Commission on Enhancing National Cyber Security
c/o National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

September 9, 2016

Dear Commissioners:

Re: Input to the Commission on Enhancing National Cybersecurity

The Cyber Secure America Coalition, an organization bringing together leading cyber experts, appreciates the opportunity to provide comments in response to the Commission on Enhancing National Cybersecurity's request for information entitled, "Information on Current and Future States of Cybersecurity in the Digital Economy." As cyber threats become more sophisticated and malicious network attacks grow exponentially, the public and private sectors must work together to share cyber threat information, coordinate cyber incident response, and increase public awareness about the importance of cybersecurity to our national and economic security. We welcome the leadership of the Obama Administration and the Commission in soliciting public comments and recommendations on how to better secure our cyber networks to bolster ongoing public-private partnerships to effectively combat evolving cyber threats.

Critical Infrastructure Cybersecurity

Promoting the acquisition of actionable threat intelligence and the sharing of cyber threat information remain essential to protecting critical infrastructure. Full implementation of the Cyber Security Act of 2015 must continue to improve bidirectional sharing of cyber threat information between the government and the private sector, while also protecting privacy. We believe government plays an important role in sharing information to assist private sector entities in combatting cyber threats, particularly as it relates to the critical infrastructure. Further, we believe that encouraging information sharing through tools that reduce market risk and provide actionable return for companies is vital to creating vibrant exchanges. Vetting, verified anonymity, and tools that redact personal and proprietary information will encourage more threat-sharing. In particular, the Commission should evaluate ways to encourage cyber incident reporting, and explore recommendations that such reporting (subject to appropriate privacy and security protections) be mandatory for critical infrastructure companies.

One of the primary challenges with respect to critical infrastructure cybersecurity is the increasing connectedness of industrial control systems (ICS) without appropriate security

controls. In the FY2015 Industrial Control Systems Assessment Summary Report, the National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) cited 638 weaknesses in the 112 cybersecurity assessments performed that fiscal year.[1] Fostering a robust security culture that leverages risk and vulnerability assessments to protect the automation and processes that underlie critical infrastructure architectures is imperative. ICS owners and operators must recognize that the significant differences between traditional corporate IT security and industrial control systems demand a multi-layered approach that evaluates physical device protection, operations controls, supervisory control and data acquisition (SCADA) controls, manufacturing operations, and corporate IT networks. Such a risk-based management approach to ICS security needs to properly assess assets, evaluate legacy systems, manage rights access, engage in vendor oversight, prioritize security patches, monitor traffic at application and protocol levels, and tailor cybersecurity training to each role in the organization instead of general awareness training.

Another area worthy of the Commission's consideration is to study, in conjunction with federal agencies, ways to promote the acquisition of threat data and intelligence from global cyber hot spots like China, the Middle East, Russia, and Eastern Europe, where a significant number of cyber threats targeting critical infrastructure seem to originate.

Cybersecurity Insurance

Cybersecurity insurance can serve as a vehicle to transfer and mitigate financial risks, as well as promote better cybersecurity practices. Developing consistent and uniform metrics by which insurance companies could potentially benchmark the cyber posture of companies and appropriately price coverage remains important. We recommend that the Commission evaluate how consensus-based approaches to enterprise cybersecurity like the NIST Cybersecurity Framework (CSF) and the SANS Institute 20 Critical Security Controls for Effective Cyber Defense can generate sufficient, quantifiable, and measurable data about an organization's cybersecurity practices and how that organization is achieving best practice outcomes on a continuous basis. In addition, the Commission should review emerging technologies that automate this process in order to make informed recommendations on how the federal government itself can more effectively utilize the NIST CSF and/or SANS 20 controls and lead the market toward the kinds of operational data necessary to the maturing cyber insurance industry. Further, the United States government should encourage the participation of the insurance industry in the sharing of threat data to better inform risk assessments and pricing.

Among the basic requirements the federal government – and ultimately the private sector – should measure for the purposes of better cyber insurance are:

- An ability to demonstrate preferably via a comprehensive, real-time, continuous cybersecurity posture metric and dashboard, the ongoing achievement of cybersecurity best practice outcomes appropriate for the value of their critical assets (i.e., the value bad actors place on them) and its threat environment.

---

[1] NCCIC/ICS-CERT assessment report

- Designating an officer of the company with responsibility and procurement authority for information security;
- Demonstrating active membership in an information sharing program designed to allow members to share impact and attack-related information in an anonymized fashion;

- Development of a cyber incident response plan; and

- Demonstrated compliance with all relevant federal and state information security laws such as data breach notification, the Gramm-Leach-Bliley Act (GLBA), and the Health Information Portability and Accountability Act (HIPAA).

Finally, companies face cyber threats on a global scale, and therefore, it is important for the public and private sectors to cooperate and coordinate internationally.

Cyber Workforce

Government and private sector reports indicate that there could be one million unfilled, high-wage cyber security jobs in 2016. Failure to address this skills gap can exacerbate the cyber risks posed to the networks that govern our daily lives and the data they generate. Given the current acute shortage, the Commission should look at public sector support for worker retraining programs in the field of cybersecurity, further encourage cybersecurity education at our colleges and universities, and better promote vocational and technical training in this area.

The government is taking positive steps with programs like the National Initiative for Cybersecurity Education (NICE) through NIST and the National Security Agency's Day of Cyber. We need to start early in the education process across the US to promote cyber education and mentorship programs so that students and their parents learn about the many opportunities in the field of cybersecurity. We believe that the Commission should examine the idea of a scalable national mentorship initiative so that leaders in the field can share their wisdom and experience and encourage both young people and those interested in changing careers to better understand cyber jobs.

Looking at the mid-to-long term, the Commission should explore whether there is any federal policy that could further support scholarship programs from both the public and private sectors to encourage students to pursue education and training programs in cybersecurity. This is a sensible complement to the President's Computer Science for All initiative. We must continue and sharpen the national focus on capacity building in our universities so that we can turn out enough skilled graduates to meet the workforce needs of both the private and public sectors in the field of cybersecurity. Further, universities need to work with the private sector to ensure that curricula that is developed matches the cybersecurity skills needed by employers.

In addition to mentorship programs and public/private sector collaboration to develop cybersecurity curricula, we should promote practical development of skills through private sector training and certification programs to best prepare our workforce to handle the threats they will face. Government-operated certifications should be avoided.

Identity and Access Management

The Administration deserves commendation for the priority it has placed upon expanding the use of multifactor authentication. The private sector, through entities like the Fast Identity Online (FIDO) Alliance, has moved rapidly toward interoperable and passswordless authentication using biometrics. This more secure, machine-to-machine authentication deserves deeper examination by the Commission with an eye towards recommendations for adoption by the federal enterprise.

International Markets

Today's cyber-attacks often target confidential information, whether it is customer data, intellectual property/trade secrets, employee information, or corporate strategy documents. Therefore, protecting that information is critical to our economic security. And, in the case of the government or critical infrastructure, protecting that information is crucial to national security. The use of encryption as a tool to protect important or sensitive information is essential to a good cyber security regime.

Recent events have drawn the use of encryption into the media spotlight. The desire of some policymakers to force the decryption of information is a dangerous approach and threatens one of the foundations of security. The benefits of encryption are well known. If we as a country choose to weaken our security practices by making encryption less secure, we risk both our economic and national security. In international markets, we would put US companies at a disadvantage in the marketplace. The companies in our Coalition believe, based on market inputs, that customers will choose alternative products and solutions if they believe their data is not safe, secure or is subject to government surveillance. We understand, and strongly support, the importance of balancing between the needs of law enforcement and the imperative to protect data. Government mandating a solution is not the answer; industry and government must collaborate to find a reasonable solution to this policy challenge. Therefore, we encourage the Commission to make a clear recommendation that use of encryption not be undermined by requirements to make software "decryptable" and to also examine the bipartisan *Digital Security Commission Act* for possible endorsement.

Internet of Things

The explosion of the Internet has spawned the growth of new products and enhancements to many existing ones. More and more products are now connected to the Internet: smart meters, smart cars, smart refrigerators and even the emergence of smart cities. With this connectivity comes both efficiency and increased risk since there are more potential attack vectors. Connected devices also raise questions about privacy and what constitutes personally identifiable information; the complexity of supply chains and who is responsible for security; the need to take a system-of-systems approach as opposed to focusing exclusively on individual devices; and how performance-based rules that define outcomes can be developed. While we would not recommend regulation, we ask the Commission to consider a federal role in promoting the security of the Internet of Things (IoT) and should examine opportunities to

incentivize companies to design security into the products and be more transparent about their privacy policies and security practices. Further, we would recommend consideration of a public awareness campaign to inform consumers about privacy and security matters related to having connected devices embedded in their homes and daily lives. Certainly an educated public is more likely to make better and more responsible decisions in this regard. The government can further increase public awareness about IoT through its own procurement and deployment of connected devices and services.

Cybersecurity Research and Development

We believe in identifying and addressing the root causes of our challenges and not just in treating their symptoms. We submit the following Cyber R&D priorities:

1. Computing and networking technologies were not originally designed to be secure and private by default in a highly connected world. The technology we use was generally sufficient when our computing environments were operating in isolated and protected facilities. The entire approach to cybersecurity -- and the industry itself -- could be considered a "band aid" trying to protect systems that are operating far beyond the design constraints of the fundamental technology, or that which they were designed to perform. Thus, we recommend that resources be focused on the creation and broad deployment of new computing technologies that are inherently more secure by default.

2. While we may never be able to produce defect-free software, there are only 25 programming errors which are the root cause of vulnerabilities exploited in 90% of successful cyber-attacks (this includes zero day vulnerabilities).[2] Most commercial software today includes vulnerabilities caused by these software programming errors, making it exceedingly difficult for any organization to effectively manage their software vulnerability risk. Therefore we recommend a focused R&D priority be placed on innovations to dramatically reduce the rate of occurrence of the most common and most exploited errors in software.

3. You cannot effectively manage, nor improve, that which is not measured. We believe a critical National Cybersecurity Priority should be the acceptance of a widely used comprehensive metric to determine if what is being done by an entity (or is not being done) is working or improving actual cybersecurity risk and cybersecurity outcomes. This is especially relevant with respect to the recent news reports about the Bangladesh Bank Heist[3] and cybersecurity deficiencies at NASA[4]. Cyber security improvements will be more successful if we can measure the various cyber tools to determine what is most effective.

---

[2] CWE/SANS Top 25 Most Dangerous Software Errors, http://www.sans.org/top25-software-errors/

[3] http://www.wsj.com/articles/in-bangladesh-cyberheist-strange-requests-odd-misspellings-and-a-lack-of-scrutiny-by-fed-1471192772. Video summary, Reuters,

[4] http://federalnewsradio.com/reporters-notebook-jason-miller/2016/08/nasas-act-desperation-demonstrates-continued-cyber-deficiencies/

Public Awareness and Education

Just as we need to strengthen cyber practices and raise the overall level of cyber protection for government and the national critical infrastructure, so too must we inform the general public and small- and medium-sized businesses about the dangers of cyber threats and the risks to their data. Threats to consumers and small businesses continue to evolve as well. The current epidemic is ransomware, but tomorrow the bad actors will find new ways to extract data for monetary gain. The government and the private sector are making progress in this area through efforts like National Cyber Security Awareness Month in October, but we believe more federal resources should be applied towards this effort if we are to succeed and reach a larger set of the US online population.

If cyber threats are undermining our national security, then we should marshal our government resources and our best marketing and training talent to mobilize the American people to confront this threat. This effort should continue to be coordinated out of DHS with assistance and support from all other agencies and the private sector.

Summary

Ultimately, we have made progress over the last several years through the Administration's cyber efforts and those of the private sector. More needs to be done if we are to succeed in getting one step ahead of the bad actors, whether they be cybercriminals or nation-state actors. This coalition of cyber companies is on the front lines every day combatting the cyber threat. We look forward to the Commission's recommendations. We will continue to work with our public and private sector partners to make America cyber secure.

Sincerely,

Hon. Phillip J. Bond
Executive Director