Testimony of John M. Gilligan
President and Chief Executive Officer
Center for Internet Security
At the hearing entitled "Secure, Safe, and Auditable: Protecting the Integrity of the 2020"
Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation
Committee on Homeland Security
United States House of Representatives
Tuesday, August 4, 2020
12:00 to 2:00 p.m. ET

Chairman Richmond, Ranking Member Katko, and members of the Subcommittee, 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. (CIS). 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 American election security. 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.

Free and fair elections are essential to our democracy. In the United States, elections are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the federal government provides some laws and regulations, the federal government does not administer elections and has a limited role in dictating how the process is conducted. States act as the primary authority for the laws and regulations that govern the process of conducting an election and, accordingly, states have substantial discretion on the process of conducting elections through Secretaries of State and state election directors. State and local officials have been defending our elections for over two centuries. The 2016 election was less about a new threat and more about the breadth and depth of threat activity. Fortunately, since 2016 we have collectively learned a great deal about how best to respond to these cyber risks and to prepare for the 2020 election.

In short, I would like to: (1) provide you a short background about CIS; (2) describe the role and functions of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which we operate in conjunction with the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) with funding from Congress; (3) describe our collaboration with elections offices and key stakeholder organizations; (4) describe CIS's other, significant best practice work in this area; and (5) respectfully make three recommendations.

(1) 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 was instrumental in establishing the first guidelines for security hardening of commercial Information Technology (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 250 professionals at CIS provide cyber expertise in three main program areas: (1) the Multi-State Information Sharing and Analysis Center (MS-ISAC) and, more recently, the EI-ISAC; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

The CIS Benchmarks.[1] CIS produces the largest number 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. Over 200 consensus-based Benchmarks have been developed and are available in PDF format free to the general public on the CIS or NIST web sites. 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 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 Controls.[2] 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 founda-

---

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

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

tion 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 web site.

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 – achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[3]

To bring another level of rigor and detail to support the development and implementation of the CIS Controls, CIS leveraged the industry-endorsed ecosystem that is developing around the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework.[4] The ATT&CK Model comprehensively lists attack techniques that an attacker could use at each step of an attack. Our analysis shows that implementing the CIS Controls mitigates approximately 83% of all the techniques found in ATT&CK.[5] This implies that application of the CIS Controls provides significant security value again a very wide range of potential attacks, even if the details about those attacks are unknown.

MS-ISAC.[6] 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 practices. 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. This designation 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 over 10,000 other SLTT government entities including local governments,

---

3 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)

4 MITRE ATT&CK Framework, https://attack.mitre.org/

5 CIS Community Defense Model v 1.0, the Center for Internet Security, August 2020.

6 Find out more information about the MS-ISAC here: https://msisac.cisecurity.org/. A list of MS-ISAC services here: https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf

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 over 72,000 instances of malicious activity for over 8,500 MS-ISAC members. CIS is installing a layered set of cyber defense capabilities for the elections infrastructure that results what is often referred to as 'defense-in-depth'. The Albert IDS capabilities are being complemented with end point protection capabilities, as well as automated blocking of known malicious internet sites.

(2) The Role and Functions of the EI-ISAC

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[7] with all 50 states and D.C. participating, and over 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.

Deploying more Albert sensors. As part of the initial launch, CIS was also tasked with deploying a network of Albert sensors to all 50 state election offices and the five largest counties in states that have bottom-up and hybrid voter registration processes. Since then, all 50 states have deployed and many states have leveraged HAVA funding to procure additional Albert sensors for every county election office. CIS now processes data from 269 Albert sensors monitor-

---

[7] Find out more information about the EI-ISAC here: https://www.cisecurity.org/ms-isac/ .
A list of EI-ISAC services can be found here: https://www.cisecurity.org/ei-isac/ei-isac-services/

ing state and local election networks, which support online elections functions such as voter registration and election night reporting. The Albert sensors processed 30 petabytes of data in the first half of 2020, resulting in nearly two thousand cyber event notifications to elections offices.

Improving Situational Awareness. Starting with the 2018 primaries and mid-term elections, the EI-ISAC has hosted the Election Day Cyber Situational Awareness Room, an online collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats for any statewide or national election. More than 600 elections officials, federal partners, and election vendors have participated in these forums. It is expected that participation in the situation room will likely grow to all 50 states for the November 2020 General Election.

Piloting New Technology. Earlier this year, the EI-ISAC, in cooperation with DHS CISA and Congressional appropriators, expanded our protection of elections through two new programs aimed at addressing the needs of lower resourced organizations. These new programs also provide a defense-in-depth capability where multiple cyber defense capabilities working together improve threat situational awareness and increase effectiveness in defeating malicious threats:

The **Endpoint Detection and Response (EDR) Pilot for Elections Infrastructure** provides a sophisticated cybersecurity technology that complements the network monitoring performed by the Albert network sensors for the elections community. The EDR sensors also expand and enrich the threat intelligence available to the MS- and EI-ISAC. The EDR solution has the capability to monitor internal network traffic, and the EDR agents can programmatically block malicious activity and quarantine compromised systems, shifting the immediate cybersecurity response effort from election offices to the CIS SOC. This will allow smaller or less mature offices to take advantage of the same protections as larger offices improving the community's cybersecurity. CIS is currently deploying EDR sensors, focusing on critical systems in the elections infrastructure, like voter registration, election management, and election night reporting.

The **Malicious Domain Blocking and Reporting (MDBR) Pilot** provides a commercial secure Domain Name System (DNS) service to block access from SLTT member organizations to known malicious domains. In effect, the capability prevents the execution of the majority of malicious attacks associated with ransomware, malware, command and control, and phishing domains. Anonymized data from this offering will be correlated with other threat intelligence feeds and provided in threat reporting to CISA and the broader SLTT community. The MDBR capability can be implemented in minutes and recent NSA analysis indicates that this solution can reduce the ability for 92% of malware, from a command and control perspective, to deploy malware on a network.[8] CIS began deploying this capability in early July. While the capability is available to all

8 "The NSA is piloting a secure DNS service for the defense industrial base", Cyberscoop, June 18, 2020, https://www.cyberscoop.com/nsa-secure-dns-service-pilot-defense-industrial-base/

SLTT organizations, the priority is to deploy to elections organizations prior to November.

(3) Collaboration with Elections Offices and Key Stakeholder Organizations

Both as a part of CIS's role in operating the EI-ISAC as well as efforts not funded by the government, we have placed emphasis on establishing a trusted relationship with elections officials and other key stakeholders. CIS has participated and conducted cyber exercise for elections offices, conducted numerous cyber webinars, and made in person visits to almost every state and many local elections jurisdictions, many of these activities in partnership with DHS CISA. In addition, we have worked closely with other key organizations supporting the elections community such as the National Association of Secretaries of State (NASS), the National Association of State Elections Directors (NASED), the Elections Assistance Commission (EAC), the Election Center, and the International Association of Government Officials (IGO). Finally, we have also worked closely with private sector organizations such as Harvard's Belfer Center, Microsoft, elections vendors, and other organizations who are working to improve the security of our elections infrastructure.

(4) CIS's Other, Significant Election Security Best Practices

CIS also makes significant investment is Election Security Best Practices and related tools. Since the release of our *Handbook for Election Infrastructure Security* in 2018, CIS has become the leading non-government provider of election security advice to SLTT election authorities, election technology vendors, and the elections community at large.

The *Handbook for Election Infrastructure Security* provides 88 best practices covering the entirety of the election administration technology. These best practices have been widely adopted by the election community with state and local offices in 34 states using them as a metric for assessing the security of elections systems. To assist states and local election officials assess and adopt these best practices, CIS developed and maintains the Election Infrastructure Assessment Tool (EIAT). The EIAT is a free online tool designed to help election officials assess their IT infrastructure against the 88 best practices from the Handbook. We have had over 600 users representing 34 states and 265 local election jurisdictions take advantage of the EIAT.

A Guide for Ensuring Security in Election Technology Procurements was released in May 2019 to assist election officials with ensuring security is properly accounted for in their election technology procurements. This guide provides 33 recommended questions to ask of election technology providers and assist election officials assess responses by providing descriptions of good and bad responses.

CIS released its ***Security Best Practices for Non-Voting Election Technology*** in October 2019 to address internet-connected election technology such as electronic pollbooks, electronic ballot delivery, and election night reporting systems. This guide covers five areas of technology:

Network and Architecture, Servers and Workstations, Software Application, Data, and Administration. The areas were chosen carefully based on similarities in threats, mitigations, and governance.

CIS has followed up these election technology best practices with an ongoing pilot project on how to verify systems against these best practices. Traditional voting systems are verified against large monolithic standards using lengthy and expensive certification campaigns. Our alternative approach, known as **Rapid Architecture-Based Election Technology Verification (RABET-V)**, focuses on the need for internet-connected election technology to be responsive and adapt quickly to changes in the threat landscape. RABET-V is addressing this with a process model that provides assurances of security, reliability, and functionality in a risk-based, flexible, change-tolerant process. We are currently piloting this process with several election technology vendors and a steering committee consisting of the Election Assistance Commission, DHS CISA, Federal Voting Assistance Program, and the States of Wisconsin, Ohio, Maryland, Texas, Pennsylvania, and Indiana. We anticipate a report following the November General Election.

Misinformation Reporting Portal Pilot.[9] CIS is currently producing a better means for election officials to report election infrastructure misinformation and disinformation to the social media platforms for their investigation and adjudication. Currently, a limited set of election officials can report to Facebook and Twitter using the means provided directly by the social media platform. Elections officials must pre-register with the platform and report independently to each one. CIS is working to facilitate a single reporting portal where election officials can report the suspected misinformation and disinformation once, and have it distributed to the various social media platforms. We have been working closely with DHS, NASS, and NASED, along with five States to vet and promote this concept to the social media platforms.

The Misinformation Reporting Portal will provide elections officials with a single place (i.e., the portal) for reporting mis- and disinformation across multiple social media platforms with a streamlined, consistent user experience. In addition, the entire elections community will have visibility of what's going on with mis- and disinformation in the elections community within and outside their jurisdictions, including to see trends and be able to strategically respond. The portal will also streamline and standardize reporting for the social media organizations. In addition, voters will have the benefit of more rapid correction of erroneous information, leading to improved voter confidence.

(5) Three Recommendations to Continue Securing Elections

While much progress has been made over the last four years, we know that the threat remains, and, as a nation, we must continue to address these new risks and vulnerabilities. We re-

---

[9] The RABET-V and Misinformation Reporting Portal are projects being funded by the nonprofit Democracy Fund.

spectfully recommend three courses of action to keep our elections safe and secure. We must: (1) continue to emphasize the importance of collaboration and foster collaboration across all elections stakeholders; (2) continue to innovate and leverage evolving security and applicable commercial technologies; and (3) consider how best to address the impact of mis- and disinformation on American elections.

Emphasize Collaboration: We hear much of the importance of resilience in the homeland security context. When you look back on it, the post-2016 response to securing our elections is an excellent example of a successful public-private partnership. The recognized shortfalls in 2016 have helped highlight a national crisis that has been responded to by many organizations working together.

NASS, NASED, the Election Center, IGO and their respective members remain central in running American elections. Collectively, they continue to provide the deep expertise in exactly how the complicated function of operating elections works, and how new processes and technology can best be used in each jurisdiction. Other state and local associations like the National Governors Association (NGA), the National Conference of State Legislatures (NCSL), the National Association of State Chief Information Officers (NASCIO), the National Association of Counties (NACo), the National League of Cities (NLC), the National Emergency Management Association (NEMA), and others have stepped up and collaborated to identify and facilitate the best approaches to improving security of the elections infrastructure within their jurisdictions.

On the federal side, Congressional appropriators were several times able to provide significant funding for critical election security grants that were, simply put, essential to help prepare elections offices with limited resources across the country. An active and engaged DHS CISA enthusiastically accepted the role of the Nation's Risk Advisor on elections, used their convening power and bully pulpit as the lead Federal agency to good effect, and CISA continues to be an excellent partner in the MS- and EI-ISACs. Despite having one of the smallest budgets in the federal government and new leadership, the Election Assistance Commission (EAC) efficiently distributed $825 million in grants to the states, helped develop guidance around voting as safely as possible during the COVID-19 pandemic, and stood up a RABET-V (with CIS as described above).

Further, the elections vendors, private sector, public and private universities, think tanks and foundations, as well as nonprofit corporations like CIS have come together to help address the technical, process, and educational challenges facing the U.S. elections community. The result is that the protection capabilities of our elections infrastructure are enormously improved from 2016 and even where they were in 2018. However, it is recognized that we are not yet where we want to be and the threat continues to increase. It will take continued collaboration to sustain and hopefully even accelerate the progress that we have seen over the past three years.

Continue to Innovate: As noted above, the progress made in deploying additional technical measures and in education and training since November of 2016 is impressive. However, there are opportunities to improve in each area. A danger when addressing the sensitive area of

elections is to be overly cautious in assessing and piloting new methods and technical solutions. CIS was grateful to be given funding from Congress and tasking from CISA to pilot EDR and the MDBR technology. We are already seeing that these technologies will be important capabilities to protect our elections infrastructure. Working with the EAC, we are piloting what we hope will be a much quicker and less costly process for verifying elections systems. We encourage Congress to continue to support experimentation and innovation so that we can continue to leverage the best talent and capabilities that the country has to offer in a way that produces the most value for the American taxpayer.

Address the impact of mis- and disinformation on elections: While we have made great strides in improving resilience against cyber threats, perhaps the biggest challenge that we face as a nation going forward is how we address the impact of mis- and disinformation on elections. While we treasure our rights granted to all citizens by the First Amendment, the power of social media in shaping opinions and attitudes is expanding rapidly. CIS is working to help address the challenge of identifying and reporting deliberate or accidental misinformation or disinformation that might prevent voters from exercising their right to vote. This is a first step. However, the broader challenge is to establish norms and conventions that will help voters understand what is factual and what is opinion or even deliberate attempts to mislead. We would encourage Congress to take an incremental approach to addressing this challenge.

Conclusion

Securing American elections is a complex, decentralized enterprise that is fundamental to preserving our democracy. Fortunately, our state secretaries of state, state elections directors, and elections officials have been successfully defending our elections for over two centuries. Furthermore, since 2016, we have learned much about how this new risk can be defended. CIS is proud to have developed and to operate the Elections Infrastructure ISAC (EI-ISAC), and to have devised several other significant best practices to help the with this vital task.

To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a national response to threats against election infrastructure.

Attachments A: Biography of John Gilligan

John M. Gilligan
President and Chief Executive Officer
CIS (The Center for Internet Security, Inc.)

John Gilligan became the President and Chief Executive Officer of CIS (The Center for Internet Security, Inc.) in October of 2018. He served on CIS' Board of Directors from 2005 – 2018 and was Chairman of the Board from 2009 – 2018.

Gilligan has more than 25 years of managerial experience in leading large organizations with expertise in cybersecurity, business strategy, organizational innovation, and program implementation. He served as President and COO of the Schafer Corporation from May 2013 until May 2017. Prior to Schafer Corporation, he was the President of Gilligan Group, a Virginia based IT and cyber consulting firm. Before founding the Gilligan Group, Gilligan was a Senior Vice President and Director, Defense Sector, at SRA International, Inc.

Gilligan served as the Chief Information Officer for the United States Air Force and the U.S. Department of Energy. Gilligan's government experience includes working as the Program Executive Officer (PEO) for Command and Control Battle Management Operations for the United States Air Force. He was a member of the Cyber Security Commission (formed to advise the 44th President) and has served as an advisor to the Office of the Secretary of Defense on IT reform.

In addition to his work with CIS, Gilligan is currently on the boards of the Software Engineering Institute, Isobar Inc., and the Armed Forces Communications and Electronics Association. He currently co-chairs the Cyber Committee of the Armed Forces Communications and Electronics Association (AFCEA). Gilligan has also served on the boards of directors for Cyber Griffin Inc., Schafer Corporation, and HDT Global Inc.

Gilligan's published work on cybersecurity includes CIS' A Handbook for Elections Infrastructure, The Economics of Cybersecurity Part I: A Practical Framework for Cybersecurity Investment and The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework. The last two publications were coordinated via the AFCEA International's Cyber Committee.