Input to the Commission on Enhancing National Cybersecurity
Submitted by The Center for Internet Security

www.cisecurity.org
Contact name: Kathryn Burns

Introduction

The Center for Internet Security (CIS) is a 501(c)(3) organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. The mission of CIS is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace. Utilizing its strong industry and government partnerships, CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls.

CIS serves a broad-based national and international constituency across the public and private sectors. The MS-ISAC comprises representatives from all 50 states, the District of Columbia, as well as over 1,000 U.S. territories, tribal governments, and local governments. Through the Nationwide Cyber Security Review (NCSR), the MS-ISAC charts nationwide progress in cybersecurity and identifies emerging areas of concern across hundreds of State, Local, Territory and Tribal (SLTT) governments. The National Campaign for Cyber Hygiene is a collaborative effort by CIS and the National Governor's Association, which offers a foundational cybersecurity program for hundreds of SLTT organizations.

CIS is a leader in the development of security best practices. The CIS Security Benchmarks organizes communities of technical expert volunteers to develop secure configurations serving over thousands of public sector organizations across the globe, and supported by essentially the entire security industry. The CIS Critical Security Controls Version 6.0 draws upon the expertise of hundreds of cybersecurity practitioners and subject matter experts. The current version of the CIS Controls, which are aligned to the NIST Cybersecurity Framework, ISO, PCI and other prominent cybersecurity frameworks, have been downloaded over 45,000 times since October 2015 and are used by thousands of organizations around the world as a means to protect their networks.

CIS provides the public with free, high quality cybersecurity guidance but believes much more can be done to promulgate and communicate proven approaches to cybersecurity. The following is a response to:

Question 4 - What can or should be done now or within the next 1-2 years to better address the challenges?

CIS recommends **a National Campaign to Improve Cybersecurity Best Practice** that would address cybersecurity for every audience, from the individual citizen to the large corporate enterprise. The Campaign would require a coordinated approach to promote a set of cybersecurity solutions and then broadly communicate it to all audiences as the nationally accepted and authoritative solution.

Step One: Adopt an Authoritative Best Practice Solution Set

Eliminate the Cybersecurity Fog - The vast majority of cybersecurity problems that plague us today could be prevented by action, technology, and policies that are already known or exist in the marketplace. In the majority of cases, we're not being attacked by wizards wielding unstoppable magic; we're being overwhelmed by massive numbers of relatively mundane actions. Unfortunately, both professional cyber defenders and private citizens are overwhelmed and confused by what we call the cybersecurity "Fog of More" – conflicting opinions, a flooded cybersecurity solutions marketplace, and daunting recommendations too complex to implement. Even for the rare enterprise that has the information, expertise, resources, and time to figure this out, it's almost certainly not true for all of their key business partners, suppliers, and clients. What's needed is a set of simple, straightforward best practices that anyone can understand and implement as a national approach to cybersecurity.

Promote a Single Standard - There is currently no officially endorsed cybersecurity approach. As a result, individuals and organizations must choose among a very wide array of tools and practices. To address this gap, California Attorney General Kamala Harris issued a report in February 2016 to California businesses, which included a recommendation to use the CIS Controls as a standard for protecting consumer information. The Attorney General endorsed the CIS Controls because they are a concise, prioritized set of universally applicable practices created to stop today's most pervasive and dangerous cyber attacks. So while implementing all the Controls may not be practical for every organization, applying just the first five CIS Controls can reduce their risk of cyber attack by around 85 percent. Attorney General Harris proclaimed that, "failure by an organization to implement the relevant Controls "constitutes a lack of reasonable security." This action by the Attorney General provided a state-wide approach to cybersecurity upon which other states could follow.

Use a Health Campaign Approach- In 2014, CIS and the National Governors Association launched the National Campaign for Cyber Hygiene as a way to promote cybersecurity as a public "health" issue. The "hygiene" term posits cyber health as a preventive strategy having the same level of importance to societal well-being as hand washing has to preventing the spread of communicable diseases. The National Campaign for Cyber Hygiene offered a plain-language, accessible, and low-cost starting point for implementation of the CIS Controls (CSCs), a set of 20 best practices created by security experts. Although the CIS Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many organizations and individuals are starting from a very basic level of security and need more specific and direct guidance to get started. The Cyber Hygiene Campaign is a one example of this idea.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer.

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using “known good” configurations? (CSC 3)
- Are we continuously looking for and managing “known bad” software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

Offer a Plain Language Approach - These questions, and the actions required to answer them, are represented in “plain language” by the Top 5 Priorities of the Campaign: **“Count, Configure, Control, Patch, Repeat”**. Like any awareness campaign, the language was meant to be simple and catchy but behind each of these questions is a primary Control that provides an action plan. The Campaign is also designed to be in alignment with the first 5 of the CIS Critical Security Controls, the Australian Signals Directorate’s (ASD) “Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation (CDM) Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

Step Two: Raise Awareness and Compel Action

Communicate at Every Level - Like the U.S. Stay Safe Online and the UK Get Safe Online cyber initiatives, a nationally led, empowering and coordinated program would articulate how to defend against the cybersecurity challenges by leveraging existing outreach and communication channels and mechanisms. The program would promote easy-to-understand best practices like the CIS Controls and product-neutral implementation guidance for using the CIS Controls. Further, government and private groups who already engage with their customers and constituents would promulgate these solutions to individuals, groups, businesses—especially small- and medium-size—and non-profits alike.

Issue a National Call to Action–Given the currently unacceptable level of data breaches and cyber crime, a larger call to action is necessary beyond awareness-building. A call to action for cybersecurity should not only provide education for cybersecurity best practice, but it should encourage cybersecurity as a profession and offer guidance for how individuals and companies can drive the marketplace to improve cybersecurity through purchasing. Stepping up to a national call to action is part and parcel to the American esprit de corps and everyone should feel empowered to change the current status quo. A scoring mechanism would accompany the specific recommended practices, so that everyone could respond to a "What's your cyberscore?" promotion as the centerpiece of this call to action.

Make Guidance Accessible to All - A key element of this effort is the establishment of a place where collective knowledge can be shared and citizens, businesses, and services can convene. This national cybersecurity website would be a singular unique resource that features practical advice about how to protect individuals, computers, and mobile devices. It would include information for businesses about how to battle fraud, identify identity theft, stem the effects of viruses, and combat online threats.

Attract Interest in Cybersecurity Professions. As part of a call to action, cybersecurity professions must be marketed and made more attractive to the public. With the immense shortage in qualified cybersecurity defenders, a national campaign should encourage cybersecurity education and training and make cyber defense a compelling career choice.

Drive the Marketplace – One of the biggest cyber attack vectors remains to be lack of vulnerability patching and poor configuration. But why should so much patching be needed at all? Many consumers today tend to accept the fact that new versions of products will have pervasive deficiencies as "the way it is," without any expectation that the product is stable and reliable. Instead the national Campaign should encourage individual and corporate consumers to demand more secure products from manufacturers and write requirements into contracting language.

Engage and Incent Expert Communities – The technical experts who develop cybersecurity best practice are essential to the Campaign. CIS has many years of experience building communities of experts who develop best practices based on their real world knowledge of the threat environment. As part of the Campaign, it will be critical to continue engaging the development community to build better products, publish open source solutions, and offer guidance for keeping safe online.

Integrate with Education - Fully integrating K–12 and higher education into this program would include teaching cyber ethics, which would add a valuable dimension to this national effort. This one-stop-shop would feature cyber news as well as tips and stories from around the world related to the topic to instruct the students how to protect themselves while online. The website would provide tip sheets, studies, info graphics, quizzes and other resources for audiences. This variety of vehicles would help users digest information in different ways.