The CSAC Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee has been tasked with advising CISA on how to use its unique capabilities to help address the societally critical challenges of mis- and disinformation. Here, we provide an initial set of recommendations.

Defining CISA's Mission in the Information Space

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 those critical functions. CISA should take a similar risk management approach to these risks that it takes to cybersecurity risks.

The interlinked problems of misinformation, disinformation, and malinformation (MDM) represent a critical challenge for democratic societies. Borrowing from a growing body of research (cite, cite, cite), 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, particularly, poses a significant risk to critical societal 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 (Rid, 2020). Pervasive mis-, dis-, and malinformation diminish trust in information, in government, and in the democratic process more generally. They can undermine the perceived legitimacy of elections, the judiciary, and other democratic institutions (cite). And they can destabilize the common ground that democratic societies need to stand upon to govern themselves (cite).

The initial recommendations from the subcommittee focus primarily on mis- and disinformation about election procedures and election results. Future recommendations may seek to address more fully 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 mis- and disinformation, 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 these risks and provide a robust set of best practices related to transparency and communication when addressing mis- and disinformation, specifically in the election context.

Focusing on MD and Critical Infrastructure

CISA is positioned to play a unique and productive role in addressing the challenges of mis- and disinformation — especially in regards to protecting critical infrastructure such as that related to elections.

CISA should focus on addressing 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 other key democratic institutions, such as the courts, or key functions, 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 what the organization does to detect, warn about, and mitigate other threats to critical functions — e.g. cybersecurity threats.

The initial recommendations from the subcommittee focus primarily on mis- and disinformation 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 elections can reduce confidence in procedures and results. Perhaps more problematically, the proliferation of false and misleading claims about elections can generate noise that may make it difficult to identify and counter any real threats to election integrity — for example 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 do their critical work of administering our elections while responding to an overwhelming amount of inquiries (including false and misleading allegations). Some are even experiencing physical threats. CISA should be providing support — through education, collaboration, and funding — for election officials to pre-empt and respond to mis- and disinformation. Here we provide some specific recommendations for how to do this.

Maintaining a Broad Aperture 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 (cite). 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 in regards to these issues may not accurately represent the proportionality of their role. These sites are part of a broader ecosystem that includes other online websites (including state-run media like RT and gray propaganda networks associated with Russia, China, and Iran) and more traditional media (such as 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, mainstream media, cable news, hyperpartisan media, talk radio, and other online resources. In regards to social media, in addition to the most popular platforms, CISA should maintain awareness of activity across the broad spectrum of social media platforms[1].

Four Dimensions of CISA MD Mission

Leveraging the unique capabilities of the organization, CISA's MD mission has multiple dimensions — from improving the public's resilience to MD generally, to communicating about specific MD threats both preemptively and retroactively, to identifying and counteracting actor-based threats from foreign and/or criminal actors.

CISA should work across four specific dimensions:

- **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 just 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 engage in content- and narrative-specific mitigation efforts. 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

[1] Informational threats (including disinformation campaigns) often take shape across multiple platforms. Smaller, niche platforms are used to organize. Platforms like YouTube can become resources. And mainstream platforms like Facebook and Twitter are used to mobilize content for widespread visibility.

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 will need to 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 foreign threats.
- **Countering Actor-Based Threats.** CISA should work collaboratively with other governmental organizations to identify, communicate, and address actor-based MD threats — i.e. 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, we have two time-sensitive recommendations related to the 2022 election.

- **CISA should support local election officials in producing a "What to Expect on Election Day" plan** to proactively address — through education and communication — misleading narratives that may arise due to the specific contours of their election materials and procedures. 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**, bringing 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 (convene by 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 dis- and mis-information that poses a significant threat to critical functions. If possible, CISA should also support external organizations doing mis- and disinformation 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 all of 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 urgency, while being accurate and thoughtful

How Do We Measure Success

To understand the impacts of mis- and disinformation — 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 mis- or disinformation 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[2].

CISA should work internally and with collaborators to develop metrics for measuring the impacts of its efforts. 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.).

[2] Thomas Rid's "Active Measures" (2020) explains how active measures (which include dis- and malinformation) can be viewed through the lens of the "social construction of reality" — not as a descriptive theory, but as a prescriptive one, where the perpetrators attempt to shift perceptions of reality and the organization of social life in ways that have lasting, but diffuse effects. Rid stresses that measuring the impact of these efforts can be extremely challenging.

- 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.

For future discussion

Building and Maintaining Trust Through Collaboration

Framing Question:

- 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”?

Suzanne: Some people, including the media. see CISA as an authoritative source. Others will mistrust it. CISA should be mindful of this latter group but not abjure its role because of it. CISA should be a clearinghouse for authoritative and trusted sources. CISA should also provide information to outside researchers and others.

Kate: Collaborating. Maintaining transparency.

Vijaya: Transparency

Framing Question

- What is the right model for CISA engagement with social media and other media entities?

Suzanne: CISA can be a poc, or help identify other poc's, between MDM targets and SM/media companies. CISA can also help educate SM/media about the role they play in MDM, and the role they could play in mitigating the threat through educating the public and building resilience. Facilitate conversations between targets of MDM and vectors (media and social media)

Social Listening, Privacy, and Protected Speech

This committee has been asked the following set of questions:

- How should CISA and the USG maintain situational awareness of MD and detect efforts to manipulate the information environment? What is the balance between social listening, privacy, and protected speech?

These questions are broader than this committee and broader than CISA. We recommend CISA use their convening authority to bring together the government and civil society to understand the objectives and limits of this work, who are the appropriate people to do this, current legal frameworks, and what changes might be needed.

Local election offices are increasingly unable to accept outside funds to help them ... so it will likely be CRITICAL that CISA provide resources for them. We may want to remove the external funding and focus on that?

Identifying the Societal Objective

Before addressing CISA's specific mission, it is important to enumerate a set of broader goals for a society-wide response to mis- and disinformation (MD).

CISA's work in this space should align with broader societal objectives for addressing mis- and disinformation, that include the following aims, ranked in order of priority:

- Iincrease individual and societal resilience to mis- and disinformation.
- Disincentivizeing the use of mis- and disinformation by both foreign and domestic actors to help reduce the prevalence of mis- and disinformation negatively impacting critical functionsacross society, including by
- Increase access to first-hand or otherwise authoritativedirect sources of information. Increase the speed with which MD is countered