role running elections. [redacted] posed the recommendation for CISA to convene workshops for elections officials across the country to address these concerns in a common place and highlight best practices.

- Subcommittee members discussed potential recommendations to pose to CISA. Members identified the need to outline CISA's operating parameters in the elections scope and limitations to inform their recommendations. [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), encouraged the subcommittee to utilize a risk management process to determine how CISA can best support elections officials. She reiterated that the best way to buy down risk is to prioritize risks according to the severity of the threat, vulnerability, and consequences. [redacted] recommended that the subcommittee focus on discussing elections in the context of critical infrastructure's ability to perform its necessary function to avoid any politicization of their recommendations. The subcommittee identified the critical function within the elections infrastructure as preserving the peaceful transition of power.
    - Subcommittee members expanded the scope of their discussion to include MDM threats impacting the judicial system. Mr. Geoffrey Hale, CISA, noted that the subcommittee must also consider the judicial system in terms of its functionality. He identified the functionality of the courts as resolving disputes in a binding, determinative way. MDM, he argued, undermines the public's trust in the courts, preventing the judicial system to perform its critical function.
    - Subcommittee members discussed areas CISA could bring a comparative advantage and offered that CISA may not be best positioned to perform pre-bunking work to counter MDM threats in the elections or judicial sectors.

- Ms. Kim Wyman, Senior Election Security Lead, CISA, highlighted [redacted] recommendations that CISA provide rumor control and share resources, trainings, and best practices as potential action items for the subcommittee to consider. She suggested incorporating state and local officials to share best practices within the

CISA CYBERSECURITY ADVISORY COMMITTEE

elections space. [redacted] affirmed that a risk-based approach is best to help the committee navigate how CISA can maximize support to combating MDM in the elections space. She reiterated the benefits of convening elections officials to establish a foundation of how to advance and address MDM threats.

- [redacted] summarized the two draft recommendations for CISA within the elections framework to include (1) convene elections officials and/or judges to build a common understanding of the MDM threat landscape and outline effective collaboration tactics, and (2) run rumor control.
    - In response to the recommendation to run rumor control, [redacted] alerted subcommittee members to the 10 ongoing projects on monitoring and aggregating MDM threats around elections, run by the National Science Foundation. She suggested that CISA coordinate and amplify resources to individual locations to connect state and local elections officials with this research capacity. [redacted] affirmed that CISA should direct media, government, and other organizations to trusted resources.

- Subcommittee members reviewed the Director's expectations for subcommittee deliverables. [redacted] shared that the subcommittee has the flexibility to implement a phased approach for recommendations to include a presentation of select recommendations for the June Quarterly Meeting. Mr. Hale shared the initial framing questions the subcommittee was charged to consider.
    - Members emphasized two framing questions for further consideration:
        - How can CISA inspire innovators to partner with the government in a way that catalyzes availability of trusted information without being seen as government "propaganda"?
        - What is the balance between social listening, privacy, and protected speech?
    - Subcommittee members suggested navigating the second scoping question of interest through collaborating with key partners under ethical guidelines to allow separation between the government and the trusted information shared.
    - [redacted] suggested partnering with the DHS Office of Civil Rights and Civil Liberties (CRCL) to convene constitutional scholars, national security professionals, and privacy activists. Subcommittee members also suggested presenting the recommendation to Congress. [redacted] CISA, suggested [redacted] Director of Programs, DHS CRCL, as a point of contact.
- Subcommittee members returned to the recommendation for CISA to amplify trusted information and discussed designating a point of contact as a clearing house for trusted information. [redacted] and Mr. Hale suggested designating the ISACs as the clearing house for information to avoid the appearance of government propaganda.
    - Ms. Wyman flagged for concern that no entity will ever be viewed as completely objective. [redacted] suggested designating multiple voices as the clearing hour so there is not one trusted voice.
- [redacted] thanked the subcommittee for their participation and informed subcommittee members that she will send out materials to help members identify initial recommendations prior to the next subcommittee meeting. [redacted] identified the next meeting date is set for April 26 and adjourned the meeting.

Action Items

- A1: [redacted] will send subcommittee members materials to help refine recommendations to CISA prior to the next subcommittee meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	CISA
[redacted]	CSIS
Ms. Kim Wyman	Illinois Emergency Management Agency (IEMA)
	CISA

Other Meeting Attendees

Name	Organization
[redacted]	CISA
	CSIS
	IEMA
	JPMorgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	TekSynap

Meeting was held via Teams/teleconference

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
June 14, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was to discuss developments from recent conversations with Maricopa County, Arizona elections officials and review strategy for the CSAC June Quarterly Meeting.

Discussion

- [redacted] Alternate Designated Federal Officer (ADFO) for the MDM Subcommittee, brought the meeting to order and turned the call over to [redacted]
- [redacted] University of Washington, MDM Subcommittee Chair, thanked the members for joining. She noted this time is dedicated to discussing the final recommendations to present for vote at the CSAC June Quarterly Meeting and share ideas of next steps for the Subcommittee.
- [redacted] shared takeaways from her conversation with [redacted] and past briefer. She obtained permission from [redacted] to use his quote "managing mis-, dis-, and mal-information is my day job. Running elections is my night job" in the subcommittee's recommendations for the CSAC June Quarterly Meeting. Subcommittee members affirmed [redacted] suggestion of adding the quote in the recommendations and stated that it was important to motivate the recommendations. [redacted] Illinois Emergency Management Agency, commented that the quote speaks to the heart of the recommendations. [redacted] took for action to incorporate the quote into the draft recommendations and return the updated draft to [redacted] by Wednesday, June 15.
- [redacted] reviewed her conversation with [redacted] Columbia Law Professor, to socialize the existence of the subcommittee and their taskings.
    - [redacted] shared that [redacted] intends to reach out to civil liberties groups to help socialize the existence of the subcommittee following the CSAC June Quarterly Meeting. He recommended that the group contact [redacted] of the Brennan Center. He provided recommendations to [redacted] on how the group could best speak to their tasking questions related to surveillance and monitoring. [redacted] recommended that the group contact the two individuals during their July meeting as they discuss issues of surveillance and monitoring. [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, affirmed this course of action.
    - [redacted] solicited additional recommendations for future briefers. [redacted] recommended that the group hear from the Electronic Frontier Foundation.

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] added that [redacted] colleague, [redacted] suggested that the subcommittee explore the idea of how CISA could develop a rapid response team to deploy virtually or in-person to local election officials' jurisdictions struggling with specific informational threats. The support would include checking equipment to verify if a breach is present or not, determining how to communicate the existence of a breach, and determining how to target certain kinds of communication.
    - [redacted] clarified if this rapid response team would only act in the context of MDM threats. [redacted] noted that the response team would require a broader range of expertise, as they first must be able to verify whether a real threat exists, then be able to communicate the existence of an MDM threat.
    - Mr. Geoff Hale, CISA, commented that this is a fascinating idea that takes CISA's existing operational responsibilities to consider MDM as part of its core mission set. He noted that this would be an evolution of CISA's current defensive posture. [redacted] agreed with this framing of the question.
    - [redacted] commented that the rapid response team would need to surge for short periods of time around elections. She suggested the subcommittee consider the requirements for the team's expandability, ability to conduct media analysis, and the level of understanding on MDM in a communications context.
    - Mr. Hale noted the possibility to stand up this team in the short term by encouraging the communications team to consider MDM equities. [redacted] took for action to discuss how CISA could stand up a rapid response team during the CSAC June Quarterly Meeting.
    - Ms. Kim Wyman, Senior Elections Official, CISA, stressed that election officials across the country are struggling most with MDM threats and physical security. She encouraged the subcommittee to lean into their work and their recommendations and noted that the group was selected by the Director for a reason.
        - [redacted] noted that physical and MDM-related threats are often interrelated, so the group cannot address the physical threats against elections officials without addressing the root cause of MDM-related threats. She continued by stressing that MDM threat exist with or without a cyber component. She noted that the idea of a rapid response team must include the ability to engage whether or not a cyber component is present.
        - [redacted] agreed with [redacted] point that threats to critical infrastructure are not limited to cyber threats.

- Subcommittee members did not express further items to raise during the CSAC June Quarterly Meeting. [redacted] noted that she and [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), will be dialing in virtually for both the closed and open sessions.

- Mr. Hale updated the subcommittee that CISA is working to determine best practices for socializing the existence of the subcommittee and the proposed recommendations with Congress. [redacted] reflected on a recent conversation with CSAC Chair, [redacted] and noted that she intends to determine a strategy with other CSAC Members during the closed session.

- Subcommittee members took for action to notify the CSAC Team whether they prefer to meet on Wednesday, July 20 or Tuesday, July 26 from 11:00a.m. to 12:00 p.m. ET. [redacted] noted that she will be on vacation during both times but encouraged the subcommittee to meet.

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] joined the meeting and updated the subcommittee on her recent conversation with [redacted] George Mason Law Professor, where she described the subcommittee's tasking and the purpose of the draft recommendations for CISA to point individuals to resources on election topics.
    - [redacted] shared that [redacted] encouraged the subcommittee to discuss their work in the context not that CISA is dealing with disinformation by deciding what is true and pointing people to resources, but that CISA has a mission to ensure National Critical Functions are secure and resilient, and disinformation poses a threat to CISA's ability to do its mission. Therefore, CISA needs to work with a range of actors on developing best practices for countering MDM threats.
- [redacted] thanked the subcommittee members and adjourned the meeting.

Action Items

- [redacted] will updated the draft MDM recommendations to include the quote from [redacted] and send the updated draft to [redacted] by Wednesday, June 15.
- MDM Subcommittee members will identify the next meeting date for late July 2022.
- Mr. Hale will continue to determine the next steps for outreach to Congress on the Subcommittee's work.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
[redacted]	CISA
Ms. Kim Wyman	CSIS
	Illinois Emergency Management Agency (IEMA)
	CISA

Other Meeting Attendees

Name	Organization
[redacted]	CSIS
	JP Morgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	TekSynap

**Meeting was held via Teams/teleconference*

CISA CYBERSECURITY ADVISORY COMMITTEE

DRAFT REPORT TO THE CISA DIRECTOR

Protecting Critical Infrastructure from Misinformation and Disinformation

June 22, 2022

Introduction:

CISA's mission is to strengthen the security and resilience of the nation's critical functions. The spread of false and misleading information can have a significant impact on CISA's ability to perform that mission. CISA should take a similar risk management approach to these risks that it takes to cybersecurity risks.

Borrowing from a growing body of research[i], we define misinformation as information that is false, but not necessarily intentionally so; disinformation as false or misleading information that is purposefully seeded and/or spread for a strategic objective; and malinformation as information that may be based on fact, but used out of context to mislead, harm, or manipulate. The spread of false and misleading information poses a significant risk to critical functions like elections, public health, financial services, and emergency response. Foreign adversaries intentionally exploit information in these domains (e.g., through the production and spread of dis- and malinformation) for both short-term and long-term geopolitical objectives[ii]. Pervasive MDM diminishes trust in information, in government, and in the democratic process more generally.

The initial recommendations outlined below focus primarily on mis- and disinformation (MD) about election procedures and election results. Future recommendations may seek to address the potential impacts on other critical functions and some of the unique challenges in identifying and countering malinformation.

The First Amendment of the Constitution limits the government's ability to abridge or interfere with the free speech rights of American citizens. The First Amendment and freedom of speech are critical underpinnings to our society and democracy. These recommendations are specifically designed to protect critical functions from the risks of MD, while being sensitive to and appreciating the government's limited role with respect to the regulation or restriction of speech.

CISA is uniquely situated to help build awareness of MDM risks and provide a robust set of best practices related to transparency and communication when addressing mis- and disinformation, specifically in the election context.

Findings:

In addition to researching the issue of MDM more broadly, our committee gathered input from election officials, many of whom are acutely struggling to address mis- and disinformation. Election officials, especially those in small jurisdictions, often lack the training and resources to identify and address the spread of false claims, which is becoming an increasingly demanding aspect of their jobs. Meanwhile, mis- and disinformation are undermining trust in their work and leading to personal harassment and even physical threats.

"Responding to misinformation is my day job. My night job is running elections."

[redacted]

Recommendations:

CISA is positioned to play a unique and productive role in helping address the challenges of MD, especially regarding its mission of protecting election-related critical infrastructure.

- CISA should focus on MD that risks undermining critical functions of American society including:
  - MD that suppresses election participation or falsely undermines confidence in election procedures and outcomes.
  - MD that undermines critical functions carried out by other key democratic institutions, such as the courts, or by other sectors such as the financial system, or public health measures.
  - MD that promotes or provokes violence against key infrastructure or the public.
  - MD that undermines effective responses to mass emergencies or disaster events.

- In this work, CISA's activities should be similar to the Agency's actions to detect, warn about, and mitigate other threats to critical functions (e.g., cybersecurity threats).
  - The initial recommendations focus primarily on MD about election procedures and election results. In the elections context, false information about when, where, and how to vote can disenfranchise voters and the proliferation of false and misleading claims about election processes can reduce confidence in results. More problematically, the proliferation of false and misleading claims about elections can make it difficult to identify and counter any real threats to election integrity, such as from foreign adversaries that leverage disinformation as part of a multi-dimensional attack on election infrastructure.
  - Currently, many election officials across the country are struggling to conduct their critical work of administering our elections while responding to an overwhelming amount of inquiries, including false and misleading allegations. Some elections officials are even experiencing physical threats. Based on briefings to this subcommittee by an election official, CISA should be providing support — through education, collaboration, and funding — for election officials to pre-empt and respond to MD. The specific recommendations below detail how CISA can do this.

- CISA should consider MD across the information ecosystem.
  - In the last decade, the challenge of MD and its threat to democratic societies has become increasingly salient around the globe, including here in the United States.[iii] The Internet, and in particular social media platforms, have played a complex role in this rise — from disrupting the role of traditional "gatekeepers" in the dissemination of information; to vastly accelerating the speed and scale at which information travels; to providing new vectors for manipulation and access for "bad actors" to vast audiences. Researchers are still working to understand the contours of the relationship between social media and MD, even as the platforms themselves — and the norms that guide use on them — are ever-changing. And it is important to note that the outsized attention paid to social media regarding these issues may not accurately represent the proportionality of their role. These sites are part of a broader ecosystem that includes other online websites (e.g., state-run media like Russia Today (RT) – an American branch of Russian state-funded media network) and gray propaganda networks associated with Russia, China, and Iran) and more traditional media (e.g., AM radio and cable news). The problem of MD manifests as information activity across many different parts of this ecosystem.
  - CISA should approach the MD problem with the entire information ecosystem in view. This includes social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio, and other online resources.

- CISA should work across four specific dimensions of MD to include:

- Building Society Resilience to MD. CISA should continue serving a mission of building resilience through broad public awareness campaigns about the challenges of mis- and disinformation and strategies for the public and other specific audiences (e.g., election officials, journalists, etc.) to use to build individual and collective resilience. Here, the focus should be both on enhancing information literacy for the modern information environment and on supporting and integrating civics education into those efforts. Information literacy should include understanding the dynamics of the modern information space (social networks, influencers, and algorithms), understanding and identifying tactics of manipulation, and generally becoming savvier participants in interactive information spaces. The goal should be to both teach people the skills (*how* to identify mis- and disinformation) and provide motivation for using those skills (*why* they don't want to engage with and/or spread mis- and disinformation). This dimension aligns with the CISA's "Cyber Hygiene" mission.

- Proactively Addressing Anticipated MD Threats. CISA should also look at ways to anticipate and mitigate the impact of specific content and narratives impacting its mission of protecting critical functions. These efforts include proactively addressing anticipated threats through education and communication. They require applying knowledge learned from responding to past mis- and disinformation to anticipated, future events. Where possible, CISA should proactively provide informational resources — and assist partners in providing informational resources — to address anticipated threats. In cases where specific narratives are anticipated, CISA should help to educate the public about those narratives, following the best practices suggested by the most recent research. (The research on "debunking vs. prebunking" is ongoing, so CISA must stay up to date on the current recommendations.) Proactive work should also include identifying and supporting trusted, authoritative sources in specific communities (e.g., in the elections context, local media and election officials). These efforts should also include building knowledge and experience that can empower individuals to be more resilient against divisive and despair-inducing disinformation. CISA should support these efforts by creating and sharing materials; by providing education and frameworks for others to produce their own materials; and through funding to local election officials and external organizations to assist in this work.

- Rapidly Responding to Emergent and/or Persistent Informational Threats: CISA should also work to rapidly respond — through transparency and communication — to emergent informational threats to critical infrastructure. This will require a system of rapid identification, analysis, and applying best practices to develop and disseminate communicative products. CISA should work with and provide financial support to external partners who identify emergent informational threats and utilize its strengths in developing and disseminating communicative products to address false and misleading narratives. CISA should also prioritize, where possible, boosting first-hand, trustworthy, and authoritative sources (e.g., election officials) in their efforts to rapidly respond to informational threats. CISA should also be a place where people can find out how to tap into credible sources, governmental and non-governmental. These response efforts can be actor-agnostic, but special attention should be paid to countering Rapidly Responding to Emergent and/or Persistent Informational Threats: CISA should also work to rapidly respond — through transparency and communication — to emergent informational threats to critical infrastructure. This will require a system of rapid identification, analysis, and applying best practices to develop and disseminate communicative products. CISA should work with and provide financial support to external partners who identify emergent informational threats and utilize its strengths in developing and disseminating communicative products to address false and misleading narratives. CISA should also prioritize, where possible, boosting first-hand, trustworthy, and authoritative sources (e.g., election officials) in their efforts to rapidly respond to informational threats. CISA should also be a place where people can find out how to tap into credible sources, governmental and non-governmental. These response efforts can be actor-agnostic, but special attention should be paid to countering foreign threats.

- Countering Actor-Based Threats: CISA should work collaboratively to identify, communicate, and address actor-based MD threats (e.g., foreign and/or criminal MD campaigns that target critical infrastructure).
- The prioritization of these different aspects of the mission will necessarily be dynamic. During non-election periods and absent other pressing concerns or crises, the primary focus should be on resilience and proactively addressing anticipated threats. During the election period and other active events, the focus shifts to addressing specific and sometimes emergent informational threats through rapid communication.

- On the proactive dimension, CSAC recommends two time-sensitive items related to the 2022 election to include:
  - CISA should support local election officials in producing a "What to Expect on Election Day" plan to proactively address misleading narratives that may arise due to the specific contours of their election materials and procedures, such as through education and communication. This work could include direct collaboration or building educational materials and templates that election officials can use to generate their own plans and resources.
  - CISA should convene a 2022 "What to Expect on Election Day" workshop, to bring together representatives from government agencies and social media platforms, legacy media including local journalists, researchers, and election officials to map out, plan for, and stage resources to address informational threats to the 2022 election (in August 2022) and the 2024 election (convene by April 2024).
  - On the response dimension, during the 2022 election, CISA should continue to proactively participate— in collaboration with outside researchers and those with first-hand authoritative information—in correcting MD that poses a significant threat to critical functions. If possible, CISA should also support external organizations doing MD response work in their own communities — especially organizations in specifically targeted communities, including veterans, faith communities, the Black and Latino communities, immigrant communities, etc. — with grant funding.
  - In doing this work, CISA should operate with the following principles to help build trust in the work and its role:
    - Transparency: Processes, participants and sources of information should be transparent.
    - Collaboration: CISA should prioritize collaboration, not only amongst the different government agencies supporting this work, but also by bringing in civil society, academia, and industry.
    - Speed/Accuracy: Time is of the essence in this work and CISA should act with speed, while being deliberate, accurate and thoughtful.

- CISA should work internally and with collaborators to develop metrics for measuring the impacts of its efforts.
  - To understand the impacts of MD and the efficacy of counter-MD efforts, society needs to develop new metrics, new methods of analysis, and new infrastructure to measure the often diffuse effects of manipulation in a complex sociotechnical system. Though a particular case of MD can have acute impact, some of the more pervasive effects can manifest over long time periods and with both direct and indirect dimensions. This presents a challenge for measuring both impact and mitigation efforts[iv].
  - More research should be done to identify measurable indicators of impact, but initial metrics may include:
    - For general resilience work and proactive messaging: Measuring the spread and engagement of specific CISA campaigns and/or messages. Measuring the efficacy of certain messages (in reducing engagement by participants in MD content).
    - For proactive work: Measuring the size and strength of the networks built (of key stakeholders, trusted sources, and voices, etc.).
    - For rapid response: Measuring how long it takes to respond, the reach of the response, and the number of threats addressed.

- For actor-based threats: Measuring the number of threats identified and/or addressed, the time to respond, and the impact of the response (e.g., on the activities of the identified actors).

- CISA should invest in external research to assess the impact of MD threats and the efficacy of interventions.
  - More research is needed to develop models and methods for assessing the direct and indirect effects of MD on society. CISA should support this research, through funding and, where appropriate, collaboration. For example, CISA should consider funding third-party research to measure the reach and efficacy of their counter-MD activities. CISA should also support efforts to increase the transparency of social media platforms to enable more research into impacts and interventions online.

---

[i] Jack, Caroline. "Lexicon of lies: Terms for problematic information." Data & Society 3, no. 22 (2017): 1094-1096. ; Wardle, Claire, and Hossein Derakhshan. "Information disorder: Tow ard an interdisciplinary framew ork for research and policymaking." (2017). ; Starbird, Kate, Ahmer Arif, and Tom Wilson. "Disinformation as collaborative w ork: Surfacing the participatory nature of strategic information operations." Proceedings of the ACM on Human-Computer Interaction 3, no. CSCW (2019): 1-26.

[ii] Rid, Thomas. Active Measures: The secret history of disinformation and political w arfare. Farrar, Straus and Giroux, 2020.

[iii] Spaulding, Suzanne E., Eric Goldstein, and John J. Hamre. Countering Adversary Threats to Democratic Institutions: An Expert Report. Center for Strategic & International Studies, 2018.

[iv] Rid.

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
June 7, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was for Subcommittee members to review and discuss the draft recommendations to present during the CSAC June Quarterly Meeting.

Discussion

- [redacted] Alternate Designated Federal Officer (ADFO) for the MDM Subcommittee, brought the meeting to order and turned the call over to [redacted]

- [redacted] University of Washington, MDM Subcommittee Chair, welcomed the members and reviewed the subcommittee's current status. She identified her goals of the meeting to include reviewing the subcommittee's current work, obtaining feedback on items she should discuss during the CSAC June Quarterly Meeting, and identifying next steps. [redacted] CSAC Designated Federal Officer, reviewed the timeline of the CSAC recommendations and immediate next steps to note that following the vote at the June meeting, the final recommendations will be posted to the CSAC website, she asked the Subcommittee not to share the recommendations until they are voted on by the full Committee. Subcommittee members confirmed their next meeting as Tuesday, June 14 to discuss the draft recommendations to present during the CSAC June Quarterly Meeting.
    - [redacted] informed the group of her upcoming meeting with [redacted] Columbia Law Professor, to socialize the existence of the subcommittee and their taskings. [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, noted that she sent the group a list of civil society groups Twitter has partnered with in the past in the event the group would like to reach out to any additional individuals. [redacted] recommended that the group reach out after the recommendations are made public.

- Subcommittee members discussed the logistics of how CISA plans to rollout the materials following the CSAC June Quarterly Meeting and best practices for socializing the recommendations once they are final.
    - [redacted] explained that CSAC Support will work with CISA's External Affairs team to inform any public materials such as press releases, and the recommendations will be posted on the CSAC website once they are approved by the Director.
    - [redacted] asked if there was value in socializing the recommendations following their release. [redacted] took for action to meet with CISA's External Affairs team to determine best practices.
    - [redacted] identified a next step of recruiting additional subject matter experts (SMEs) to help inform the next recommendations for the CSAC September Quarterly Meeting.
    - [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), suggested that the subcommittee contact civil society groups prior to the June Meeting to notify them of the subcommittee's interest and intent in seeking their input in the future. [redacted] took for action to start reaching out to groups to socialize the existence of the subcommittee.

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] asked for additional feedback on items to share with the full Committee and ideas of individuals to invite to future subcommittee meetings.
  - [redacted] recommended that [redacted] solicit recommendations for additional SMEs during the June Meeting. [redacted] noted her intent to solicit feedback from the full Committee on the difficult aspects of the subcommittee's scoping questions.
  - [redacted] recommended that the subcommittee focus on the scoping questions and topics they were charged with but did not target for the June Meeting.
  - [redacted] commented that any additional work will come in the form of a formal tasking from Director Easterly. [redacted] stressed that the CSAC and individual subcommittees are not operational, meaning that CISA is not seeking the subcommittee to implement the recommendations.
  - [redacted] recommended that [redacted] ask the full Committee whether the group correctly outlined the scope of this work and correctly targeted MDM that threatens critical functions and democratic institutions that are core to CISA's mission.
  - [redacted] suggested asking the Committee how to socialize this work with their individual connections in Congress.

- Subcommittee members continued to discuss how to socialize the recommendations.
  - [redacted] suggested that CISA socialize the existence and charter of the subcommittee prior to the June Meeting, then continue to keep necessary parties informed as it progresses.
  - Mr. Hale took for action to determine, internally with CISA, the best way to socialize the subcommittee's actions with Congress once they are finalized.
  - Subcommittee members discussed the option to pull back the recommendations given the current landscape, as offered by Director Easterly.
    - [redacted] all agreed not to pull back the recommendations that they've put forth for the June Meeting and encouraged the group to present the set of recommendations for full Committee vote during the June Meeting.
- [redacted] asked the group to identify the next meeting date following the June Meeting and future briefers. [redacted] thanked the subcommittee members and adjourned the meeting.

Action Items

- CSAC Support will send out the meeting information for Tuesday, June 14 from 4:30 to 5:30pm ET and cancel the meeting scheduled for Tuesday, June 21.
- MDM Subcommittee members will identify the next meeting date for late July 2022 and develop a list of future briefers.
- Mr. Hale will determine the next steps for outreach to Congress on the Subcommittee's work.
- CSAC Support will meet with CISA's External Affairs Team to determine guidance on if / how Subcommittee members should share and amplify the recommendations and work of the Subcommittee following the CSAC June Quarterly Meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
[redacted]	CISA
Ms. Kim Wyman	CSIS
	Illinois Emergency Management Agency (IEMA)
	CISA

Other Meeting Attendees

Name	Organization
[redacted]	CISA
Ms. Allison Snell	CSIS
[redacted]	CISA
	JP Morgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	CISA
	TekSynap
	TekSynap

Meeting was held via Teams/teleconference

From: [redacted]@uw.edu]
Sent: 5/31/2022 6:49:14 PM
To: [redacted]@cisa.dhs.gov]
CC: [redacted]@associates.cisa.dhs.gov]; [redacted]@gmail.com]; [redacted]@cisa.dhs.gov]; [redacted]@csis.org]; [redacted]@gmail.com]; [redacted]@twitter.com]; [redacted]@illinois.gov]; Wyman, Kim (She/Her/Hers) [redacted]@cisa.dhs.gov]; Hale, Geoffrey (He/Him) [redacted]@cisa.dhs.gov]; [redacted]@cisa.dhs.gov]
Subject: MDM Subcommittee June 2022 recommendations V2
Attachments: MDM Subcommittee - Recommendation1 - v2.docx

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi folks,

I'm attaching our update version of the recommendations from the MDM subcommittee. The recommendations themselves have not substantively changed, but we've updated the language per our conversation last week.

The document will likely need help re: formatting and moving the citations into place. I also left a couple of comments… but those can be removed. Most are just the citations.

I'm at a conference these next few days so might not be able to respond quickly to email. Sorry!

[redacted]

On May 26, 2022, at 10:32 AM, [redacted]@cisa.dhs.gov> wrote:

Thanks for the response and clarification. Yes, the conversation highlighted below is within bounds to discuss with the Director. I look forward to talking tomorrow but please reach out if you have any questions/concerns before then.

[redacted]
CISA Cybersecurity Advisory Committee DFO
Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency
Mobile: [redacted]@cisa.dhs.gov
<image001.png>

From: [redacted]@uw.edu>
Sent: Thursday, May 26, 2022 1:23 PM
To: [redacted]@cisa.dhs.gov>
Cc: [redacted]@cisa.dhs.gov>; [redacted]@associates.cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Re: Minutes/Meeting Summary 5 - 24- 2022:

Hi [redacted]

Thanks for the information here regarding transparency. Let me clarify that we aren't planning to get feedback around the recommendations themselves... just on socializing among key stakeholders the existence of the committee and the fact that we are making recommendations about mis- and disinformation.

This is my note from [redacted] suggestion at the Tuesday meeting: "ask Director Easterly about the roll-out... if we can be helpful in your effort to pre-socialize the existence or purpose of this committee with key stakeholders, please let us know."

Can I confirm that this conversation is within bounds?

We are still deciding how to approach having a similar conversation with [redacted] – and possibly others who have made what we see as good faith criticisms of the DGB. But we don't yet have a strategy for that.

[redacted]

On May 26, 2022, at 3:49 AM, [redacted]@cisa.dhs.gov> wrote:

Thanks to all of you for the quick turn on the minutes.

[redacted] – we can discuss this more on tomorrow's planning call, but wanted to send a quick email in case you were planning to take any additional action between now and that time...The Subcommittee should not be socializing its work with outside parties (work = deliverables/recommendations), as it's pre-deliberative at this time. We also shouldn't be soliciting feedback on the recommendations from outside parties. If the subcommittee would like to bring in [redacted] to be a part of a discussion on the validation of their findings and recommendations, that is fine.

For your meeting tomorrow with the Director, you are also not permitted to discuss the specifics of the subcommittee recommendations with the Director, again, as they are pre-deliberative and have not been reviewed/voted on by the full Committee. You are certainly permitted to discuss your broader MDM concerns and those around socializing the existence of the subcommittee in advance of the June meeting, etc.

Again, happy to discuss all of this more tomorrow or to get on a call today, if needed.

Thank you,

[redacted]
CISA Cybersecurity Advisory Committee DFO
Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency
Mobile: [redacted]@cisa.dhs.gov
<image001.png>

From: [redacted]@cisa.dhs.gov>
Sent: Wednesday, May 25, 2022 7:52 PM
To: [redacted]@uw.edu>
Cc: [redacted]@associates.cisa.dhs.gov>; [redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Re: Minutes/Meeting Summary 5 - 24- 2022:

10 4; good feedback. Will incorporate

Get Outlook for iOS

From: [redacted]@uw.edu>
Sent: Wednesday, May 25, 2022 5:54:02 PM
To: [redacted]@cisa.dhs.gov>
Cc: [redacted]@associates.cisa.dhs.gov>; [redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Re: Minutes/Meeting Summary 5 - 24- 2022:

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi [redacted]

The notes look great — thank you to [redacted]

I do want to note that [redacted] and I realized we were talking about [redacted]

- [redacted] (Columbia law professor)
- [redacted] (George Mason law professor)

We may want to note that we were discussing both of these individuals. We are likely to contact [redacted] (who wrote the article I was referencing when we brought up [redacted] initially) first.

[redacted]

On May 25, 2022, at 4:15 AM, [redacted]@cisa.dhs.gov> wrote:

Good Morning [redacted]

[redacted] was able to take the notes from yesterday's meeting and turn them around quickly. I took an initial review and believe they are well put together. Thank you again [redacted]

- If you have any commentary on the minutes/meeting summary please let us know.
- Glad to make changes as needed before circulation to our larger group.
- Great meeting yesterday.

Personal mobile is 917 580 0279 as well.

Best,

[redacted]
CISA Cybersecurity Advisory Committee
Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency
Cell: [redacted]@cisa.dhs.gov

Please tell us how we are doing in our Customer Service Survey

<image001.png>

<Draft CSAC MDM Subcommittee Meeting Summary_05242022.docx>

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
May 24, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was for Subcommittee members to review and discuss the draft recommendations to present during the CSAC June Quarterly Meeting as well as the DHS Disinformation Governance Board.

Discussion

- [redacted] Alternate Designated Federal Officer (ADFO) for the MDM Subcommittee, brought the meeting to order and introduced the newly appointed ADFO for the MDM Subcommittee, [redacted] CISA.
- [redacted] University of Washington, MDM Subcommittee Chair, discussed the Subcommittee's recommendations to present during the CSAC June Quarterly Meeting and the path forward to strategically approach MDM in the government during the current discourse. [redacted] restated the Subcommittee's commitment to transparency but expressed concern for the Subcommittee's efforts and cautioned the group on how to communicate their ongoing work.
    - [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, affirmed this caution and shared her recent communication cautioning Director Easterly about her own involvement in the Subcommittee's work given the fraught time, especially in advance of the election season.
    - [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), suggested that the group recruit subject matter experts (SMEs) to support the Subcommittee's efforts, solicit different perspectives, and apply creditability to the Subcommittee's work with a broader audience. [redacted] offered an additional suggestion of asking Director Easterly for her perspective of socializing this Subcommittee's work with Congress to prevent outside parties from being blindsided by their efforts. She further suggested the Subcommittee re-read and refine the recommendations and stressed that the safest ground in election is the recommendation for CISA to 1) point individuals to an authoritative source and 2) utilize their convening power. She stressed that CISA should examine MDM beyond elections, but suggested including in the recommendations that the Subcommittee is scoping their work around elections given the approaching election cycle. [redacted] offered an additional recommendation for CISA to scope their mission space to MDM that poses significant risk to national critical functions (NCFs).
    - [redacted] suggested revisiting each recommendation to ensure each is scoped to the scale of building societal resilience. [redacted] noted that the group can frame pre-bunking efforts differently to target the perspective of clarifying election procedures. She suggested removing mention of MDM and framing the recommendations more targeted to directing people to clear information about elections procedures. [redacted] suggested editing the recommendations to change MDM to "informational threats to critical infrastructure."

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] expressed that she was uncomfortable with the term "informational threats" and posing information as a threat.
- Mr. Geoff Hale, CISA, offered that there is not a practical solution from removing the language of MDM, but suggested the Subcommittee think to frame of the divesting activities– such as tactical education in the form of tactics of foreign influence activities– to root understanding in the power dichotomy of well-resourced nation states against individual social media users or election officials. He stressed the importance of CISA's role performing risk analysis and understanding where information manipulation exists, then extending this information forward as a type of FAQ model across CISA's authorities, rather than thinking of this work as countering MDM. [redacted] noted that this is consistent with the Subcommittee's recommendation to build public resilience.

  - [redacted] stressed the recommendation for CISA to educate the public about the tactics, techniques, and procedures used by foreign adversaries to spread MDM. She emphasized that the spread of false information is a technique used by our adversaries. She affirmed the need for CISA to conduct voter risk analysis and risk identification in the context of tactics, techniques, and procedures.

- [redacted] reemphasized the recommendation for CISA to direct the public to authoritative sources of information and suggested defining authoritative sources as first-hand sources of information, most notably from elections officials themselves. She noted the concerns in this context to include MDM regarding how election procedures operate and recommended that CISA point people towards when, where, and how elections are run. Following this, CISA must publish elections procedures and audits that reinforce the credibility. This recommendation fits under the pre-bunking work while not restricting CISA to calling out false information, but instead releasing authoritative information ahead of an event so individuals can recognize attacks.

- Subcommittee members discussed potential briefers and brainstormed ways to socialize the Subcommittee's work.
  - [redacted] recommended [redacted] Columbia Law, as a potential briefer.
  - [redacted] recommended that the Subcommittee meet with Director Easterly about socializing their work.
  - [redacted] took for action to identify a point of contact from a progressive civil rights and civil liberties angle to recruit as a SME.

- [redacted] noted a challenge for the subcommittee to lay the groundwork to socialize their work with key parties in advance. She recommended that CISA point to more state officials and state laws to make the authoritative source of information less controversial.
  - [redacted] restated her offer to remove herself from the Subcommittee when the recommendations are released. Mr. Hale offered that Director Easterly would not support removing [redacted] due to her respect of [redacted] work.
  - [redacted] resurfaced the suggestion to solicit additional SME to supplement the Subcommittee's efforts.

- Subcommittee members discussed the importance of scoping their recommendations around the First Amendment.

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] suggested the group begin their introduction by highlighting the First Amendment and framing their work purely around exercising speech rights of elections officials so as not to infringe upon the rights of voters.
- [redacted] said this is an opportunity to remind the public of CISA's scope, as the First Amendment applies to CISA as a government agency in a way that it does not apply to the private sector.
- Ms. Kim Wyman, Senior Election Security Lead, CISA, reflected on her time as the Secretary of State for the state of Washington. She noted that the adversaries, such as Russia, use the First Amendment against Americans very effectively. She commented that CISA's education efforts and resilience building efforts are about helping people see our adversaries use these tools in ways they couldn't 20 years earlier to effectively spread MDM for malicious ends. She realized our adversaries utilize this part of our Constitution effectively.
- [redacted] noted the recommendation to remind individuals of our strengths and playing to these strengths rather than allowing them to be used against us by our adversaries.

- [redacted] reiterated the Subcommittee's recommendation for CISA to work to discern the truth and point to authoritative sources with firsthand knowledge when they are notified of harmful MDM. She recommended that CISA should not determine what qualifies as truth, but instead empower the public with the skills and tools while pointing to information so that they can discern for themselves. This recommendation would empower individuals to make their own decisions about information.

- [redacted] asked the group to revisit the recommendations document this week. [redacted] asked the members to identify any resources that could be put in place to communicate the work of the subcommittee when their work becomes public.
  - [redacted] suggested contacting Director Easterly in preparation for the rollout during the CSAC June Quarterly Meeting to solicit her feedback on how to pre-socialize the existence of the subcommittee with key members of Congress or outside validators.
  - Mr. Hale confirmed that the DHS Secretary, Alejandro Mayorkas, has been briefed on the CISA CSAC and the subcommittees. [redacted] shared the publicly available information on the CSAC and the Subcommittees.
  - [redacted] noted this group is different from the DHS Disinformation Governance Board since it is an external advisory group to direct CISA to define their mission and scope in this work in a transparent way.
  - [redacted] suggested soliciting feedback from [redacted] CSAC Chair, to notify him of their ongoing work.

- [redacted] noted the path forward of continuing to refine the recommendations and asked the group to brainstorm potential briefers or SMEs.
  - [redacted] suggested recruiting past briefers to review their draft recommendations.
  - [redacted] noted that the DHS Disinformation Governance Board raised the risk of potential criticisms for the Subcommittee and asked Mr. Hale to share any strategic communication regarding their work for awareness or input to assist in pre-staging messaging.

- [redacted] thanked the Subcommittee for their input, noted that he will flag the initial recommendations as a draft in revision, and adjourned the meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Action Items

- A1: Subcommittee members will refine the list of recommendations to present for Committee vote during the CSAC June Quarterly Meeting.
- A2: [redacted] will contact [redacted] for input on their initial recommendations.
- A3: [redacted] will brainstorm additional SMEs to recruit to aid the Subcommittee's efforts, particularly progressive civil rights and civil liberties advocates.
- A4: [redacted] will notify CSAC Support that the Subcommittee's initial recommendations are under current revision.
- A5: Subcommittee members will discuss recommendations to socialize their efforts with Director Easterly.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
[redacted]	CISA
Ms. Kim Wyman	CSIS
	CISA

Other Meeting Attendees

Name	Organization
[redacted]	CISA
	CSIS
	JP Morgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	CISA
	CISA
	TekSynap

Meeting was held via Teams/teleconference

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
May 10, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was to refine the list of recommendations to present to the full CSAC for vote during the June Quarterly Meeting and to advise on a deliverable due 5/11/2022 (Update Document). This Update Document was intended for the Director's review so she has a rough idea of what the subcommittees will discuss during the June meeting.

Discussion

- [redacted] Alternate Designated Federal Officer (ADFO) for the CSAC, brought the meeting to order and turned the meeting over to MDM Chair, [redacted]
- [redacted] University of Washington, MDM Subcommittee Chair, began the meeting by asking subcommittee members to discuss the announcement of the new DHS Disinformation Governance Board and the broader implications for this subcommittee.
    - Ms. Kim Wyman, Senior Election Security Lead, CISA, stressed that misinformation and disinformation are elevated to national awareness due to this board. [redacted] suggested refining the name of the subcommittee to "Informational Threats to Critical Infrastructure" or "Informational Threats to Election Security" so as not to conflate the group's efforts with the work of the DHS Disinformation Governance Board. [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, affirmed this and cautioned the group against pursing any social listening recommendations for the CSAC June Quarterly Meeting.
    - [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), cautioned the group against changing the name of the subcommittee. She expressed worry about the concept that information itself is threatening and emphasized the need for the prefixes of mal-, mis-, and dis- when discussing informational threats. Subcommittee members highlighted that any prefix used as a modifier to describe threats from information distortion could be attacked.
    - [redacted] stated the fact that this board was not adequately socialized within DHS and to Congress was a key problem. She stressed a lesson learned for the subcommittee to socialize the work they are doing prior to the CSAC June Quarterly Meeting. She identified an action item to obtain permission to discuss to outside groups who may be skeptical about this work to help get them on board. Ms. Wyman encouraged the group and CISA to build stronger partnerships with civil rights and civil liberties advocates moving forward.
    - Considering these expressed concerns, subcommittee members recommended removing recommendations from their June deliverables that include social listening. [redacted] recommended returning to the discussion of the subcommittee's name at a later date.

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] asked subcommittee members to review the document of draft recommendations in preparation for the CSAC June Quarterly Meeting and began discussion on specific recommendations. Subcommittee members agreed that topics on building trust should be saved for later discussion in preparation for future quarterly meetings. [redacted] commented that while the subcommittee is advancing specific proposals, they should also advance outlined operating procedures for CISA's consideration. She emphasized the need for CISA to maintain the role as a resource, rather than pushing out information. Subcommittee members described the importance of CISA's convening power out of a service to other organizations rather than being prescriptive in the information provided.

- Subcommittee members discussed whether CISA should solely maintain a convening and resource-sharing role.
  - [redacted] questioned how to view this convening role while CISA releases educational messaging on cybersecurity that aims to push towards larger audiences. She encouraged subcommittee members to consider the delta between proactive organizations that rely on CISA as a resource of information and those that perceive information sharing as government overreach.
  - Ms. Wyman added that this questioning is the healthy part of elections in our democracy. She stated that CISA needs to occupy the space that provides information that educates the public on how the process works, leaving the public to believe those results, rather than force the public to trust that elections are run ethically. [redacted] stressed the difference between good faith questioning versus the exploitation of information techniques that cause questioning by issuing unfalsifiable claims.
  - [redacted] emphasized the difference between CISA releasing educational information prior to an event versus highlighting after the fact that it was secure. She recommended that CISA remain transparent in all information sharing processes and release authoritative findings or resources for assessing information to the public, rather than label this practice "rumor control."
  - [redacted] explained the importance of providing enough information without being too complicated to get taken out of context. In election spaces, she described the need to provide enough information preemptively to counter narrative attacks.

- [redacted] asked subcommittee members to prepare for the reality that there might be election mischief. She explained that the task is not solely to reassure the public about election legitimacy, but the need for paucity of information in what CISA releases. Subcommittee members commented that while they are utilizing election-specific cases, the need to be thoughtful and purposeful in the words we use exists across all spaces.

- Subcommittee members continued to discuss potential recommendations to pose to CISA. [redacted] reminded subcommittee members of the importance of resilience efforts to manage the consequences of MDM in their recommendations.

- Subcommittee members updated a document of initial recommendations they plan to present during the CSAC June Quarterly Meeting. The finalized document will be made public prior to the meeting.

- [redacted] thanked the subcommittee members for their participation and adjourned the meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Action Items

- A1: Subcommittee members will refine the list of recommendations to present for Committee vote during the CSAC June Quarterly Meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
	CISA
	CSIS
[redacted]	Illinois Emergency Management Agency (IEMA)
Ms. Kim Wyman	CISA

Other Meeting Attendees

Name	Organization
[redacted]	CISA
	CSIS

Government and Contractor Support

Name	Organization
[redacted]	CISA
	TekSynap

**Meeting was held via Teams/teleconference*

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
April 29, 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 draft recommendations and begin to identify initial recommendations to CISA to present during the CSAC June Quarterly Meeting.

Discussion

- [redacted] Alternate Designated Federal Officer (ADFO) for the CSAC, brought the meeting to order, reviewed the CISA Director's expectations for deliverables for the CSAC June Quarterly Meeting, outlined the timeline for crafting recommendations to CISA, and turned the meeting over to MDM Chair, [redacted]
- [redacted] University of Washington, MDM Subcommittee Chair, asked subcommittee members to determine the subcommittee's preparedness to deliver recommendations for consideration during the CSAC June Quarterly Meeting. She asked the subcommittee to review a document with framing questions and a lightweight structure of recommendations before opening the call for further discussion.
- Subcommittee members discussed potential recommendations to pose to CISA. [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, recommended keeping the aperture of recommendations broad regarding media to prevent the subcommittee from limiting recommendations to just social media. [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), highlighted a role of government to fund research to identify media best practices for countering MDM.
- Subcommittee members questioned how CISA can measure success to evaluate if the recommendations provided by the Committee are working.
    - [redacted] recommended the subcommittee develop metrics for CISA to utilize such as establishing a determined number of points of contact for key stakeholders, helping to broker a certain number of channel concerns to media, researching the impact through focus group feedback. Subcommittee members identified the difficulty in measuring success in a developing landscape but recommended that the media focus first on evaluating the time between recognizing MDM, and the time of response.
    - [redacted] encouraged subcommittee members to determine their overall goal and questioned whether that is 1) reducing the overall amount of MDM or 2) increasing public education and awareness to a level where the overall impact of MDM is reduced.
        - Mr. Geoff Hale, CISA, shared that CISA defines the overall goal as "to reduce Americans' engagement with MDM."

CISA CYBERSECURITY ADVISORY COMMITTEE

- [redacted] stated the need to identify best practices for media to call out and respond to MDM but questioned whether the government was best positioned to act as the clearing house for information. [redacted] expressed concern over CISA's resilience through change in administrations and emphasized the need to be transparent when evaluating best practices.

- Returning to the discussion of metrics to evaluate success, [redacted] noted that social media companies attempt to measure qualitative metrics in addition to quantitative metrics. She shared that Twitter evaluates the level of harm done in MDM incidents. [redacted] also recommended the quantitative metric of how many counter-narratives an organization can issue in response to identified MDM claims.
    - Mr. Hale commented that it would be appropriate to ask CISA to sponsor, fund, or be the requirements-holder for a potential longitudinal study on measure of the effectiveness of certain mitigations.
    - In response to the suggestion to track the amount of counter-narratives issued in response to a claim, Mr. Hale alerted the subcommittee of CISA's limitations in countering politically charged narratives. [redacted] recommended that CISA develop and publicize a list of what types of claims they will issue a response to.

- Subcommittee members recognized that public confidence in the legitimacy of the courts system can be subject to MDM and stressed the importance of CISA's role to point the public to a trusted source, as to not to affect the credibility of the courts.
    - [redacted] recommended that courts publicize information on their websites to alert the public of the procedural information. Subcommittee members agreed that CISA and other clearing houses are then able to redirect false claims to websites to inform the public of procedural information.

- Subcommittee members agreed to issue at least one recommendation for full Committee vote in preparation for the CSAC June Quarterly Meeting. [redacted] clarified that the vote would take place during the open session at the CSAC June Quarterly Meeting, with the public participating virtually.

- Subcommittee members decided they are not currently on track to make a recommendation concerning privacy and social listening, and plan to push the recommendation to a broader governing body such as Congress. [redacted] stressed that this is the most sensitive recommendation and could overshadow other recommendations posed by the subcommittee.

- [redacted] reviewed the path forward on how to scaffold recommendations and prioritized the following items:
    - CISA's role in convening media and governing bodies to share best practices,
    - CISA's role in outlining specific metrics to track the success of the recommendations,
    - Resilience efforts should be reserved for future recommendations, and
    - Partnership with media companies in preparation for the election season. CISA should work to ensure specific points of contact are identified to strengthen communication between targets of MDM and media or the delivery mechanism of the attack.

- [redacted] thanked the subcommittee members for their participation and adjourned the meeting.

CISA CYBERSECURITY ADVISORY COMMITTEE

Action Items

- A1: Subcommittee members will outline the structure of the recommendations for the CSAC June Quarterly Meeting prior to the next subcommittee meeting.
- A2: CSAC Support Staff will determine if the subcommittee's recommendation to push an item to a higher governing body for final decision should be listed as a formal recommendation, or part of the larger discussion.
- A3: [redacted] will determine additional qualitative metrics for consideration, in addition to harm.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
[redacted]	CISA
	CSIS
	Illinois Emergency Management Agency (IEMA)

Other Meeting Attendees

Name	Organization
[redacted]	IEMA
	CISA
Ms. Allison Snell	CSIS
[redacted]	CISA
	JPMorgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	CISA
	TekSynap

Meeting was held via Teams/teleconference

CISA CYBERSECURITY ADVISORY COMMITTEE

Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee Meeting
March 1, 2022

Purpose of Meeting

- The purpose of the CISA Cybersecurity Advisory Committee (CSAC) Protecting Critical Infrastructure from Misinformation & Disinformation (MDM) Subcommittee meeting was to receive a briefing from Ms. Laura Dehmlow, Section Chief, FBI's Foreign Influence Task Force (FITF), regarding the FBI's Roles and Responsibilities in Combating Foreign Influence.

Discussion

- [redacted] Designated Federal Officer (DFO) for the CSAC and the MDM Subcommittee brought the meeting to order and turned the meeting over to the Chair, [redacted]
- [redacted] University of Washington, MDM Subcommittee Chair, introduced Ms. Dehmlow to provide an overview of the FITF's mission charter.
- Ms. Dehmlow proceeded to give background on the FITF with its start in 2016, focusing on the Russian influence on the elections and then based on mission scope, became an eighty-person organization within the FBI's Counter Intelligence Division. The office established the charter of Foreign Malign Information (FMI), which is subversive data utilized to drive a wedge between the populace and the government. Categories of MDM the FBI addresses are:
    - Undeclared – covert intelligence and activities are not transparent
    - Criminal – cyber violations or election crimes such as voter suppression
    - Coercive Activity – attempting family, political, or economic coercion
    - Foreign Actors – FTIF focuses on "actors" and "activities", not content

  The FTIF engages with policy makers on the Hill and with appropriate partners for information exchange. It also works with the Department of Justice (DOJ) related to what does and does not apply based on the Foreign Agents Registration Act (FARA).

- [redacted] thanked Ms. Dehmlow and opened up the meeting for questions and comments by the Subcommittee Members.
    - [redacted] asked for verification from Ms. Dehmlow that MDM is only monitored or under the purview of the FBI/FTIF based on the connection to Foreign or Criminal activity. FBI does not perform narrative or content-based analysis. [redacted] thought CISA might have a role based on the Subcommittee helping to define the narrative so the "whole of government" approach could be leveraged.
    - [redacted] further asked if there were adequate laws in place around MDM related to elections in order for the FBI to pursue misinformation. Ms. Dehmlow mentioned there were adequate laws

CISA CYBERSECURITY ADVISORY COMMITTEE

in place particularly related to threats of violence at polling locations and interstate harassment; however, integrity of election results might be another matter.

- There was discussion between team members related to organizational information sharing between public/private sector; how to collaborate across channels; driving resiliency building and education about MDM; with FBI focused on foreign efforts, how do we disentangle foreign actors embedded in the MDM process; and, what is the government's strategic approach related to MDM? Ms. Dehmlow was asked to provide her thoughts or to define a goal for approaching MDM and she mentioned "resiliency". She stated we need a media infrastructure that is held accountable; we need to early educate the populace; and that today, critical thinking seems to be a problem currently. [redacted] Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), stated that civics education should be provided at all ages.

- [redacted] asked the members for additional comments with regards to the Subcommittee's way forward. A series of questions was identified in order to move toward providing an approach or recommendation on MDM.
  - [redacted] mentioned, "How do we get to push the envelope to obtain traction in this area? Who has done appropriate social media monitoring for the government?'
  - [redacted] Advisor, Illinois Homeland Security, and Director, Illinois Emergency Management Agency (IEMA) asked, "Who is doing the analysis and has the reach of MDM?"
  - Ms. Kim Wyman, Senior Election Security Lead, CISA, identified a study out of Stanford University and stated a recommendation was for social media companies not to promote MDM actors, which would reduce the promulgation of information from these people.
  - [redacted] Legal, Public Policy, and Trust and Safety Lead, Twitter, stated Twitter utilizes a "three strike system" to de-amplify bad actors.

- The next meeting date was set for March 15 and the meeting was adjourned.

CISA CYBERSECURITY ADVISORY COMMITTEE

Attendees*

Participants

Name	Organization
[redacted]	University of Washington
Mr. Geoff Hale	Twitter
[redacted]	CISA
Ms. Kim Wyman	CSIS
	Illinois Emergency Management Agency (IEMA)
	CISA

Other Meeting Attendees

Name	Organization
Ms. Laura Dehmlow	FBI
[redacted]	CISA
Ms. Allison Snell	CSIS
[redacted]	IEMA
	CISA
	JP Morgan Chase

Government and Contractor Support

Name	Organization
[redacted]	CISA
	MountChor Technologies
	TekSynap
	MountChor Technologies
	Arcfield
	Arcfield
	TekSynap
	Arcfield

Meeting was held via Teams/teleconference

Sent: 3/16/2022 2:03:56 PM
To: [redacted]@fb.com]; [redacted]@fb.com]
CC: [redacted]@fb.com]; Hale, Geoffrey (He/Him) [redacted]@cisa.dhs.gov]; Wyman, Kim (She/Her/Hers) [redacted]@cisa.dhs.gov]; [redacted]@cisa.dhs.gov]
Subject: RE: Comms Check

We're also gong to need dial

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

From: [redacted]@fb.com>
Sent: Wednesday, March 16, 2022 2:03 PM
To: Protentis, Lauren <[redacted]@cisa.dhs.gov>; [redacted]@fb.com>
Cc: [redacted]@fb.com>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) <[redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Re: Comms Check

use this instead: [redacted]

Join our Cloud HD Video Meeting

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars across mobile, desktop, and room systems. Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle, and training rooms, as well as executive offices and classrooms. Founded in 2011, Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Zoom is a publicly traded company headquartered in San Jose, CA.

fb.zoom.us

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>
Sent: Wednesday, March 16, 2022 11:01 AM
To: [redacted]@fb.com>
Cc: [redacted]@fb.com>; [redacted]@fb.com>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) <[redacted]@cisa.dhs.gov>; [redacted] <[redacted]@cisa.dhs.gov>
Subject: RE: Comms Check

Hi [redacted] We're getting an invalid meeting link message. Are you getting the same? Can you send along an updated link?

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

From: [redacted]@fb.com>
Sent: Wednesday, March 16, 2022 1:37 PM
To: Protentis, Lauren [redacted]@cisa.dhs.gov>
Subject: Re: Comms Check

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

[redacted]

I think this is because we have separate emails (with dial-in instructions) for you (for our USG partners) and the rest of industry (that [redacted] shares with our peers).

They are the same link. Note the meeting ID's & passcodes are the same in both links. (FYI—I asked [redacted] to fix it after our last call ☺)

Also, I may come back to you separately on sharing our security measures. We have a whole team that works with election officials, etc. I thought it might be helpful to sked a sync with you & them.

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>
Date: Wednesday, March 16, 2022 at 10:25 AM
To: [redacted]@fb.com>
Subject: Comms Check

Hi [redacted]

For our last call, we somehow ended on different zoom links. Can you check to make sure this is the info your side will be dialing in from? Thank you!

Join Zoom Meeting
[redacted]

Meeting ID: [redacted]
Passcode: [redacted]

Computer or mobile guest sharable join link
[redacted]

One tap Mobile
[redacted] US (San Jose)
[redacted] US (San Jose)

Dial by your location
toll: [redacted] (San Jose US)
toll: [redacted] (Houston US)
toll: [redacted] (Tacoma US)
toll: [redacted] (Washington DC US)
toll: [redacted] (Chicago US)
toll: [redacted] (New York US)
tollfree: [redacted] (US)
tollfree: [redacted] (US)
tollfree: [redacted] (US)
tollfree: [redacted] (US)
Meeting ID: [redacted]
Passcode: [redacted]

Join by SIP:
[redacted]

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

Sent: 2/18/2022 5:14:31 PM
To: [redacted]@fb.com]
CC: [redacted]@fb.com]; [redacted]@fb.com]; Snell, Allison (She/Her) [redacted]@cisa.dhs.gov]; Hale, Geoffrey (He/Him) [redacted]@cisa.dhs.gov]; [redacted]@cisa.dhs.gov]; [redacted]@cisa.dhs.gov]
Subject: RE: Proposed Engagement Next Week: Industry and Sector Risk Management Partners

Great – thanks for your offer to give our industry partners advanced notice.

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

From: [redacted]@fb.com>
Sent: Friday, February 18, 2022 4:19 PM
To: Protentis, Lauren <[redacted]@cisa.dhs.gov>
Cc: [redacted]@fb.com>; [redacted]@fb.com>; Snell, Allison (She/Her) [redacted]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Re: Proposed Engagement Next Week: Industry and Sector Risk Management Partners

Many thanks, Lauren.

First, we haven't yet heard from Treasury yet but look forward to connecting with them. We appreciate you connecting us.

Additionally, we are happy to participate in your forum next week and also (if helpful) happy to flag for our industry partners that you and your team will be reaching out on this. Let us know if you would like us to do that.

With regard to the forum, we think it is best for CISA to invite/ask other companies to participate.

Lastly, we look forward to hearing more from you next week. Please feel free to reach out to me over the weekend if you need anything. We are here to help.

Best,
[redacted]

On Feb 18, 2022, at 3:16 PM, Protentis, Lauren [redacted]@cisa.dhs.gov>wrote:

Hi [redacted]

Thanks for your prompt response to our request yesterday; if the Department of Treasury hasn't reached out yet, I suspect they will soon.

Relatedly, as Russian-Ukrainian geopolitical tensions escalate, CISA is looking to convene our industry partners and our critical infrastructure Sector Risk Management Agencies (IT, telecommunications, finance, energy, etc.) to discuss potential risks, response postures, and opportunities for coordination. We wanted to gauge interest in such a convening and whether or not, you/META would like to serve as the facilitator with your industry partners, or if you would prefer that we engage everyone directly?

The intent of the forum would be to share the current threat landscape and information across the two groups, along with our interagency partners, similar to what we do in the election security space.

If of interest and value, we'd work with you to set up an agenda setting call early next week (feel free to offer times that work for you) with this group and our SRMA coordination team. Following that call, we'd target setting up the larger call with your partner and the Sector Risk Management Agencies in the days after.

Let us know if you have any questions.

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

Sent: 2/17/2022 2:45:56 PM
To: [redacted]@google.com]
Subject: RE: Connection Request: Dept. of Treasury

Sure, I should have mentioned that in my initial note.

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

From: [redacted]@google.com>
Sent: Thursday, February 17, 2022 2:43 PM
To: Protentis, Lauren [redacted]@cisa.dhs.gov>
Subject: Re: Connection Request: Dept. of Treasury

Hi Lauren,

I didn't appreciate there was an urgency. Sorry for the lag. Please pass along my contact information. Depending on what the topic is, I may need to pull in others.

Thank you.

[redacted]

On Thu, Feb 17, 2022 at 10:56 AM Protentis, Lauren <[redacted]@cisa.dhs.gov> wrote:

Hi [redacted]

Apologies for the second email, this is somewhat time-sensitive, so thank you for your prompt attention to this request! Let me know if you have any questions.

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency

O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

From: Protentis, Lauren
Sent: Thursday, February 17, 2022 9:41 AM
To: [redacted]@google.com
Cc: Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; [redacted]@cisa.dhs.gov>
Subject: Connection Request: Dept. of Treasury

H[redacted]

I hope this email finds you well. The Department of Treasury has asked our team for appropriate POCs to discuss social media and influence matters. We'd like to make the connection to Google if you're amenable? If there's another POC this should be routed to, please let us know!

Thanks in advance.

All my best,

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov | CLAN: [redacted]@dhs.ic.gov

Sent: 11/3/2020 3:38:07 PM
To: [redacted]@fb.com]; Scully, Brian [redacted]@cisa.dhs.gov]
CC: [redacted]@fb.com]
Subject: RE: Election Misinformation Confirmation Requested

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
[redacted]@hq.dhs.gov

From: [redacted]@fb.com>
Sent: Tuesday, November 3, 2020 3:31 PM
To: Scully, Brian [redacted]@cisa.dhs.gov>; Masterson, Matthew <[redacted]@cisa.dhs.gov>
Cc: [redacted]@fb.com>
Subject: Election Misinformation Confirmation Requested

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian and Matt,

Can you please confirm the below is election misinformation?

https://mobile.twitter.com/peterjhasson/status/1323716141202739201?s=21

Thank You,
[redacted]

Sent: 8/11/2020 2:13:42 PM
To: [redacted]@fb.com]; Scully, Brian [redacted]@cisa.dhs.gov]
CC: [redacted]@fb.com]; [redacted]@fb.com]
Subject: RE: Draft August 2020 Agenda for USG/Industry Meeting

[redacted] thanks. I know WSJ reached out for comment but not sur

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
[redacted]@hq.dhs.gov

From: [redacted]@fb.com>
Sent: Tuesday, August 11, 2020 2:12 PM
To: Masterson, Matthew <[redacted]@cisa.dhs.gov>; Scully, Brian <[redacted]@cisa.dhs.gov>
Cc: [redacted]@fb.com>; [redacted]@fb.com>
Subject: Re: Draft August 2020 Agenda for USG/Industry Meeting

Matt,

Thanks for the quick reply and for forwarding to your partners.

On your other question, our desire to make a statement has been in the "works" for a while—it just took us time to coalesce and pull it together. Bottom line--we have wanted to highlight all the good work we have done together; it is It is unrelated to the WSJ story.

From: [redacted]@cisa.dhs.gov" [redacted]@cisa.dhs.gov>
Date: Tuesday, August 11, 2020 at 1:58 PM
To: [redacted]@fb.com>, "Scully, Brian" [redacted]@cisa.dhs.gov>
Cc: [redacted]@fb.com>, [redacted]@fb.com>
Subject: RE: Draft August 2020 Agenda for USG/Industry Meeting

Thanks [redacted] We will share with our Gov't partners. Is this being offered in part because of WSJ outreach? I spoke off the record with the reporter and reinforced the good work we are all doing.

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
[redacted]@hq.dhs.gov

From: [redacted]@fb.com>
Sent: Tuesday, August 11, 2020 1:56 PM
To: Masterson, Matthew [redacted]@cisa.dhs.gov>; Scully, Brian [redacted]@cisa.dhs.gov>
Cc: [redacted]@fb.com>; [redacted]@fb.com>
Subject: Re: Draft August 2020 Agenda for USG/Industry Meeting

Gents,

Hope you are doing well. We saw your email about the Clemson researchers and are taking a look and will come back on that. Appreciate your sharing and advocacy there.

In the meantime, we wanted to share for awareness that tomorrow after our USG/Industry meeting, the industry side will be releasing the below statement (close hold/under embargo until released), and we wanted to let you know in case you would like to share with the other USG participants?

Separately, would it be possible for DNI attendees on the call to share more detail and color around the Evanina statement released last week? Many of our industry attendees are keen to hear and learn more about this tomorrow during our meeting: https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

Thanks so much, and see you tomorrow!

[redacted]

Joint industry statement:

"For the past several years, we have worked closely to counter information operations across our platforms. We have collaborated in preparation for the upcoming election and regularly meet to discuss trends with U.S. government agencies tasked with protecting the integrity of the election. We held the latest in a series of meetings with government partners today where we each provided updates on what we're seeing on our respective platforms and what we expect to see in the coming months. Specifically, we discussed preparations for the upcoming conventions and scenario planning related to election results. We will continue to stay vigilant on these issues and meet regularly ahead of the November election."

Background:

- Since 2018, the tech industry and U.S. government agencies tasked with protecting the integrity of the election have been regularly meeting to discuss election security and ways to counter information operations across the Internet.
- Among participants in today's industry-government meeting were: Google, Facebook, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).

From: [redacted]@fb.com>
Date: Friday, August 7, 2020 at 8:57 AM
To: Matthew Masterson <[redacted]@hq.dhs.gov>, "Scully, Brian" <[redacted]@cisa.dhs.gov>
Cc: "Snell, Allison" <[redacted]@hq.dhs.gov>, [redacted]@cisa.dhs.gov" <[redacted]@cisa.dhs.gov>, [redacted]@fb.com>, [redacted]@fb.com>
Subject: Draft August 2020 Agenda for USG/Industry Meeting

Brian & Matt,

Provided below is industry's proposed agenda for next week's meeting. Let us know if you have any questions.

Best,
[redacted]

[redacted]

August 2020 USG/Industry Meeting

- 10 minutes: Dial In/Opening
  - 30 minutes: Threat Updates
    - Threat update from USG (FBI, I&A)
    - Threat update from industry (TW, FB, GOOG)
  - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
    - Election process update from USG (Vote-by-Mail, Polling Places, Poll Workers, and Election Results)
    - Threat Landscape in Advance of the Conventions & Debates
    - Election Day Coordination
  - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

From: "Scully, Brian" [redacted]@cisa.dhs.gov>

Date: Tuesday, April 21, 2020 at 2:40 PM

To: [redacted]@fb.com>, [redacted]@fb.com>

Cc: [redacted]@cisa.dhs.gov" [redacted]@cisa.dhs.gov>

Subject: Call with NASS, NASED, and Center for Internet Security

[redacted]

Hope this finds you and the family well. The Center for Internet Security, which manages the Election Infrastructure ISAC, is developing a portal to facilitate reporting from State and local election officials. The idea is to establish a centralized portal for reporting disinformation or other issues on platforms so that election officials only have one place to go to report. NASS and NASED support use of this portal and have asked CISA to facilitate a meeting with you all to discuss further. Would you, and anyone at Facebook you think appropriate, have time for a call with NASS, NASED, CIS and CISA over the next week or two?

Thanks,

Brian

Brian Scully

Chief, Countering Foreign Influence Task Force

DHS/CISA/NRMC

[redacted]@cisa.dhs.gov