Testimony of Curtis W. Dukes
Executive Vice President & General Manager, Security Best Practices
Center for Internet Security
Public Hearing on H.B. No. 6607
An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses
Commerce Committee
General Assembly
State of Connecticut
Via Zoom and YouTube Live
Thursday, March 18, 2021
12:00 p.m. ET

Co-Chairs Hartley and Simmons, Vice-Chairs Cohen and Rochelle, Ranking Members Martin and Buckbee, and members of the Committee, thank you for inviting me today to this hearing. My name is Curtis W. Dukes, and I serve as Executive Vice President & General Manager, Security Best Practices of the nonprofit Center for Internet Security, Inc. (CIS).[1] I have spent most of my career in service to the Federal government, including serving in various senior positions at the National Security Agency. I appreciate the opportunity today to share our thoughts on how we as a country can improve our cyber defense. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical national security.

In short, I will: (1) introduce you to CIS and the CIS Critical Security Controls ("CIS Controls"); (2) discuss the scope of the cybersecurity problem facing this country; and (3) explain why the approach taken by H.B. No. 6607 serves as an excellent step to improve our cybersecurity.

(1) About CIS and the CIS Critical Security Controls

Established in 2000 as an independent nonprofit organization, the Center for Internet Security's primary mission is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for security hardening of commercial IT systems at a time when there was little online security leadership. Today, 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 approximately 300 professionals at CIS provide cyber expertise in three main program areas: (1) the Multi-State and more recently the Elections Infrastructure Information Sharing and Analysis Center, the MS-ISAC and EI-ISAC respectively; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

MS-ISAC.[2] In late 2002, the Multi-State Information Sharing and Analysis Center (MS-ISAC) was created by the State of New York with the recognition that the state government community needed an information-sharing mechanism (i.e., an information sharing and analysis center or 'ISAC') to coordinate cybersecurity efforts and promote best prac-

[1] Find out more information about the Center for Internet Security here: https://www.cisecurity.org/

[2] Find out more information about the MS-ISAC here: https://www.cisecurity.org/ms-isac/

tices. In January 2003, the MS-ISAC had its first meeting, formally launching an ISAC for state governments. DHS first reached out to the MS-ISAC in September of 2004 and began providing some funding. In 2010, DHS officially designated the MS-ISAC as the key resource for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments and issued the first Cooperative Agreement. Also, in 2010, the MS-ISAC moved to its current organizational home within CIS, where it has since resided.

The members of the MS-ISAC, the largest ISAC in the world, include all 56 states and territories, and more than 10,000 other SLTT government entities including local governments, schools, hospitals, and publicly owned water, electricity, and transportation elements of the U.S. critical infrastructure. MS-ISAC's 24x7 cybersecurity operations center provides: (1) cyber threat intelligence that enables MS-ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) incident response support; and (4) various educational programs and other services. Furthermore, MS-ISAC provides around-the-clock network monitoring services with our Albert network monitoring devices for many SLTT networks, analyzing over one (1) trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2019, MS-ISAC analyzed, assessed, and reported on more than 72,000 instances of malicious activity for more than 8,500 MS-ISAC members. The Albert IDS capabilities are being complemented with end point protection capabilities, as well as automated blocking of known malicious internet sites.

EI-ISAC.[3] After the interference in the 2016 election, DHS, the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), the Elections Assistance Commission (EAC), as well as local elections organizations, and CIS discussed the possibility of creating an ISAC devoted solely to the Nation's elections infrastructure. In 2017, DHS agreed to conduct a pilot elections ISAC with seven states. This pilot group developed and tested a range of products geared towards communicating cybersecurity issues to state and local election officials. Upon the success of that pilot, in 2018, DHS and the Election Infrastructure Subsector Government Coordinating Council tasked CIS to stand up the Elections Infrastructure ISAC (EI-ISAC). Leveraging the services offered and experience gained through the MS-ISAC, the EI-ISAC is now fully operational with all 50 states and D.C. participating, and more than 2,600 total members, including the election vendor community. The EI-ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials. CIS is installing a layered set of cyber defense capabilities for the elections infrastructure that results in what is often referred to as "defense-in-depth."

---

3 Find out more information about the EI-ISAC here: https://www.cisecurity.org/ei-isac/ .

The CIS Benchmarks.[4] CIS is the world's largest independent producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Benchmarks (also known as "configuration guides" or "security checklists") provide highly detailed security setting recommendations for a large number of commercial IT products, such as operating systems, data base products and networking systems. These benchmarks are vital for any credible security program. The CIS Benchmarks are developed through a global collaborative effort of public and private sector security experts. More than 200 consensus-based Benchmarks have been developed and are available in PDF format free to the general public on the CIS or NIST websites. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called "hardened images" that are based on the benchmarks that we are deploying in the Amazon, Google, Oracle, and Microsoft cloud environments. These hardened images help to ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS Hardened Images are used worldwide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan
- DHS Continuous Diagnostic Mitigation Program
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI)
- CIS Controls
- U.S. Department of Defense Cloud Computing Security Requirements Guide

The CIS Critical Security Controls.[5] CIS is also the home of the CIS Critical Security Controls (or the CIS Controls), the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene and essential cyber defense. They are developed by an international community of volunteer experts and are available free on the CIS website.

The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order, based on the current state of the global cyber threat. The CIS Controls are devised based on *how* malicious actors attack--and are updated regularly. What results is the clearest, most definitive blueprint of how to protect your organization from cyber-attacks. The NIST Cybersecurity Framework (CSF) is the *what*--NIST defines the categories of cybersecurity. The Controls are the *how*--the prioritized pathway to achieve the NIST goals. Moreover, the CIS

---

4 Find out more information about the CIS Benchmarks here: https://www.cisecurity.org/cis-benchmarks/

5 Find out more information about the CIS Controls and download them for free here: https://www.cisecurity.org/critical-controls.cfm

Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[6]

To bring another level of rigor and detail to support the development and implementation of the CIS Controls, CIS has developed its Community Defense Model,[7] which leveraged the industry-endorsed ecosystem that is developing around the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework.[8] The ATT&CK model comprehensively lists attack techniques that an attacker could use at each step of an attack.

In assessing the security value of the CIS Controls, we identified from the Verizon Data Breach Investigations Report and other sources the five most important attack types we want to defend against: Web-Application Hacking, Insider and Privilege Misuse, Malware, Ransomware, and Targeted Intrusions. Then, we examined the impact of Implementation Group 1 (IG1)—a prioritized subset of the CIS Controls that we have proposed as "Basic Cyber Hygiene"—security actions that are applicable to even the smallest and least-funded enterprises. Our analysis shows that implementing the Safeguards listed in IG1 is enough to defend against the top five attacks. That is, for each of the five attacks, the Safeguards in IG1 provide mitigation against all of the Techniques found in two or more steps (Tactics) of that attack. In addition to the value against this chosen set of five important attacks, IG1 mitigates against 62% of all ATT&CK Techniques, demonstrating significant value against a wide range of attacks. Taken together, these results strongly reinforce the importance of a relatively small number of well-chosen and basic defensive steps.

More broadly, our analysis shows that implementing the CIS Controls (in total) mitigate approximately 83% of all the Techniques found in ATT&CK, creating significant security value against a very wide range of potential attacks, even if you don't know any details about those attacks.

In summary, applying the CIS Controls provides critical, measurable security value against a very wide range of potential attacks, even if the details about those attacks are unknown. Our analysis shows that implementing the CIS Controls mitigates:

- approximately 83% of all attack Techniques found in the MITRE ATT&CK Framework.
- 80% of targeted intrusion techniques.
- 100% of instances of web-application hacking techniques.

Further, Implementation Group 1 ("IG1"), a subset of the Controls that is considered basic cyber hygiene, is effective in mitigation:

- 62% of all Techniques in the MITRE ATT&CK model.

---

6 NIST Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls)

7 https://www.cisecurity.org/white-papers/cis-community-defense-model/

8 MITRE ATT&CK: https://attack.mitre.org/

- 79% of malware attack pattern techniques.
- 100% of the Insider Privilege & Misuse techniques.

Many governments and private sector organizations around the world have seen the benefit of the CIS Controls and have endorsed or adopted them, including:

- **NIST Cybersecurity Framework.** Version 1.1 cites and maps to "CIS CSC" throughout Appendix A: Framework Core: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- **The American Aerospace and Defense Industry** based its National Aerospace Standard (NAS) on Cybersecurity on the CIS Controls: http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf

- **The Federal Reserve Bank of Richmond**: https://www.cisecurity.org/case-study/manage-cybersecurity-risk-with-the-cis-controls/

- **Federal Financial Institutions Examination Council** recommended a standardized approach to assessing cybersecurity preparedness and named the Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions: https://www.ffiec.gov/press/pr082819.htm

- **Conference of State Bank Supervisors**: *Cybersecurity 101: A Resource Guide for Bank Executives (2017)*, pages 8, 12, 24 https://www.csbs.org/sites/default/files/2017-11/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

- **Boeing and Exostar, Best Practices in Cyber Supply Chain Risk Management**: Boeing and Exostar chose the Critical Security Controls as the primary standard (page 4). This case study was part of the U.S. Resilience Project, National Institute of Science and Technology, U.S. Department of Commerce. https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf

- **U.S. Department of Transportation,** Federal Highway Administration, Transportation Management Center Information Technology Security, Final Report: https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf

- **National Consortium for Advanced Policing,**"Cybersecurity Guide for State and Local Law Enforcement": https://www.nccpsafety.org/assets/files/library/Cybersecurity_Guide_for_State_and_Local_Law_Enforcement.pdf

- **The Ohio Data Protection Act** became the first American statute to incentivize organizations to develop a strong data protection and cybersecurity program. The statute establishes legal protections for organizations that voluntarily adopt certain

recognized cybersecurity best practices and implement a written information security program. (Senate Bill 220, codified at O.R.C. §§ 1354.01-1354.05, CIS Controls at page four: http://codes.ohio.gov/orc/1354)

- **State of California**: The California Data Breach Report published by then-Attorney General Kamala Harris (2016) warns that failing to implement all relevant Controls in California "constitutes a lack of reasonable security." The Report effectively constitutes the world's first minimum level of information security. Find the Report here: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf) (see Recommendation 1).

    - CIS, CA standard of care: mentioning the CA AG citation of the Controls: https://www.littler.com/publication-press/publication/employers-receive-last-minute-reprieve-most-onerous-ccpa-compliance?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

- **The World Economic Forum (WEF)**:

    - White Paper, Global Agenda Council on Cybersecurity, World Economic Forum (lists CIS Controls as the first best practice at page 19, CIS cyber hygiene at Appendix A at page 26) (April 2016): http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

- **The European Union Agency for Network and Information Security (ENISA),** "Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers" (cites the CIS Controls as an industry standard at page 10 and maps to it throughout): https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/at_download/fullReport

- **The European Telecommunications Standards Institute (ETSI)** designated the CIS Controls as a principal means of implementing the European Union (EU) Network Information Security Directive (NISD) in a suite of Technical Reports (August 1, 2016):

    - CYBER; Critical Security Controls for Effective Cyber Defense; Part 1: The Critical Security Controls (Doc. Nb. TR 103 305-1 Ver. 2.1.1): http://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/02.01.01_60/tr_10330501v020101p.pdf

    - CYBER; Critical Security Controls for Effective Cyber Defense; Part 2: Measurement and auditing (Doc. Nb. TR 103 305-2 Ver. 1.1.1): http://www.etsi.org/deliver/etsi_tr/103300_103399/10330502/01.01.01_60/tr_10330502v010101p.pdf

    - CYBER; Critical Security Controls for Effective Cyber Defense; Part 3: Service Sector Implementations (Doc. Nb. TR 103 305-3 Ver. 1.1.1): http://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/01.01.01_60/

tr_10330503v010101p.pdf

    - CYBER; Critical Security Controls for Effective Cyber Defense; Part 4: Facilitation Mechanisms (Doc. Nb. TR 103 305-4 Ver. 1.1.1): http://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/01.01.01_60/tr_10330504v010101p.pdf

- ETSI subsequently added an additional technical report in this series featuring the CIS Controls:
    - CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement (2018-09) (includes as Section 5, "How to support the EU General Data Protection Regulation (GDPR) using the Critical Security Controls") (Doc. No. TR 103 305-5 V1.1.1) (September 2018): https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/01.01.01_60/tr_10330505v010101p.pdf

- ETSI also referenced the CIS Controls in this technical report:
    - CYBER; "Implementation of the Network and Information Security (NIS) Directive," provides guidance to meet the legal measures and technical requirements relating to the implementation of the EU Network and Information Security (NIS) Directive (CIS Controls at page 19) (Doc. No. TR 103 456 V1.1.1) (October 2017): https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

Further, the CIS Controls are, by design, aligned with existing government standards, and we provide an authoritative way to map from them to all of the major government as well as recognized industry standards.

The CIS Controls, therefore, are a *wise* choice because of the rigor and underlying data used in their creation; an *accepted* choice by private sector and government organizations around the world plus the industry eco-system that supports them (see Appendix A???); and a *safe* choice because it is already aligned with almost any path a that a future mandatory or expanded program could take.

(2) The scope of the cybersecurity problem facing this country

By now, the threat to governments, businesses, and American citizens is well known. In the most recent Worldwide Threat Assessment, the U.S. Office of the Director of National Intelligence concluded that "[O]ur adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners."[9]

Another report concluded that 88% of organizations worldwide experienced spear phish-

9 https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

ing attempts in 2019.[10] And this year alone, cybercrime is predicted to cost $6 trillion globally.[11]

No organization is immune. The recent SolarWinds attack revealed that approximately 18,000 of its customers have been exposed, including big businesses like Microsoft, Federal agencies like the U.S. Department of Defense and the U.S. Department of Homeland Security, as well as state hospitals and universities.[12]

(3) Why the approach taken by H.B. No. 6607 serves as an excellent step to improve our cybersecurity.

Cybersecurity is, largely, unregulated today. There is no national statutory minimum standard of information security. This condition makes it difficult to improve cybersecurity on a wholesale basis. Until there is a national legal standard, we are in a period where organizations must *voluntarily* adopt cyber best practices--the Wild, Wild, West. The result: We are not as safe as we could be.

Rep. Simmons's bill recommends that Connecticut adopt a critical interim step: *incentivizing* the voluntary adoption of cyber best practices. This bill would establish a legal safe harbor for organizations that *voluntarily* adopt certain recognized cybersecurity best practices (e.g., the NIST Cybersecurity Framework or our CIS Critical Security Controls) and implement a written information security program.

This approach does not *require* any organization to do anything. Instead, it creates an incentive to do the right thing--to improve cybersecurity according to a recognized industry standard--and receive an additional benefit in the bargain.

Therefore, absent from creating a specific statutory minimum cyber standard, which most legislative bodies are not ready to do, states can incentivize the voluntary adoption of cyber best practices. This provides a concrete approach that this country can adopt to improve our network defenses as we continue to define the appropriate roles and responsibilities among governments and businesses--and navigate cybersecurity's frontier period.

Conclusion

We thank the Connecticut General Assembly for allowing us this opportunity to testify today and for considering such a creative way to protect its citizens and organizations from cyber attacks. We respectfully recommend the passage of H.B. No. 6607.

---

[10] https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf at page 12.

[11] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[12] See, for example, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Attachment A
Biography of Curtis W. Dukes

Curtis W. Dukes
Executive Vice President & General Manager, Security Best Practices
The Center for Internet Security
https://www.cisecurity.org/

Curtis W. Dukes joined CIS as the Executive Vice President and General Manager of the Best Practices and Automation Group in January 2017. The CIS Benchmarks™ and CIS Controls™ program provides vendor-agnostic, consensus-based best practices to help organizations assess and improve their security. Prior to CIS, Curtis served as the Deputy National Manager (DNM) for National Security Systems (NSS). On behalf of the Director of NSA, the DNM is charged with securing systems that handle classified information or are otherwise critical to military and intelligence activities.

Dukes joined the National Security Agency in 1984 as a Computer Scientist. He served in a variety of organizations within NSA and earned the Distinguished Executive, Meritorious Executive, as well as Exceptional Performance and Meritorious Civilian Service Awards. He completed an overseas assignment and an intelligence community assignment for the Department of Defense. In Germany, Curtis had operational responsibilities for implementing Information Assurance activities across the European command. Following his community assignment, he became Deputy, then Chief of the Network Architecture and Applications Division, then Chief of the Systems and Network Attack Center. He later led highly skilled technical workforces as Director NSA/CSS Commercial Solutions Center. His last roles of responsibility at NSA were Deputy Director, then Director, of the Information Assurance Directorate.

Dukes earned a Bachelor's Degree in Computer Science from the University of Florida, and a Master's Degree in Computer Science from Johns Hopkins University. He is a 2004 graduate of the Intelligence Community Officer Training Program and a 2009 graduate of the Kellogg School Executive Development Program at Northwestern University.