NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Mr. Mark McLaughlin
Palo Alto Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054

March 10, 2016

The Honorable Barack H. Obama
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500

Dear Mr. President:

You requested that your National Security Telecommunications Advisory Committee (NSTAC) share insights from industry experience to support the Government as it harnesses current, emerging, and expected technologies and manages cyber risks. In Phase I of this effort, the subject of this letter, the NSTAC focused on examining current technologies and providing near-term recommendations, aiming to deliver industry insights that can be actioned by your Administration in the immediate future. In Phase II, the NSTAC will assess emerging and expected technologies and deliver longer-term recommendations for the next Administration.

In recent years, technology and the threat landscape have changed dramatically. Mobility, the Internet of Things, and cloud computing are powering more agile and innovative services. At the same time, data breaches have become mainstream news, advanced persistent threats are being reported across sectors, and attacks are having destructive effects. In recognition of these opportunities and challenges, you have prioritized and invested in cybersecurity initiatives to advance our national security and emergency preparedness (NS/EP) functions. The recently released *Cybersecurity National Action Plan* (CNAP), which incorporates key elements of the Office of Management and Budget's "30-Day Cybersecurity Sprint" and the *Cybersecurity Strategy and Implementation Plan* (CSIP), exemplifies this commitment.

Working from a baseline understanding of current Administration initiatives as well as industry's experiences, the NSTAC offers the below summary of our insights and recommendations, which focus on governance and risk management best practices. In addition, we provide more context for and detail about our insights and recommendations in the *Attachment to the Letter to the President – Emerging Technologies Strategic Vision*.

Governance

Through the CNAP, you have taken the important step of establishing a chief information security officer (CISO) role. This action has enormous potential to enhance our Nation's cybersecurity and resiliency. However, additional actions must be taken to realize that potential. According to industry's experience, vital next steps include: (1) clearly defining the CISO's roles and responsibilities in relation to other Federal officials that may have overlapping missions; (2) creating an operating model for regular cross-organizational coordination and collaboration; and (3) projecting meaningful executive-level support for the CISO, recognizing that the process of integrating the CISO into agency activities may be disruptive.

Within the attachment, the NSTAC provides additional detail regarding what industry has learned in taking these steps. In summary, industry CISOs have proven most effective when they have the authority to: assess risks; establish baseline security requirements to manage those risks; measure organizational compliance against those baselines; evaluate whether the baselines are managing risk effectively; and set goals for improvement. In addition, CISOs operate most successfully when they are empowered to work with stakeholders to develop incentives and establish penalties to foster implementation of policies and practices. To enable cross-organizational coordination and collaboration, industry has also found value in establishing an action-oriented cybersecurity council or leadership team that is convened by the CISO.

Risk Management

Through the "30-Day Cybersecurity Sprint" and the CSIP, you have outlined steps to strengthen Federal cybersecurity by developing capabilities to: identify and protect high value assets; and more rapidly detect, respond to, and recover from incidents. Similarly, much of industry approaches risk management by organizing around the five functions described within the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology: identify, protect, detect, respond, and recover. Within the attachment, the NSTAC describes steps that have been vital to industry's successful implementation of those functions. For example, with regard to protection, industry experience has validated the importance of giving rigorous attention to implementing basic cyber hygiene and embracing new technologies and processes to address persistent threats. To detect incidents, industry utilizes integrated, intelligent platforms that enable cross-organizational visibility into configurations, vulnerabilities, and attacks. Industry also increasingly approaches internal testing with a focus on threat isolation and security resiliency. To respond to and recover from incidents, industry has benefitted from developing operational frameworks that enable a standardized approach to incident prioritization and seamless coordination in utilizing expertise to contain the most severe incidents.

The NSTAC has described current industry insights into governance and risk management best practices to support the Administration's effort to better manage cyber risks in the immediate future. The recommendations described within this letter and the attached document seek to align with this time constraint, focusing on immediately actionable ideas based on industry experience, sometimes at the exclusion of higher priority issues that will take longer to affect. The NSTAC will study and, as appropriate, make recommendations on longer-term, systemic challenges, such as budget, procurement, and workforce development, in Phase II of our tasking.

On behalf of the NSTAC, I thank you for the opportunity to provide our industry insights and recommendations on immediate steps that your Administration can take to improve NS/EP communications, including our Nation's cybersecurity and resiliency.

Sincerely,

Mark McLaughlin
NSTAC Chair

Attachment:
Attachment to the Letter to the President – Emerging Technologies Strategic Vision