REPORT TO THE CISA DIRECTOR

Strategic Communications

June 22, 2022

Introduction:

The CSAC Strategic Communications (SC) Subcommittee was tasked to evaluate and make recommendations on expanding CISA's reach with critical partners to help build a national culture of cyber resilience. The recommendations below aim to help promote CISA as a willing and collaborative partner, working arm-in-arm with partners to understand, manage, and reduce risk to cyber and physical infrastructure.

Findings:

CISOs, CIOs, and media representatives have informed the outlined recommendations to better understand the perception of CISA, explore opportunities to improve cyber resilience for the U.S. public, and gauge willingness to participate in campaigns. Based on this work, CISA should implement the following recommendations: (1) "More than a Password" Partnership Program; (2) 311 call line; and (3) building a broader base of support.

Recommendations:

- CSAC recommends that CISA create a **"More than a Password" Partnership program** with Fortune 500 companies. The following steps to roll-out the plan should be considered:
  - CISA should assign a program manager to create the partnership program and work with companies on the best way to amplify the campaign message.
  - CISA should devote resources to creating a "More than a Password" partner portal, marketing materials, including a website and collateral materials.
  - CISA should establish success metrics (e.g., number of companies enrolled in partnership program, etc.).
  - CISA should develop a campaign for "More than a Password" with identified target audiences including:
    - Kids Cyber Education campaign,
    - Senior Cyber hygiene campaign,
    - Celebrity endorsements for campaign, and
    - Faith-based organizations campaign.
  - Once the partnership program is established and meets the outlined metrics, CISA should consider targeting other affinity groups including CISO forum, ISACs, media, schools.

- In support of the recommendation to develop a Cyber 311 Pilot in Austin, CISA should develop a communications plan to amplify the Austin-University of Texas efforts to other cities. This will engage more cities in this initiative and raise awareness of this important work.

- CISA should build out a broader base of support and create new channels for amplifying the agency's key messages.
  - Current and emerging threats such as election interference, mis-, dis-, and mal-information campaigns, network-enabled espionage, ransomware, and IP theft require high levels of response and resiliency across the nation. By building a broader base of support to amplify its cyber hygiene messaging and two-way information sharing with the broadest set of constituents, CISA can increase the nation's resilience to cyber-attacks.
  - CISA should implement the following actions to broaden the agency's base of support for key initiatives:

- Develop a regular cadence of background briefings to cybersecurity reporters.
- Expand the agency's list of validators and create a mechanism to communicate information to validators in real-time. These validators should include individuals and organizations that have broad reach to the American public.
- Capture any messaging (e.g., Shields Up, Russia's invasion of Ukraine, cybersecurity alerts, etc.) and develop narratives to showcase successful messaging campaigns to the public to build trust and confidence in CISA, DHS, and USG writ large.

Conclusion:

CISA has done a tremendous job with stakeholder engagement and public awareness, to date. The outlined recommendations focus on how to amplify key messages, create new programs, and expand reach into a broader audience in order to improve the resiliency of our nation to cyber-attacks.

Acknowledgements:

Members of the SC subcommittee:

Niloo Razi Howe

Ted Schlein

Nicole Perlroth

Mayor Steve Adler

Thank you to the outside experts, CIOs, and CISOs who helped identify the greatest opportunities for increasing resiliency through communication and engagement.