Written Testimony
Amit Yoran
Chairman and CEO, Tenable, Inc.
House Committee on Oversight and Reform
"Hearing to Examine H.R 7331, the National Cyber Director Act"
July 15, 2020

Introduction

Chairwoman Maloney, Ranking Member Comer, and members of the Committee, thank you for the opportunity to testify today on the creation of a National Cyber Director (Director or NCD) role within the Executive Office of the President. There are steps we can and should take now to protect against devastating cyberattacks in the future. If there's one thing we have learned from the current health crisis, it's that the worst-case scenario can happen and the best time to prepare for it is now. I applaud the Committee's efforts to better understand all aspects of these issues.

My name is Amit Yoran and I am the Chairman and CEO of Tenable. I have spent over 20 years in the cybersecurity field. I received a Master of Science in computer science from The George Washington University and a Bachelor of Science in computer science from the United States Military Academy. I served as the Director of the National Cybersecurity Division from 2003 to 2004 and as the founding Director of the U.S.-CERT program. Additionally, I have served on a number of Presidential advisory commissions. As an innovator and entrepreneur in the security space, I founded and built two security companies: Riptech, acquired by Symantec; and NetWitness, acquired by RSA, where I went on to serve as the president of RSA from 2014 through 2016. I have also served as a director and advisor to security startups and industry advisory boards. I have previously testified before congressional committees on cybersecurity policy, encryption and other related issues.

The company I lead, Tenable, is headquartered in nearby Columbia, Maryland. Tenable has 1,400 employees globally and more than two million users and 30,000 customers worldwide. Tenable is publicly-traded on the NASDAQ and is the world's leading provider of vulnerability management technologies. Our company is laser-focused on transforming the cybersecurity industry by providing organizations with an unmatched breadth of visibility and depth of analytics to measure and communicate cyber risk to make better strategic decisions. Our goal is to eliminate blind spots, prioritize threats and reduce exposure and loss.

Simply put, Tenable empowers organizations of all sizes to understand and reduce their cyber risk. For the federal government specifically, Tenable provides the most widely deployed vulnerability assessment solution, serving just about every department and agency. Our solutions are also broadly used by state and local governments to manage cyber risk.

H.R. 7331 and the Role of the National Cyber Director

The Cyberspace Solarium Commission's mission was to develop recommendations to improve our country's cybersecurity posture. The Commissioners offered a bi-partisan look at actionable steps to scale best practices across the government and improve public-private partnerships for greatest effect. The Commission recommendations focus on improving U.S. Government structures for cybersecurity, strengthening cybersecurity norms, enhancing military cybersecurity capabilities, improving public private partnerships, and driving a stronger national cybersecurity ecosystem.

One of the key recommendations was the establishment of the Office of the National Cyber Director, and I'd like to thank Commission members – including Rep. Jim Langevin and Rep. Mike Gallagher – for their foresight and leadership in developing the report and for drafting this legislation to codify that recommendation. I'd also like to thank Chairwoman Maloney for serving as a co-sponsor of this legislation.

I concur with the commission's recommendation and H.R. 7331, to establish the role of a National Cyber Director and the supporting Office of the NCD. As cybersecurity threats grow increasingly more complex and the consequences to American democracy and way of life become clearer, the need for a consolidated and harmonized approach to cyber across all levels of the U.S. Government, internationally, and with the private sector, becomes increasingly critical. Cyber silos in different federal agencies create a patchwork of disjointed cyber activities that confuse both industry and government, undermine accountability, and put citizens at greater risk.

As Rep. Jim Langevin has said, "[By] establishing a National Cyber Director with the policy and budgetary authority to reach across government, we can better address cybersecurity vulnerabilities and gaps holistically and prevent catastrophic cyber incidents."[1]

A National Cyber Director, to be housed within the Executive Office of the President, is needed to oversee and coordinate federal government activities that ensure the U.S. is prepared to defend against adversarial cyber operations and to formulate and maintain an international cybersecurity strategy and lead international efforts to develop norms for responsible state behavior in cyberspace. The President would benefit tremendously from an advisor with not only the technical understanding to deal with emerging technology issues, but also experience working with private industry and knowledge of how interagency processes work. Operating at the White House level will enable him or her to see cyber activities across the whole of government to more effectively plan, resource, and deploy government cyber resources and develop better orchestrated policies. This position has become more critical as the federal government leverages more connected technologies, which can make it more susceptible to exploit.

The reality is that a whole-of-nation risk requires a whole-of-nation effort. Indeed, the massive expansion of digitally connected government and critical infrastructure assets constitutes a broadly

[1] Congressman Jim Langevin, "Congressional Cybersecurity Leaders Introduce Bipartisan Legislation to Establish a National Cyber Director,"
https://langevin.house.gov/press-release/congressional-cybersecurity-leaders-introduce-bipartisan-legislation-establish

expanded attack surface, which stretches across the entire government and critical services. Every agency. Every department. Health and Human Services, the Internal Revenue Service, the Departments of Energy, Education, Transportation, Commerce, Agriculture as well as our military and intelligence services—none are immune from the threat of cyberattacks that imperil national security as well as government services that citizens rely on. And each has a role to play in our government efforts to help secure the nation. This whole-of-nation effort must work closely with the private sector that performs many critical functions for the nation.

H.R. 7331 would provide the National Cyber Director with several important authorities to help drive stronger enterprise risk management practices across the federal government. It is critical for the Director to have visibility into, and coordination authority with, the Department of Defense (DoD), intelligence agencies, and law enforcement community, in order to coordinate cyber strategy, policy and activities across the entire federal enterprise.

With visibility into all the systems, equipment and processes required to deliver on a business continuity and disaster recovery plan, cybersecurity leaders are increasingly a critical part of business functionality. In the private sector, we find that Chief Information Security Officers, Chief Security Officers and other cybersecurity leaders are uniquely suited to take on a bigger role in the risk management activities of the enterprise as their work puts them directly at the intersection of technology and business. These roles are empowered by company leadership and frequently brief the CEO, Board of Directors, and/or Audit and Risk Committee of the Board on a regular basis. They plan and execute whole-of-company defense processes and practices and are instrumental to understanding and managing enterprise risk in the technology era.

Similarly, the President needs a principal advisor for cybersecurity. In that capacity, the Director will lead the development of cybersecurity strategy and policy in coordination with federal agencies; conduct oversight of federal agency implementation of national and international cyber strategies; and make recommendations to the Office of Management and Budget on federal agency cybersecurity budget requests.

In addition, the Director will have the authority to work with the Department of Homeland Security (DHS) and private sector critical infrastructure owners and operators to push for effective risk management practices to manage the growth in cyber exposure and risk. With the convergence of information technology (IT) and operational technology (OT) infrastructures, an OT security event can have a material effect on operations spanning beyond information leakage to equipment damage, safety concerns for employees, or a major environmental incident. As Congressman Gallagher has noted, the Office of the National Cyber Director must be interdisciplinary and functionally oriented.[2] The Office of the NCD must be able to coordinate cyber activities across industries in the private sector, in addition to the work that sector-specific agencies and DHS are doing.

[2] Nextgov, "Senator Pushes to Require National Cyber Director in Defense Authorization Bill," https://www.nextgov.com/cybersecurity/2020/05/senator-pushes-require-national-cyber-director-defense-authorization-bill/165374/

These authorities will provide the Director with visibility across the federal government, the ability to drive important risk management practices across the enterprise, and the trust necessary to coordinate with private sector critical infrastructure owners and operators on cybersecurity strategy. In the private sector, organizations that prioritize cybersecurity do better – they're less prone to breaches, both small and large, that cause real impacts to their operations. The same is true in government. This is an investment with tangible benefits.

Additional Authorities for the National Cyber Director

Beyond the authorities already included in H.R. 7331, I recommend additional authorities for the National Cyber Director that would improve the nation's cybersecurity risk management for both the public and private sectors. These additional authorities include developing a national encryption policy, managing the Vulnerabilities Equities Process (VEP), coordinating with regulatory entities, driving cybersecurity workforce development, and leading all international cybersecurity efforts, to include the development of international cyber strategies and international engagement.

Encryption Policy

The Director's role should include the development of a national encryption policy to safeguard our systems – not make them more vulnerable. The role should bring a cyber practitioner's knowledge of encryption to balance industry and government objectives in security and access to information. As I've testified before on April 19, 2016, to the House Energy and Commerce Subcommittee on Oversight and Investigations, promoting strong encryption improves public safety.[3] A Director should provide balance to the argument put forth by law enforcement to ensure they are leveraging the lawful tools and methods available to them, and have robust technical training to access needed information without weakening overall security. Weakening encryption increases cyber exposure for us all – something we can't afford in today's threat landscape. This will achieve balance between the needs of law enforcement on the one hand and cybersecurity on the other.

Vulnerabilities Equities Process

The Director should oversee the VEP and Review Board, which is tasked with determining "whether, when, how, to whom, and to what degree" a vulnerability held by a government entity should be disclosed to a non-government entity. Disclosing these vulnerabilities as appropriate helps improve our overall cyber posture, our critical infrastructure and our economy. The process must also consider national security and law enforcement needs. The Director should bring together government officials with equities in vulnerability disclosure and drive a government consensus on disclosure decisions that will safeguard the public interest and improve our national cyber posture.

[3] Testimony of Amit Yoran before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/Yoran2_Testimony-OI-Encryption-Hrg-2016-4-19.pdf

Regulatory Coordination

The Director should have the authority to coordinate cybersecurity policies and practices with regulatory agencies to promote greater accountability and mitigate risk. These agencies could include the Department of Energy (DOE), Department of Transportation, Securities and Exchange Commission (SEC) and others. For example the Cyber Solarium Commission Report recommends Congress amend the Sarbanes-Oxley Act to explicitly account for cybersecurity in addition to the other corporate accountability requirements already enforced by the SEC on publicly traded U.S. companies. The Director can also work with the SEC to evolve its enforcement practices with respect to cybersecurity risk management.

This critical step would increase transparency and improve security practices without dictating specific technologies. Attestation by CEOs that an organization has reviewed their security practices and believes them to be in line with the threat environment and risk to their business might be the singular act that has the greatest transformation on corporate cybersecurity and standards of care. This process is vital to get organizations to implement best practices that will fundamentally improve our corporate and national preparedness.

Cybersecurity Workforce

The Director should be responsible for overseeing cybersecurity workforce development initiatives and developing and enforcing policies for greater inclusion. There is a well-documented talent shortage in the cybersecurity workforce. According to the Global Information Security Workforce Study released in February, the workforce shortage is projected to reach 1.8 million people by 2022. The lack of diversity in the industry is a contributing factor. Women constitute only 14% of the cybersecurity workforce in North America and just 11% of the cyber workforce globally.[4] Minority representation within the cybersecurity profession is 26%, only slightly higher than the overall U.S. minority workforce (21%).[5] Only through increased inclusion and diversity—of race, gender, perspective and thought—can our industry achieve greater creativity and innovation and develop new solutions to our most vexing challenges. Among other initiatives, Tenable's efforts in this areas include implementation of a "Rooney Rule"[6] to force greater inclusion during hiring, especially for leadership and senior positions, dedicating recruiting efforts to source more diversity candidates, employee resource groups with executive sponsorship for greater inclusion of our minority workforce, and initiatives that evaluate and enforce equal pay and promotion opportunities.

The nation needs a bold, new cyber workforce strategy that develops and advances the ranks of people from all walks of life. While the private sector can lead the way, we need buy-in and partnership from the government to invest in recruiting, developing and retaining talent. Cyber workforce development requires top level attention and should be at the forefront of priority initiatives for the National Cyber

[4] Frost & Sullivan, "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf

[5] Frost & Sullivan, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

[6] Wikipedia, https://en.wikipedia.org/wiki/Rooney_Rule

Director to ensure that the U.S. remains competitive for the best cyber talent available. The Director should also consider cyber workforce policies to attract foreign cyber experts with needed technical talent.

International Engagement

The Director should develop and maintain an international cyber strategy for the nation. This should include the development of international norms for responsible state behavior in cyberspace and represent the U.S. position in international engagements with foreign governments. This work will supervise and lead the interagency process for implementation of the strategy across the federal agencies, to include the Department of State, Department of Justice and other key stakeholders. In consultation with the Office of Management and Budget, the Director should monitor and assess the effectiveness, including cost effectiveness, of federal departments' and agencies' implementation of the strategy. The Director should also make recommendations for organizational changes or resource allocation and policies for departments and agencies responsible for implementing the strategy.

The Modern Attack Surface

I joined the Department of Homeland Security in 2003 as the Director of the National Cybersecurity Division. It was the National Cyber Security Division's mission at the time to get our critical federal cybersecurity program off the ground. In that role, our team led the launch of the U.S.-Computer Emergency Readiness Team (US-CERT), with a series of programs to protect the nation by coordinating defense against and response to cyberattacks of significant consequence.

The cyber threats that we face today are far greater in scope and scale than a decade ago.[7] Across the country, government agencies, businesses and consumers are connecting more to the internet than ever before utilizing cloud computing, Internet of Things (IoT) and OT. These technologies optimize production, drive innovation and increase sustainability; however, they also increase the overall cybersecurity attack surface. This includes industries that are essential to our public safety and well-being, such as power, water, transportation and healthcare as well as industrial production. As we grow more reliant every day on data and technology, our adversaries continue to innovate new and bolder ways to compromise these systems for economic, political and military gain.

Over the last ten years, nation state actors, criminals and other adversaries have repeatedly relied on cyberattacks to conduct espionage and intellectual property theft, to target oil and natural gas pipelines, to attempt to undermine U.S. elections,[8] to steal personal information and generally to disrupt and disable governments, including the United States. In a report that Tenable commissioned from the Ponemon Institute in 2019, 90% of critical infrastructure operators stated that their environments had

[7] Privacy Affairs, "Cyberwarfare Statistics: A decade of geopolitical attacks," https://www.privacyaffairs.com/geopolitical-attacks/

[8] Axios, "Russia has already won the fight to undermine U.S. elections," https://www.axios.com/putin-russia-undermine-trust-us-elections-4dce1cb3-4696-41d0-8a71-ef8fe362f1f8.html,

been damaged by at least one cyberattack over the past two years, with 62% experiencing two or more attacks.[9]

The loss of hundreds of millions of dollars and damage to global economic capacities through incidents like WannaCry and Not Petya should be a call to action for organizations, governments and enterprises to protect more than just their IT infrastructure. Now more than ever, we need a National Cyber Director to coordinate our national activities, policies and actions in cyber.

Pandemic-related Threats on the Rise

In the past several months, we've seen cybercriminals take advantage[10] of the current COVID situation by ramping up malware and phishing campaigns, some specifically targeted at state and local governments, schools, and healthcare systems trying to administer vital aid to impacted communities.[11]

Despite this increase in cyberattacks and the criticality of protecting essential resources, infrastructure and public services, state and local governments lack the resources needed to bolster their cybersecurity posture.[12] States have been forced to choose between protecting their citizens from a global health emergency or having their personal data, health records and unemployment benefits held hostage by cybercriminals. As Rep. Mike Gallagher stated, "The coronavirus has elevated the importance of cyber infrastructure and demonstrated how incredibly disruptive a major cyberattack could be….But while we are woefully unprepared for a cyber calamity, there is still time to right the ship."[13]

---

[9] Tenable, "Cybersecurity in Operational Technology: 7 Insights You Need to Know," https://www.tenable.com/ponemon-report/cybersecurity-in-operational-technology; Tenable, "Ponemon-Tenable Study, https://www.tenable.com/press-releases/ponemon-tenable-study-find-60-of-organizations-suffered-two-or-more-business

[10] Tenable, "COVID-19: Coronavirus Fears Seized by Cybercriminals," https://www.tenable.com/blog/covid-19-coronavirus-fears-seized-by-cybercriminals

[11] Tenable, "COVID-19: Coronavirus Fears Seized by Cybercriminals," https://www.tenable.com/blog/covid-19-coronavirus-fears-seized-by-cybercriminals; CBS Chicago, "Ransomware Attack Renders LaSalle County Government Computers Unusable," https://chicago.cbslocal.com/2020/03/04/ransomware-attack-renders-lasalle-county-government-computers-unusable/; Government Technology, "Ransomware Attack Forces Texas Court Servers Offline," https://www.govtech.com/security/Ransomware-Attack-Forces-Texas-Court-Servers-Offline.html; Healthcare IT News, "Ransomware attack leaves 5 years of patient records inaccessible at Colo. Hospital," https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital; KrebsonSecurity, "Florence, Ala. Hit By Ransomware 12 Days After Being Alerted by KrebsOnSecurity," https://krebsonsecurity.com/2020/06/florence-ala-hit-by-ransomware-12-days-after-being-alerted-by-krebsonsecurity/; WBIR 10 News, "City of Knoxville computer network hit by 'ransomware' attack," https://www.wbir.com/article/news/local/city-of-knoxville-computer-network-hit-by-ransomware-attack/51-3302a2bd-8e1f-4387-bf81-a387d20087da

[12] Statescoop, "States say next pandemic relief bill needs IT and cybersecurity aid," https://statescoop.com/states-say-next-pandemic-relief-bill-needs-it-cybersecurity-aid/

[13] Homeland Preparedness News, "Bill introduced to establish National Cyber Director," https://homelandprepnews.com/stories/51525-bill-introduced-to-establish-national-cyber-director/

To solve this problem, state and local governments are urging the federal government to step in and fill this funding gap.[14] Targeted cybersecurity funding, either from DHS or through established grant programs, is needed to ensure that state and local governments have the resources they need to protect their citizens, assets and maintain continuity of operations. A National Cyber Director in the White House, with the ability to scale budgets is key to protecting these critical systems and assisting all levels of government navigate through this difficult time.

At Tenable, we are proud to help customers,[15] including federal, state, and local governments, reduce their cyber risk during the pandemic by extending licenses of our products for free, providing free weekly sessions with our engineers to share tips and best practices, and offering free webinars and sound advice[16] on securing the remote workforce.[17]

We Are Not Helpless: The Benefits of Modern Cyber Risk Management

In 2018, David Hogue, a National Security Agency official, said the NSA had not responded to an intrusion that was the result of a zero-day exploit in over two years. The vast majority of breaches have leveraged unpatched, known vulnerabilities.[18] Government policy should not allow for "learned helplessness" by federal government agencies or private industry. Helplessness allows individuals and organizations to remain negligent and avoid accountability for not taking even the most basic steps to improve cyber posture.

On the contrary, government policy should raise the bar for baseline cyber hygiene practices in both the public and private sectors. While the government can play a stronger role in deterrence, to include thoughtful consideration of offensive capabilities, attributing attacks and establishing sanctions regimes, those efforts should not replace the promotion and implementation of basic cyber hygiene practices and processes.

At Tenable, we've taken cyber hygiene a step further by prioritizing vulnerabilities that are most likely to be exploited and cause the most harm through our Cyber Exposure platform. As the attack surface grows, so too does the volume and severity of vulnerabilities. Beginning in 2017, the average number of new vulnerabilities roughly doubled from prior years and continues to climb. The number of new

---

[14] Statescoop, "States say next pandemic relief bill needs IT and cybersecurity aid," https://statescoop.com/states-say-next-pandemic-relief-bill-needs-it-cybersecurity-aid/

[15] Tenable, "We're Here to Help: Securing Your Remote Workforce," https://www.tenable.com/blog/we-re-here-to-help-securing-your-remote-workforce

[16] Tenable, "Security Advice for Government Agencies in the Age of COVID-19," https://www.tenable.com/blog/security-advice-for-government-agencies-in-the-age-of-covid-19

[17] Tenable, "We're Here to Help: Securing Your Remote Workforce," https://www.tenable.com/blog/we-re-here-to-help-securing-your-remote-workforce; Tenable, "Security Advice for Government Agencies in the Age of COVID-19," https://www.tenable.com/blog/security-advice-for-government-agencies-in-the-age-of-covid-19

[18] Public Technology, "NSA: 'We have not responded to a zero-day in two years – our adversaries are hitting known vulnerabilities,'"https://www.publictechnology.net/articles/features/nsa-%E2%80%98we-have-not-responded-zero-day-two-years-%E2%80%93-our-adversaries-are-hitting-known

vulnerabilities in 2019 was 17,313, increased by 10% compared to 2018 (16,556), by 14% compared to 2017 (14,714), and by 37% compared to 2016 (6,447).[19] Providing dynamic and continuous visibility of vulnerabilities, threats and asset criticality data, Cyber Exposure allows end-users to focus on the vulnerabilities and assets that matter most, and allows organizations to focus on their actual cybersecurity risks.

A National Cyber Director with visibility across the whole of governments would be able to apply a similar discipline across the federal government.

There are steps we can take to protect ourselves—as individuals, as organizations, and as a nation. The Director would help ensure that the government holds itself and industry accountable for those steps and that federal government agencies and private sector organizations that are negligent answer to authorities at the highest levels of government.

The Benefits of Cross Collaboration

Cybersecurity is too important to be managed in silos. Cross-agency collaboration in the federal government and with industry can help reduce risk by sharing actionable information between agencies, limiting duplicative efforts, and improving results. Recently, DHS, DOE and DoD extended their joint effort to develop common cyber threat indicators and defense capabilities to protect critical infrastructure in the energy sector, allowing them to share threat information, better patch vulnerabilities and more.

This collaboration will help all three agencies improve their cyber capabilities without duplicating efforts. The type of coordination to protect the nation's OT and critical infrastructure needs to happen among all departments and agencies across the government to protect every asset, from the electric grid to next-generation weapons systems and agency information.

Cyberspace Solarium Commission Recommendations on Strengthening the Cybersecurity Infrastructure Security Agency

The Cyberspace Solarium Report also included recommendations on how to further strengthen the Cybersecurity Infrastructure Security Agency (CISA) in order to ensure the national resilience of critical infrastructure, promote a more secure cyber ecosystem and serve as the central civilian authority to support federal, state, local and private sector cybersecurity efforts.

CISA has established information sharing capabilities across the government, provides technical assistance to cybersecurity operators in the public and private sectors, and engages stakeholders both inside and outside the federal government.

However, CISA's role has clear limitations:

[19] Tenable, "Vulnerability Intelligence Report," https://www.tenable.com/cyber-exposure/vulnerability-intelligence#download

- CISA's convening power is not widely understood or consistently recognized.
- CISA does not have jurisdiction over law enforcement, the Department of Defense or federal intelligence agencies, which are all critical pieces of a unified approach to U.S. cyber defense, nor are these organizations required to collaborate and share their activities with CISA.
- CISA does not have the budget or the analytic capacity to assess, plan for and lead a unified effort to mitigate national systemic cyber risk.

The creation of the National Cybersecurity Director role should be done in conjunction with efforts to empower and appropriately resource CISA as a critical player to improve the nation's cybersecurity.

To strengthen CISA, Congress should elevate the Director position as recommended by the Cyberspace Solarium Commission and provide additional funding and program support that will enable the organization to enhance current operations. An expanded budget would also allow CISA to increase funding for the Continuous Diagnostics and Mitigation (CDM) program in order to meet surge capacity to protect .gov networks, support state and local cybersecurity networks and systems, and expand other programs that support the private sector, including many of the public-private operations that comprise the U.S. critical infrastructure.

Additional Cyberspace Solarium Commission Recommendations

In addition to the creation of the National Cyber Director position, the Cyberspace Solarium Commission report includes other cogent recommendations to help the government prepare for major cyberattacks on our critical infrastructure and economic system.

Among the most impactful, actionable policy recommendations included in the report are the need to harmonize standards for vulnerability disclosure and patch management; requirements for the military to conduct vulnerability assessments of major weapons systems; requirements for increasing public company cybersecurity transparency; and the establishment of critical technology security centers in areas such as network technology and connected industrial control systems. These recommendations should be passed by Congress immediately.

There are also important issues that the report raises, but where we would recommend complementary legislative approaches. For instance, while the report calls for greater liability for manufacturers that release products with known, unpatched vulnerabilities, we believe a complementary approach would be to also pass legislation that shields organizations from increased liability if they can demonstrate that they follow a risk-based standard of care. A risk-based approach requires that you know what's on your network. When you have visibility into your cyber exposure, you can identify and prioritize the risks that pose the greatest threat to your organization. A legislative approach that incentivizes a risk-based standard of care would drive stronger security practices, while continuing to support innovation.

Conclusion

It would be difficult to overstate the cyber risk that we face today. From our cities to the electric grid and transportation relying on connected devices and networks, the risk is more than a technical one. It is

political. It is social. It is economic. It is physical. Cybersecurity risk is an existential threat to our democracy.

There are steps that we can take to improve our cybersecurity posture in advance of a national crisis, including the creation of an Office of the National Cyber Director within the White House.

I would like to thank Chairwoman Maloney, Ranking Member Comer and all the members of the Committee for their attention to this important issue. I would also like to thank members of the Cyberspace Solarium Commission and Representatives Langevin and Gallagher for their leadership. I appreciate the opportunity to testify today and look forward to working with you and your colleagues as cybersecurity topics remain at the forefront of so many policy decisions we face.