NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

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

This document complements the National Security Telecommunications Advisory Committee's (NSTAC) March 10, 2016, letter to President Barack Obama. It provides additional context for and detail about industry's experience in managing cyber risk and the committee's shared insights and recommendations, which focus on governance and risk management best practices.

Governance

Industry's experience demonstrates that having a chief information security officer (CISO) role with clearly defined authorities and executive-level engagement and support is vital for effective governance and successful implementation of cybersecurity policies. Industry CISOs are often responsible for coordinating and collaborating with stakeholders across their organizations to develop and drive holistic, risk management-based cybersecurity strategies and policies. To do so, they assess risks, establish baseline security requirements designed to manage those risks, measure organizational compliance against those baselines, evaluate whether the baselines are effectively managing risk, and set goals for improvement.

Establishing a baseline and meaningful metrics against which progress can be measured enables CISOs to use a standardized approach and then evolve strategies and policies, adjust baselines, and mature processes for measuring internal compliance and advancing risk management. CISOs may also work with organizational stakeholders to develop incentives and establish penalties to foster implementation of policies and practices. Within industry, for instance, utilizing reputation-based incentives such as intra-organizational reporting on CISO metrics or incident remediation timelines has been effective.

As the CISO role matures, CISO baselines and compliance considerations should be integrated into the development of technologies and processes as well as into other business decisions, ensuring that security considerations are built in from the outset to reduce long-term costs. In industry's experience, CISOs must have the authority to approve or escalate inquiries about the development of appropriate technologies and processes being considered for deployment across numerous verticals.

Establishing a CISO role also provides an important opportunity to create a more robust, organization-wide governance model and structure to enable effective coordination and collaboration. Ideally, in recognition of the seriousness of cybersecurity threats, CISOs and their staff will be funded as a new security investment. Alternatively, a centralized, horizontal CISO function may draw capital or resources from existing verticals within organizations. Either way, risk managers within existing verticals must also continue to drive security policies and strategies for their organizations, operating within and building from the CISO's broader strategy. In industry's experience, effective governance models establish an operating model whereby CISOs in the horizontal function regularly interact, coordinate, and collaborate with their vertical counterparts. Many companies have created an action-oriented cybersecurity council or leadership team, a body within which the CISO convenes and collaborates with existing verticals and oversees a clear decision-making process and dispute resolution mechanism, including an escalation path when business/security disputes arise. Delineating the purpose and span of control of such a council, team, or other operating model is essential; in addition, encouraging a regular cadence of discussions and decision-making is helpful to raise visibility and collaboration.

Finally, while establishing a CISO role is a valuable step toward centralizing some security functions, doing so can also be disruptive, especially if the CISO's authority overlaps with or alters the role or function of preexisting authorities with related missions, such as the chief information officer (CIO) or chief risk officer. In such cases, executive support is necessary to clarify the CISO's role vis-à-vis partner officials and organizations. Moreover, in any case, clearly designating a CISO's responsibilities is key, and empowering a new CISO with top-down support and engagement is essential to minimize disruption. In industry's experience, a one-off announcement is not sufficient; companies that have successfully integrated CISOs as empowered enterprise risk managers have done so over a period of time, with CIOs and other executive-level officials regularly pointing to and highlighting the value of the CISO role.

Summary of governance recommendations:

- Empower the CISO with the authority to develop, make decisions about, and drive forward cross-organizational cybersecurity strategies and policies, including by establishing baselines and metrics, measuring internal compliance, advancing risk management maturity, and working with other organizational stakeholders to develop incentives and establish penalties for policy implementation;

- Create an operating model that empowers the CISO to regularly convene cross-organizational risk managers, enabling meaningful coordination and collaboration and instituting a decision-making and dispute resolution mechanism;

- Formalize executive-level support for the CISO, recognizing that the process of effectively integrating the CISO into department/agency activities may be disruptive; and

- Clearly define and enforce the roles and responsibilities of the CISO relative to other Federal officials, including the Federal CIO and department/agency CIOs and CISOs.

Risk management

Industry has learned that sharp, highly stringent risk management, prioritization of risks and risk mitigations, and rigor are essential for securing enterprises and technology systems. Large organizations in particular need to design processes to be scalable and implement risk management in a prioritized, thorough, and consistent way. More specifically, and consistent with the *Framework for Improving Critical Infrastructure Cybersecurity* (2014) that has been developed by the National Institute of Standards and Technology (NIST), much of industry approaches risk management by organizing around five functions: identify, protect, detect, respond, and recover. From industry's perspective, those functions are the building blocks of a holistic risk management program, and successful implementation of those functions amplifies the impact of each.

<u>Identify and Protect</u>

To protect what you have, you have to know what you have. Accordingly, a first step for industry is the identification of high value assets, a process that should first transpire within enterprise verticals; then, the highest value assets across those verticals should rise to the level of the CISO's horizontal visibility. For a large organization with many technology systems, establishing a highly discerning process for prioritization is critical, ensuring that, in a complex ecosystem, risks to the most important systems are given the most attention. At the same time, in industry's experience, a prioritized list of assets will never be perfectly comprehensive or current, and because this process cannot be allowed to take an inordinate amount of time, moving forward with clear and enumerated top-line priorities is sufficient.

Once an organization identifies its assets and prioritizes what is most critical, the next step is to use a mix of people, processes, and technology to protect those assets, focusing on the highest-value assets first. Within the immediate future, from industry's experience, protection should focus on three concurrent sub-

steps: ensuring rigorous attention to basic cybersecurity hygiene; using the latest versions of technology; and embracing new technology and associated processes (e.g., next-generation credentials and integrating preventive security technologies) to address persistent threats. The NSTAC's collective experience validates the importance of implementing and rigorously monitoring the implementation of basic cybersecurity hygiene best practices. Among those best practices, industry has most urgently implemented patch management, whitelisting, identity management (i.e., multi-factor authentication), access control (especially for system administrators), and isolation or segmentation of environments. Industry considers these steps foundational to all successful enterprise-protection and cybersecurity-risk management strategies. Additionally, protective technology and processes must be deployed and utilized strategically throughout the network to prevent and disrupt malicious activity at different phases of the attack lifecycle. Rather than relying upon an antiquated concept of protection at a single point of potential failure (i.e., exclusively at the endpoint or the network perimeter), using a defense-in-depth approach and automating an integrated system of preventive technologies increases an organization's ability both to protect against attacks and to prevent detected incidents from advancing through the attack lifestyle (i.e., to exfiltration). Moreover, in industry's experience, if a number of diverse verticals require these capabilities, then developing them as shared and/or managed services is more efficient, cost-effective, and scalable and creates more opportunity for cross-organizational maturity.

In collaboration with risk managers situated within verticals, industry CISOs typically also establish processes that measure the extent to which best practices to protect systems are being implemented. Within industry, auditing organizational compliance with best practices and other security measures is as important as defining those measures and mandating their implementation. While measuring and auditing compliance has been done for years, increasingly, industry is continuously monitoring systems and data for real-time status (e.g., patch compliance) and anomalies as well. These approaches are similar to some implemented in the last few years in some areas of the Government. By continuously monitoring systems, industry firms seek to capture not only whether internal policies are being followed but also the efficacy and value of their security policies in managing and reducing risk. Recognizing that continuous monitoring is only meaningful if it is used to improve risk management, industry is still learning how best to manage and act on the large volumes of data that we are accumulating from continuous monitoring and diagnostics.

Detect

Identifying and protecting assets are essential functions, enabling industry to take important steps toward preventing breaches and other incidents. In industry's experience, given today's cybersecurity threat environment, while organizations' primary focus should be on preventing breaches, they should also assume that they have already been breached and prepare and act accordingly. Such an assumption elevates the importance of effectively preventing when detecting, responding to, and recovering from incidents. In addition, it has altered how industry tests its own environments, shifting attention toward more proactive efforts to contain and hunt for adversaries.

Just as industry has moved towards continuous monitoring for protection, we have also adopted the approach of continuous monitoring to detect breaches, attempted breaches, and incidents. To ensure that critical vulnerabilities and incidents are quickly detected and contained, industry filters through security information and event management (SIEM) inputs, using security orchestration and threat intelligence to prioritize response. In developing cross-organizational detection processes and implementing large-scale security systems, industry has also discerned the value of using an integrated, device-agnostic platform, accessible to both horizontal and vertical stakeholders, to enable immediate visibility across the enterprise environment. Using multiple SIEMs that cannot communicate with one another is no longer sufficient; instead, using interoperable technologies, a standardized data format, and an integrated platform is essential to providing comprehensive and complete visibility into incidents, abnormalities, and patterns across an organization's environment. Industry is implementing integrated platforms with considerable urgency as we recognize the near-term operational value as well as the importance of using real events to

inform longer-term strategies, including around the adoption of emerging technologies such as software-defined networking. In addition, by utilizing highly integrated, automated capabilities throughout a segmented, "zero-trust" network, industry is increasingly using detection capabilities to help prevent malicious actors from accomplishing their end goals.

Industry also does extensive internal testing, using results and learnings to measure the impact of and to mature the policies and controls being implemented to secure data and systems and, increasingly, detecting adversary activities. Recently, industry has begun to significantly evolve its approaches to such testing, aiming to ascertain a comprehensive view of not only security but also resilience. In particular, some organizations have begun to measure and use penetration testing in a different way. Since a zero-trust model would assume that systems have been compromised, industry is increasingly measuring not only the time required for penetration testers to access systems but also the time required for them to reach a desired target—as well as the time required for defenders and mitigations to detect, contain, and remediate issues. Looking across this data has driven industry to prioritize certain defense-in-depth strategies, including thorough segmentation of environments and robust access controls. In addition, industry has moved toward the use of "hunt" teams to detect adversaries that have already established a foothold in their organizations' systems. The use of such teams is consistent with the assume-breach mentality and takes important steps toward learning more about adversaries, reducing the immediate and future impacts of an incident, and preventing incidents.

Respond and Recover

In responding to and recovering from incidents, industry has benefitted from developing operational response frameworks that clarify prioritization of and related processes for responses across the full spectrum of potential events with cyber implications; the NSTAC studied this in depth and advised the President on it within the *NSTAC Report to the President on Information and Communications Technology Mobilization* (2014). While less sophisticated incidents may be remediated through automated responses (e.g., by removing common malware from infected systems), more sophisticated incidents may require the involvement of incident response teams associated with the affected organizational verticals. However, successful remediation of particularly sophisticated incidents will also require coordination with experts. Industry's experience demonstrates the importance of treating and containing more critical incidents with greater urgency and resources.

Considering the importance of treating particularly sophisticated incidents with greater urgency and resources, industry finds value in developing an incident response group with significant expertise and the capability to respond to the most severe incidents. This horizontal, cross-organizational group complements other organizational capacities as they are overwhelmed by an incident or an incident passes a pre-determined threshold of severity. To function seamlessly together, a centralized, horizontal group and other organizational incident response entities must have a common understanding of incident response processes, including a standardized methodology for prioritizing among incidents and a mutually-understood threshold that triggers escalation to a more rigorous and broadly-inclusive response framework. Additional context and information regarding how industry has benefitted from developing operational frameworks that allow for agile, effective, and distributed implementation across numerous stakeholders is included within the *NSTAC Report to the President on Information and Communications Technology Mobilization*.

Summary of risk management recommendations:

- Mandate the identification of key cross-organizational assets and personnel and rigorously prioritize what is most important;

- Protect assets by implementing basic cyber hygiene measures (viz. patching, whitelisting, identity management, access control, and zero-trust network segmentation); using the latest versions of

hardware and software; and embracing new technology and processes to address persistent threats, including next-generation credentials and security as a service;

- Regularly review and compare the metrics of departments/agencies demonstrating compliance with basic cyber hygiene, identifying departments/agencies that are performing poorly;

- Mandate the use of an integrated, intelligent platform to prevent incidents effectively through automation and zero-trust network segmentation and to detect incidents, abnormalities, and patterns across an organization's entire environment, limiting greatly any exceptions or compliance extensions;

- Advance internal testing capacities to better understand how to achieve resilience, including by giving importance to time to detect, contain, and remediate issues, and to reduce the immediate and future impact of compromises, including through the use of hunt teams;

- Capitalize on security, cost, and personnel talent efficiencies by incentivizing and, where appropriate, mandating use of Government's common platforms and shared security services and by encouraging use of commercial managed security services to reduce the necessity for departments/agencies to construct their own capabilities;

- Direct the use of a framework to prioritize among incidents and ensure seamless coordination among incident response teams, enabling effective response to and recovery from incidents that reflect varying levels of sophistication; and

- Regularly review and compare the metrics of departments/agencies utilizing the incident response framework, identifying departments/agencies that are lagging in response and recovery.