Testimony of John M. Gilligan
President and Chief Executive Officer
Center for Internet Security
At the hearing entitled
Exploring Recent Data Breaches: What State, Local, and Private Institutions Can Do to Protect Themselves and the Public
The Select Committee on Cybersecurity and Identity Theft Protection
California State Senate
Monday, November 8, 2021
1:30 p.m. (Pacific Time)

Chair Min, members of the Select Committee, thank you for inviting me today to this hearing. My name is John Gilligan, and I serve as the President and Chief Executive Officer of the nonprofit Center for Internet Security, Inc. (or CIS), an organization that has as one if its focuses improving the cybersecurity of state, local, tribal, and territorial organizations. I have spent most of my career in service to the Federal government, including serving as the Chief Information Officer of both the U.S. Department of Energy, and the U.S. Air Force.

I appreciate the opportunity today to share our thoughts on the current state of cybersecurity within state, local, and private organizations. I commend the California Senate on the creation of this Select Committee, and I look forward to offering some specific recommendations on how we can collectively build on the progress being made in this critical area of national security. As I will discuss in a few minutes, it is essential that state legislatures take a proactive role in establishing the governance structures and the expectations, or metrics, necessary to improve cybersecurity across their states.

Protecting the infrastructure of California's cyber networks and systems as well as the personally-identifiable information that resides on those networks and systems is of the upmost importance. The current global pandemic has reinforced how much we as a nation, as states and local governments, and as private organizations are dependent on the Internet and the multitude of interconnected systems for essential communications, commerce, health, education, entertainment, and so much more.

Today, I would like to: (1) provide you a short background about CIS; (2) briefly describe the set of proven best practices – called Essential Cyber Hygiene – that CIS recommends for all government and private sector organizations; and (3) summarize the recommendations in a recent report developed for governors and state legislators regarding establishing governance as a necessary foundation and an accelerator in improving state-wide cybersecurity.

First, let me provide some background about the Center for Internet Security

Established in 2000 as a nonprofit organization, the primary mission of CIS is to advance cybersecurity readiness and response. CIS works with the global security community using collaborative deliberation processes to define security best practices for use by government and private-sector entities. The resulting best practice guidance is provided for free on our website with

over a million downloads per year. In addition, as I noted earlier, CIS executes with federal funding two organizations focused on improving cybersecurity of state, local, tribal, and territorial organizations: the Multi-State Information Sharing and Analysis Center, or MS-ISAC and, the Election Infrastructure Information Sharing and Analysis Center, or EI-ISAC. We have over 12,000 state, local, tribal and territorial government organizations participating in the MS-ISAC and EI-ISAC (including almost 1,000 in the state of California), who are taking advantage of cyber best practice educational and training opportunities, cyber threat indicator sharing and threat alerts, network and end point monitoring, as well as incident response and recovery.

Second, I would like to highlight one of our recommended cybersecurity best practices.

Let me first start with some context for the best practice recommendation. One of the challenges that organizations have with regard to cybersecurity is what we like to call "the fog of more". That is, there are a plethora of security frameworks and guidelines from the U.S. government, private companies as well as international organizations such as the International Standards Organization (ISO), the Payment Card Industry (PCI), and the Institute for Electrical and Electronics Engineers (IEEE). In addition, there are uncountable security vendors who promise absolute or at a minimum improved security – if you only use my company's tool. Having been a CIO at several large organizations, I have seen the result the fog of more firsthand – many well-intended, but costly, cybersecurity efforts that are mis-focused and fragmented, resulting in little actual improvement in the security resilience of the organization leading to repeated embarrassments as the organization falls victim to ransomware or confidential data breach or some other cyber-attack.

As a personal example, I can share that as CIO of the U.S. Air Force I found that despite spending almost $2B annually for cybersecurity, the National Security Agency, or NSA, was able to easily penetrate our cyber defenses in their annual penetration testing. I knew that the Air Force had lots of bright cybersecurity experts and almost every security tool in existence, yet our overall security posture was embarrassingly weak. I asked NSA, "where should I start?" The advice they provided was to "start with strengthening defenses against the most common attack patterns", and based on their analysis, 'where to start' turned out to be identifying and fixing software that did not have up-to-date security updates and patches. We did this over the next 18 months. The result was improved security, better operational availability, and, surprisingly, lower operating costs. This same philosophy of focusing on defeating the most common attack patterns has continued to underpin the Center for Internet Security's best practice efforts.

CIS has developed a best practice that we strongly believe is the way to avoid costly, disjointed, and ineffective cybersecurity efforts. In essence, this best practice is "where to start". Working with a set of global collaborators leveraging threat data from the U.S. intelligence community, the Department of Homeland Security, and many private sector organizations, CIS has developed what we call "Essential Cyber Hygiene" – a relatively small set of security best practices, or safeguards, that we recommend every organization implement to protect them from the most common attack patterns. For context, the Essential Cyber Hygiene safeguards comprise the first of three "implementation groups" of a carefully curated set of security safeguards to be incrementally implemented. We call the full set of safeguards the CIS Critical Security Controls. The set of 56 safeguards that comprise the first implementation group, called Essential Cyber

Hygiene, are concrete actions with measurable completion criteria that address the root issues that account for the overwhelming majority of successful cyber-attacks. Examples of these safeguards are:

1. Establish and maintain a secure configuration process (where I "started" in my AF journey)
2. Establish an access granting process
3. Establish an access revoking process
4. Manage default accounts on Enterprise assets and software
5. Restrict Administrator privileges to dedicated administrator accounts
6. Disable dormant accounts
7. Configure data access control lists

There are 49 more. You may have noticed that the examples that I listed all reflect good systems and network management processes – there truly is no magic here. Essential Cyber Hygiene that can prevent most cyber-attacks consists mostly of good systems and network management practices! That is an important revelation.

As a companion to the Critical Security Controls, CIS recently developed and published the results of a rigorous analytical effort, called the Community Defense Model, to document the formal analysis of the effectiveness of the Essential Cyber Hygiene safeguards and the subsequent increments of safeguards. This analysis showed that the Essential Cyber Hygiene safeguards were effective in defending against 77% of the top cyber-attack types including Ransomware, Malware, and Insider Privilege Misuse. Implementing Essential Cyber Hygiene for all organizations makes good sense, and we recommend that you consider mandating it across California.

Third, I want to briefly describe the recommendations from the recent study on the necessity of governance to implement and accelerate the expansion of effective cybersecurity.

A year ago, the Center for Internet Security working with the University of Albany Center for Technology in Government (CTG), the National Governors Association (NGA) and the National Conference of State Legislators (NCSL) published the results of a study examining how effective cybersecurity governance within states correlated to improved cybersecurity resilience. The title of the study report is: *Managing Cyber Threats through Effective Governance, A Call to Action for Governors and State Legislatures*. A copy of the report has been provided as part of the hearing preparation materials.

The study conducted interviewed dozens of state officials – CIOs, CISOs, as well as executive and legislative branch leaders. The study found that effective cyber governance was a prerequisite for an effective cybersecurity program within a state. Among the key finds of the study were the following:

1. Few states have cybersecurity governance that effectively ensures that their risk is managed to a level and in ways that have been determined through governance processes acceptable to the governor and the state legislature.

2. Few commonly-agreed upon indicators or metrics exist to assess cybersecurity operations. Those that do exist, are used intermittently, and few, if any, indicators exist or are used to assess effectiveness of cyber governance activities.
3. Finally, there was clear recognition of the need to expand governance beyond state executive level agency assets, to a "whole of state" perspective that engages stakeholders across multiple sectors and levels of government in a coordinated and collaborative process of cyber risk management.

The study identified four recommendations for governors and state legislatures:

1. Establish Authorities through both Executive Order and Legislation (we found that a strong governor or executive leader is very valuable – perhaps essential – but that improving cybersecurity across a state is not a one or two term effort. Legislation is needed to codify and formalize the necessary governance processes.
2. Formalize Key Processes – (I will provide some examples shortly)
3. Clearly Assign Roles and Responsibilities
4. Monitor Indicators for Decision-Making and Adaptation (again, I will provide a few examples)

During the study, we found that states that had implemented the four recommended actions had made significant progress in improving state-wide cybersecurity.

Key processes for improving effective governance (the second recommendation) include the following:

- Defining and enforcing a Enterprise Cybersecurity Architecture
- Establishing a standard for conducting Cyber Risk Assessments
- Establishing and leveraging Control over IT Procurement and Acquisition
- Control over Network Connectivity – mandating that state organizations leverage common networks and enforcing security compliance before systems can be connected to the networks

The report also defined sixteen indicators or metrics across three categories. These are intended to help governors and state legislators set expectations regarding assessing the state of cybersecurity across the state. Examples of the metrics are as follows:

- Do we know what the three biggest cyber risks are to our state? What are we doing about them?
- Have we been told how we are protecting our state's most important assets from the cyber threats they face?
- Are the state's Chief Risk Officer, the governor's Homeland Security Advisor, the governor's Emergency Management Director, and the Chief Information Officer synchronized? Do they all give the same answers to the above questions?

Closing

Having reviewed your biographies, I realize that none of you are cybersecurity experts and that this is a very complex arena. I encourage you to cut through the "fog of more" and keep your actions simple and focused. To summarize, our first recommendation would be to establish a requirement for Essential Cyber Hygiene for all systems and networks statewide. This is not the final step, but it is achievable by almost any organization and is effective in preventing about 80% of the most common cyber-attacks. The California legislature may want to consider an approach similar to legislation in Ohio, Utah, and Connecticut which provides safe harbor for organizations who implement appropriate cybersecurity safeguards like Essential Cyber Hygiene. Second, we would recommend a collaborative effort between the governor's office and the California legislature to establish state-wide cyber governance. Our study provides a solid outline for how to get started.

I appreciate your time and attention and look forward to your questions.