Commission on Enhancing National Cybersecurity- Request for Information
Palo Alto Networks

Palo Alto Networks appreciates the opportunity to respond to the Commission on Enhancing National Cybersecurity's ('Commission') Request for Information (RFI), "Information on Current and Future States of Cybersecurity in the Digital Economy," as issued by the National Institute of Standards and Technology (NIST) on August 10, 2016.

We commend the Commission's efforts—through this RFI and during a series of public meetings throughout the country—to solicit input from a broad range of key cybersecurity stakeholders. This approach soundly recognizes that cybersecurity is a fundamentally distributed problem that can only be effectively addressed through robust public-private sector collaboration. Palo Alto Networks is firmly committed to this principle of shared responsibility. Our Chairman and CEO Mark McLaughlin was honored to provide his expertise on cybersecurity innovation at the June 2016 Commission meeting in Silicon Valley, and we appreciate this opportunity to continue to provide Palo Alto Networks' unique perspective to this important dialogue.

Given the broad scope of the Commission's RFI, Palo Alto Networks has chosen to focus on providing key recommendations on a select subset of the requested issues. Our recommendations reinforce a number of key themes previously highlighted during Mark McLaughlin's June Commission testimony and address additional topics that have been raised at subsequent Commission meetings.

Recommendations

Addressing the modern cybersecurity threat requires a comprehensive approach that effectively leverages innovative principles across people, process, and technology. Our recommendations address all of these categories in recognition that each is an essential component to regaining leverage against our adversaries and actually preventing successful cyber attacks— not simply responding and recovering from such attacks.

Recommendation: Focus on Implementation and Execution of Existing Policies & Authorities

United States cybersecurity policies have benefitted from bipartisan continuity across the Bush and Obama Administrations, and there has been a consistent arc of cybersecurity policymaking progress over this period. These policies—through both legislation and executive action—have addressed a diverse set of issues, including critical infrastructure and federal government cybersecurity, workforce development, and cyber incident management. These policies have clarified and complemented established public-private partnership activities in a productive way, and we recommend that the Commission align any new policy suggestions to build upon and enhance this progress.

Collectively, these policies have also helped foster a shared understanding of the distinct roles, responsibilities and authorities of entities across the cybersecurity ecosystem. In particular, the federal government has made significant progress in more clearly delineating and building operational coordination across the distinct policy, operational and law enforcement authorities held by individual Departments and Agencies. Though work remains, these efforts have subsequently made it easier for the private sector to identify and coordinate with the appropriate government stakeholders on cybersecurity issues. We strongly recommend that the Commission encourages the federal government to continue to refine and clarify these statutory authorities and not create new agencies or reassign the established interagency roles and responsibilities.

Recommendation: Foster Maturity and Expansion of the Cybersecurity Framework Model

The development of the voluntary Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") spearheaded by the National Institute of Standards and Technology (NIST) provides an excellent model of a truly collaborative process that should be replicated by future U.S. Administrations and governments around the world. Substantively, the Framework's establishment of a common cybersecurity risk management lexicon fosters dialogue within organizations and across the interconnected, global cybersecurity ecosystem. This Commission's recommendations can play an important role in continuing to mature the Framework to reflect the evolving cyber threat landscape.

In particular, we believe future discussions of the Framework's core tenets—Identify, Protect, Detect, Respond and Recover— should more closely reflect global security trends towards threat prevention as an integral part of the "Protect" function. While all five Framework tenets are important for security, a particular focus on effective Identification and Protection from the start is critical to actually preventing successful attacks – not simply at the perimeter of a network, but throughout the key points in the lifecycle of an attack. While prevention cannot be absolute, it can be effectively applied to limit an organization's need to devote resources to detecting, responding and recovering after a compromise has already occurred. As cyber attacks become increasingly destructive and the potential for physical damage to industrial control systems and hardware proliferates, it's become clear that a detection and response-focused strategy is no longer tenable.

Recommendation: Incentivize Innovative Approaches to Cybersecurity Education

As this Commission knows well, people are a critical piece in an entity's overall cybersecurity posture and the practice of good cyber hygiene is core to securing an organization's networks. The Commission can play a vital role in making recommendations that increase cyber awareness and education across the country to reduce human vulnerabilities and ensure we are growing the next generation of cyber-savvy citizens.

One recommendation is to integrate cybersecurity education and training into existing and proven content delivery models, such as virtualized, e-learning platforms. These cybersecurity educational efforts need to reach children at the earliest possible age so that cybersecurity is fundamental, hands on, and fully ingrained in educational curriculum.

Conclusion

Adopting these innovative approaches is a critical first step in changing the economics of the cybersecurity problem and driving towards cyber threat prevention. Fundamentally changing the current dynamic requires collective action across the cybersecurity ecosystem, and we greatly appreciate the opportunity to continue to drive this important dialogue forward. Should the Commission require any further clarity or additional information about any of the recommendations contained within this response, we would be happy to set up further discussions. Thank you.