CISA CYBERSECURITY ADVISORY COMMITTEE

REPORT TO THE CISA DIRECTOR

Strategic Communications

October 11, 2024

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established a Strategic Communications (SC) subcommittee (hereinafter referred to as the "subcommittee") to examine how CISA can ensure that its strategic communications efforts align with agency goals, raise awareness of what CISA is and does, and provide actionable guidance to CISA's key stakeholder groups.

Since its inception in 2018, CISA has been working to build awareness of its mission and services. In 2023, CISA released a comprehensive Strategic Plan which includes a Strategic Communications plan. As part of these plans, CISA has implemented several key initiatives, including establishing the Joint Cybersecurity Defense Collaborative (JCDC), its Secure by Design campaign, and its first public service announcement, Secure Our World.

Some of CISA's key stakeholder groups/constituencies include:

- Citizen/Consumer
  - Private citizens who must remain safe in their online transactions.
  - Technology professionals and cybersecurity experts with whom CISA collaborates, including members of the Cybersecurity Advisory Committee's Technical Advisory Council.

- Government
  - State, county, city, and tribal governments, including those responsible for critical infrastructure (including election security) and information security of government systems.
  - Other U.S. federal agencies, with which CISA collaborates and to which CISA delivers capabilities.
  - The U.S. Congress, which authorizes and funds CISA's mission.

- Corporate
  - Critical sector companies in the U.S.
  - All U.S. companies.

The questions posed to the subcommittee by the CISA Director were as follows:

1. How should CISA position itself to ensure stakeholders across the board, and the American people more broadly, know what CISA is, what we do, and the value we add to reducing risk to the nation? What are the most effective ways to communicate this to the American people?

2. How can CISA best encourage consumers to take action through the agency's messaging efforts? CISA is currently distributing information via HSIN, the CISA.gov website, email, and social media channels including X, Threads, LinkedIn, Facebook, and Instagram. In addition, the agency also leverages traditional media and public engagements to promote CISA products and guidance. Are there other communications channels or communications products that the agency could be using that it is not right now to reach different and unique audiences?

Findings:

A solid and well-resourced strategic communications function is critical to ensuring that CISA's messages are heard and trusted by stakeholders, which is foundational to a resilient society. For such a young agency with comparatively limited resources, CISA has done an excellent job of reaching and building trust within a diversified group of stakeholders. Since CISA's creation, the U.S. government has significantly increased the guidance, support, and resources it provides to owners and operators of critical infrastructure to better protect these critical assets from cyber threats and physical attacks. Critical infrastructure in the U.S. has increasingly come under threat from adversaries due to various factors, including the critical sectors' increased reliance on communications technology, the strategic value of critical infrastructure targets, and the growing sophistication of cyber-attacks. Cyber attackers have discovered increasingly novel ways to target and monetize infrastructure such as power grids, water systems, health delivery organizations, and transportation systems. CISA has improved the efficacy of delivering this guidance, support, and resources to the critical sectors. CISA's campaigns designed to explain policy, convey warnings (e.g. Shields Up), provide context around emergency or binding operational directives, and educate have been especially impactful. Further, through CISA, the U.S. government has, for the first time, delivered programming aimed at informing and changing the behavior of the U.S. public to help build a more cyber-resilient society.

CISA is not a traditional regulatory agency. It cannot require stakeholders to do things the way regulatory agencies can. Therefore, CISA must rely on its ability to convince its stakeholders to take recommended actions, and it can only do this if its messages are heard and trusted. CISA needs more capacity to reach stakeholders and must employ different strategies to reach different stakeholder groups. The subcommittee also noted that trust and confidence in CISA's brand will be critical to the agency's ability to recruit top talent.

The subcommittee heard from subject matter experts leading communications and branding strategies at the National Aeronautics and Space Administration (NASA), the American Association of Retired Persons (AARP), Blackbird.AI (a firm specializing in combating disinformation and narrative attacks), and former representatives from the Federal Bureau of Investigations (FBI).

Recommendations:

1. Right-size CISA's Strategic Communications function to meet growing demand.

   Almost all other U.S. agencies with heavy public-facing missions have exponentially larger strategic communications budgets than CISA. The ability to reach all its intended stakeholders and create programs that genuinely build trust within them is directly linked to the resources available to support CISA's strategic communications strategy. Given the number and diversity of its stakeholders – namely, all American citizens – CISA needs more capacity. In particular, it must further mature and expand its crisis communications capabilities. In the July 2024 incident that crashed millions of computers worldwide, users turned to the Internet, including Reddit threads, for help getting technical information but had no means to verify the validity of the information they were getting. The Subcommittee recommends that CISA initiate a discussion with other relevant government partners that considers how the policies, procedures, and authorities in place for disseminating accurate information and technical assistance to stakeholders in the event of large-scale cybersecurity incidents or IT outages be improved in a unified manner.

2. Develop key performance indicators for its strategic communications efforts and measure achievement of these.

   CISA has already measured the effectiveness of its strategic communications efforts through methods such as tracking the number of news articles featuring CISA, social media engagements across platforms (Facebook, Twitter, and LinkedIn), speaking engagements supported by External Affairs ranging from Director to Deputy Director and Executive Assistant Directors and visitors to CISA.gov. However, CISA could develop more sophisticated key performance indicators, both quantitative and qualitative, to measure the success of CISA's communications strategy. This is partially addressed in the next paragraph on adopting new technologies. As

CISA develops more ambitious communications campaigns, it must evaluate the success of the campaigns, for example, through sentiment analysis or message "uptake" by constituent groups. CISA must set clear benchmarks for its communications campaigns targeting its various stakeholder groups, which CISA develop against internal and external benchmarks. The progress made by U.S. health agencies in catalyzing vaccine adoption could provide such external benchmarks, for example. More methods of measurement of attainment of goals and more diversified metrics will give CISA a far more nuanced understanding of the effectiveness of its communications strategy and will help it to optimize the use of its minimal resources.

3. Incorporate communications strategies implemented by other U.S. agencies that have effectively cultivated stakeholder trust.

   CISA's mission is ultimately to get its stakeholders to act, not just inform them. They will not follow CISA's guidance if they do not have trust and confidence in CISA. The main goal, therefore, of CISA's strategic communications effort, above all else, is building trust and confidence amongst its stakeholder groups. CISA should thoroughly study the creative ways other U.S. agencies have, over time, stimulated interest in and cultivated trusted relationships with stakeholders and built brand trust within their various stakeholder groups. CISA can identify new and unique ways to connect more effectively and authentically with its own stakeholder groups through this study. NASA has helped build a generation of scientists by sending astronauts and other employees to U.S. schools. It also works cooperatively with private companies, including toy manufacturers, to allow less restricted logo use to promote brand awareness. The FBI has created a largely favorable public opinion of the agency by making information and support available to the entertainment industry. CISA is the U.S. government's newest agency and has not had decades to develop and refine its communications strategies like NASA and FBI. However, it can learn techniques from these agencies that CISA could apply to persuade citizens to adopt safe online practices. For example, the subcommittee learned that some agencies extensively use gaming to educate citizens and encourage desired behaviors.

   CISA could better leverage its directors' and other top-level leaders' strengths and personas to cultivate relationships and trust with its corporate stakeholders. CISA has already built a strong public and industry engagement culture, but it can improve by leveraging stakeholders' interest in interacting with and following its key leaders. Additionally, other agencies, such as the FBI, create content and messaging in multiple languages to increase their reach among its intended audiences.

   Lastly, CISA should continue its consistent cadence of media outreach, including, but not limited to, quarterly background briefings with cybersecurity journalists at major media publications, and cybersecurity trade publications, to provide a regular dialogue with them on CISA's top mission and communications priorities.

4. Evaluate the technology platforms it uses to connect with stakeholder groups to identify new ways to connect with them.

   Related to the first recommendation, CISA should thoroughly evaluate the methods through which it reaches stakeholder groups. CISA's communications campaigns must be uniquely designed for each of CISA's stakeholder groups. CISA has begun to successfully reach its public/citizen constituents through its website content and advertising campaigns, but there may be other media through which CISA can reach the public. Some examples include gaming apps or deploying speakers or content in schools. CISA has significantly improved how it reaches its corporate, not-for-profit, academic, and government-based stakeholder groups through public-private partnership initiatives like the JCDC and its program supporting states and regions, but there may be other methods to reach them. CISA could do this by developing more impactful ways to provide value to these stakeholder groups, such as augmenting the services it already provides and further defining itself as the place to turn for these entities to achieve cyber resiliency to prevent breaches and to access resources and guidance in the event of a breach.

5. Explore the use of additional technological capabilities to measure the effectiveness of CISA's strategic communications strategy and identify and counteract damaging counter narratives.

   CISA utilizes many technologies commonly employed by private sector companies to help evaluate the success of advertising and outreach campaigns. However, some private companies leverage cutting-edge, AI-based technologies to assess impact and trends in far more sophisticated ways than before. These technologies leverage open source, public data, and AI-based analytics capabilities. Laws that govern how U.S. agencies can use data generated from public sources are well-intentioned and necessary but can, in some cases, create limitations for CISA that hamper its ability to carry out its mission to ensure the resilience of the critical sector. CISA must work with legislators and regulators to ensure that it can access and leverage advanced analytics capabilities and have reasonable access to public data to ensure it can effectively measure how it is reaching its stakeholders and evaluate the success of its strategic communications strategy. It must have access to technologies that allow it to identify disinformation and destabilization campaigns aimed at CISA's stakeholder groups and at CISA itself so it can respond and counteract this effort.

Appendix 1:

The following SC subcommittee members contributed towards this report:

- Dave DeWalt, Chair
- Katherine Gronberg
- Niloofar Razi Howe
- Nicole Perlroth
- Ted Schlein
- Kiersten Todt
- Nicole Wong