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>