Commission on Enhancing National Cybersecurity- Request for Information
Information Technology-Sector Coordinating Council (IT-SCC)

On behalf of the IT-Sector Coordinating Council (IT-SCC), we respectfully submit the following recommendations in response to the Commission on Enhancing National Cybersecurity's (the 'Commission') Request for Information (RFI) issued on August 10, 2016. For this RFI response, the IT-SCC chose to highlight a select number of recommendations based on common themes identified in the inputs of our member companies and associations. Many of our member companies and associations have also chosen to submit individual RFI responses to the Commission.

Background

The IT-SCC is the principal entity for coordinating with the government on a wide range of critical infrastructure protection and cybersecurity activities and issues. The IT-SCC brings together companies, associations, and other key IT sector participants, to work collaboratively with the Department of Homeland Security, government agencies, and other industry partners.

Recommendations

Foster Continued Maturity and Expansion of the Cybersecurity Framework Model

The development of the voluntary Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") provides an exemplary model for the type of open, collaborative and multi-stakeholder processes that must be embraced and expanded upon by future U.S. Administrations. The Framework leverages public-private partnerships, is grounded in sound risk management principles, provides a common lexicon for talking about cybersecurity risks, and helps foster innovation due to its flexibility and basis in global standards. Though the Framework remains in its infancy, its existence has already fostered conversations that have tangibly improved cybersecurity. These conversations must continue to mature and expand to encompass more of the cybersecurity ecosystem, domestically and globally.

- The Framework model should be built upon as a means to streamline Government regulatory efforts. In particular, promoting the Framework as a common language for policymakers can help align U.S. federal agency cybersecurity and risk management efforts by orienting them toward the Framework, and help expand use of the Framework globally. Especially as the number of internet connected devices proliferates— and lines blur between sectors and geographic borders—the need to commonly develop and promote international and cross-sector cybersecurity standards becomes increasingly essential. Further, since multiple companies in the IT sector provide cybersecurity services to both the government and commercial sectors, alignment of terminology and functions consistent with those of the Framework encourages greater market participation and competition, leading to stronger outcomes.

- Framework discussions should evolve to incorporate the development of metrics and

other more tangible means to measure cybersecurity effectiveness. As outlined in the Executive Order, the focus should be on developing a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to cybersecurity.

Focus on Implementation and Execution of Existing Policies

Through multiple Administrations—from the Comprehensive National Cybersecurity Initiative (CNCI) to legislative actions like the Cybersecurity Act of 2015 and a series of recent Executive Orders—there has been a continuous arc of cybersecurity policymaking progress in the United States. Collectively, these policies have helped clarify statutory cybersecurity responsibilities within the Federal Government, and between the Federal Government and the private sector. We recommend that the Commission thoroughly assess this existing collaborative work and focus on its implementation and execution before making new recommendations to future Administrations.

Continue to Leverage Public-Private Partnerships in Cybersecurity Policy Development

Engagement with private sector entities in the development of cybersecurity policies and practices can lead to stronger security outcomes because of the shared responsibilities of both public and private organizations in promoting stronger cybersecurity. The National Infrastructure Protection Plan, which outlines the government's strategy for engaging with sector coordinating councils in the protection of critical infrastructure, is a good example of these types of partnerships and should be expanded.

Continue to Promote Cybersecurity Information Sharing across the Ecosystem

The U.S. Government has devoted significant resources to fostering an expanded cybersecurity information sharing environment between the public and private sectors, but significant work remains to be done. The effectiveness of sector-specific Information Sharing and Analysis Centers (ISACs) varies significantly, and the Federal Government can play a role in incentivizing strong participation across all sectors by using these forums and emerging ISAOs to deliver timely and highly valuable intelligence on emerging cybersecurity threats. Further, we recommend that the Commission encourage the Federal Government to refine and expedite declassification processes, and more closely evaluate how to leverage and enhance the cyber threat intelligence that exists in private sector information sharing channels. Finally, we recommend that the Commission encourage continued development of automated information sharing mechanisms that can disseminate cyber threat indicators in close to real time.

Cybersecurity Workforce Development: Innovative Approaches to Existing Initiatives

Developing a well-rounded and adequately robust cybersecurity workforce remains a significant problem that will continue through future Administrations and requires innovative solutions. To address this workforce deficit, we recommend integrating cybersecurity education and training into a number of existing initiatives with proven models and the requisite infrastructure, such as leveraging the gaming community, E-Learning platforms, and considering a cyber-specific ROTC program.

Each of these forums aims to reach potentially qualified and interested people where they already exist. Career influencers — including counselors at high schools, community colleges, and universities — also need to be provided with the knowledge and messaging to reach these particular audiences at the formative stages of their lives.

Conclusion

We greatly appreciate the opportunity to contribute to this important dialogue. Should the Commission require any further clarity or additional information on any of the IT-SCC recommendations contained within this response, we would be happy to set up further discussions.