ITI Promoting Innovation Worldwide

Written Testimony of

Rob Strayer
Executive Vice President of Policy
Information Technology Industry Council (ITI)

Before the
U.S. House Committee on Homeland Security
Subcommittee on Cyber, Infrastructure Protection & Innovation

United States House of Representatives

Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks

June 22, 2022

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Written Testimony of

Rob Strayer
Executive Vice President of Policy
Information Technology Industry Council (ITI)

Before the

Committee on Homeland Security
Subcommittee on Cyber, Infrastructure Protection & Innovation
United States House of Representatives

Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks

June 22, 2022

Chairwoman Clarke, Ranking Member Garbarino, and Distinguished Members of the Subcommittee, thank you for the opportunity to testify today. My name is Rob Strayer and I'm the Executive Vice President of Policy at the Information Technology Industry Council (ITI).[1] I lead ITI's global policy team, driving ITI's strategy and advocacy efforts to shape technology policy around the globe to enable secure innovation, competition, and economic growth, while supporting governments efforts to achieve their public policy objectives. ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. We represent leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and other organizations using data and technology to evolve their businesses.[2]

Prior to joining ITI, I served as the Deputy Assistant Secretary for Cyber and International Communications and Information Policy at the U.S. State Department. In that role, I led dozens of bilateral and multilateral dialogues with foreign governments on digital economy regulatory and cybersecurity issues. In 2018, I was the U.S. ambassador for the U.S. delegation to the International Telecommunication Union (ITU) Plenipotentiary Conference in Dubai, United Arab Emirates. Before joining the State Department, I was the general counsel for the U.S. Senate Foreign Relations Committee.

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

[2] See ITI membership list at: https://www.itic.org/about/membership/iti-members

Companies in the United States have long spearheaded the development of the most innovative and cutting-edge technologies. These technologies have produced tremendous growth for the United States and transformed the global economy. In 2020, the digital economy in the United States accounted for $2.14 trillion of value added (translating to 10.2% of U.S. GDP), $1 trillion of compensation, and 7.8 million jobs.

U.S. national security depends on continued U.S. technological leadership. This leadership drives innovation, job creation, and economic growth domestically and makes the U.S. more resilient and secure as we continue to set the pace for innovation. Remaining at the cutting edge of developing and commercializing technologies will ensure they are available to the private sector and the government for a wide range of applications, including homeland security.

Today, other nations and their companies are competing to find the next major technological advancement. In some cases, competitor nations and their national-champion companies go to great lengths to innovate and achieve a market advantage.

Two overarching principles should guide U.S. policy on emerging technology. The United States should adopt policies that enhance the ability of the private sector and academic institutions to increase the pace of innovation to out-compete rivals and develop globally leading emerging technology. With this global competition in mind, the United States should design security policies related to emerging technology that are **risk-based and proportionate**. Unduly burdensome and restrictive security requirements will undermine the ability to innovate and compete in global markets, as well as keep pace with the evolution of technological capabilities.

In general, the private sector has a strong market-based incentive to protect technology from compromise and misuse, as that is the expectation of business users and consumers. The adoption of dynamic cybersecurity risk management practices and establishment of voluntary, industry-led, consensus-based cybersecurity standards have yielded tremendous capability enhancements for the protection of all digital technologies, including emerging technology, and improved their resilience. While these principles could be applied to any foundational and emerging technology, below are the technology sector's views about how they should be applied to securing 5G, Artificial Intelligence (AI), and the Internet of Things (IOT).

Securing 5G

Security is fundamental to successfully deploying and using 5G. The future will be filled with exciting new applications and services that will run on top of 5G, but an increasingly connected world will also increase security risks, ranging from an accelerating and evolving cybersecurity threat landscape to concerns regarding sophisticated adversaries exploiting ICT supply chain vulnerabilities. Given this increased interconnectedness, emerging threats can pose a danger to the 5G ecosystem more widely -- for example, critical infrastructure and services like energy, manufacturing, and utilities -- if not adequately planned for and managed. The good news is that 5G networks and standards are being designed with security in mind from the outset, and 5G networks will include several security enhancements that will enable business and government

enterprises to confidently deploy new applications and IoT services to harness the full value of 5G.

While investments in 5G infrastructure and the accompanying digital transformation are well under way, consumers, businesses, and governments should prioritize security during the implementation and seek to leverage the security enhancements available for the first time in 5G. Industry around the world is actively working to secure mobile networks, including 5G. This includes investing time and resources into developing cybersecurity technologies and services to secure 5G networks and the applications and services running over them, helping to educate business leaders on the importance of cybersecurity investments, sharing operational threat information on threats traversing mobile networks so that relevant parties can take action, and participating in the development of relevant global 5G security standards and reference documents. Industry and government are also collaborating via public-private partnerships to ensure that we arrive at the desired policy outcome of more secure 5G networks, including operational partnerships to share information on threats to 5G, and partnerships to further supply chain risk management best practices and solutions. No one organization in the private or public sectors can see all supply chain or cyber security threats, so it is imperative that both sides work together to fully understand and assess the full range of potential security threats in order to develop and implement appropriate mitigations.

ITI and its member companies have spent significant time considering how best to efficiently deploy the next generation of wireless technology while simultaneously ensuring that such technology is secure and have developed a set of 5G Policy Principles intended to help guide policymakers as they consider how to approach this set of issues.[3] Below, we offer specific suggestions based upon that work.

5G-related security policies should be risk-based. Any policy intended to address challenges related to 5G security, should be risk-based, evidence-based, adaptable, and fit-for-purpose – i.e., such policies should address concrete, identifiable security risks. Governments should undertake or promote risk assessments to gain fuller visibility into the threat landscape, including the supply chain ecosystem and which risks can be mitigated and which ones cannot. Policies should promote the procurement of equipment from trusted suppliers that adhere to industry-driven, consensus-based international standards, consider geopolitical implications of manufacturing locations, localization and sourcing requirements, and encourage diverse supply chains to help manage risk. In some cases, the level of risk may justify government spending to support the replacement of untrustworthy ICT infrastructure. In formulating any policy related to 5G security, we recommend that policymakers leverage the Prague 5G Security Proposals,[4] which were developed at a conference where more than 30 countries participated, to understand relevant risk assessment criteria and to further effective cybersecurity risk management.

Additionally, 5G security policies should seek to manage the full range of security risks to mobile network infrastructures, applications, and services, including devices and data. For

[3] ITI 5G Policy Principles and 5G Essentials for Global Policy Makers, https://www.itic.org/policy/ITI_5G_Full_Report.pdf.

[4] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

instance, automated and distributed threats such as botnets will likely be a more pervasive issue in the context of 5G network deployment, and emerging technology may provide innovative cybersecurity solutions to adequately mitigate such threats, including through the use of AI and other automated tools.

Finally, government and industry must share responsibility and collaborate. Government and industry share the goals of mitigating cybersecurity threats to network infrastructures, preventing cyberattacks, and reducing the impact of cybercrime. As in all areas of cybersecurity, achieving these goals is a collective effort. Public-private partnerships should be leveraged to ensure that both industry and government arrive at the desired policy outcome of more secure 5G networks. Industry has developed a multitude of security best practices that can be referenced or built upon, and any new best practices should be developed in conjunction with industry. Operational partnerships are key as well, particularly regarding sharing information on threats to 5G. No one organization in the private or public sectors can see all cyberthreats, and industry often does not have access to classified or sensitive government cyberthreat intelligence. It is imperative that both sides work together to fully understand and assess potential threats.

Securing Artificial Intelligence

As innovation in Artificial Intelligence (AI) continues and the technology itself evolves, it is important for policymakers to consider how to harness the benefits of AI while simultaneously addressing societal or other challenges that may emerge. For example, malicious actors can use adversarial AI to cause machine learning models to misinterpret inputs into the system and behave in a way that is favorable to the attacker. To produce the unexpected behavior, attackers create "adversarial examples" that often resemble normal inputs, but instead are meticulously optimized to break the model's performance. Malicious attackers may also attempt to influence a system's outputs by polluting the training data on which a model or system is trained – also known as data poisoning. Such pollution of the data can result in faulty outputs or outcomes. As such, it is important that businesses and the U.S. government also invest in cybersecurity directed at countering adversarial AI. At the same time, adversarial AI represents an incremental threat compared to traditional cyberattacks, so it is important that governments do not place an outsized focus on countering it.

Furthermore, data poisoning – or when a malicious actor pollutes a system's training data -- can be viewed as a more pronounced form of data drift, which happens when AI systems are trained on bad data. Data drift is not due to a malicious actor attempting to manipulate the system, but can be due to a variety of factors, like changing the input data, a change in environment, errors in data collection, and others.

In order to mitigate risks associated with the use of AI systems, we encourage public and private sector stakeholders to incorporate AI systems into threat modeling and security risk management. This should include encouraging organizations to ensure that AI applications and related systems are in scope for organizational security program monitoring and testing and that the risk management implications of AI systems as a potential attack surface are considered. We are particularly supportive of ongoing the collaborative work being undertaken by the U.S. National Institute of Standards and Technology (NIST) to develop a voluntary AI Risk

Management Framework, which organizations will be able to leverage to mitigate security and other risks that may be associated with particular uses of the technology.

We also encourage policymakers to support the use of strong, globally-accepted and deployed cryptography and other security standards that enable trust and interoperability in AI systems. The tech sector incorporates strong security features into our products and services to advance trust, including AI systems. Policymakers should promote policies that support using published algorithms as the default cryptography approach as they have the greatest trust among global stakeholders, and limit access to encryption keys.

Although there are new risks that may be introduced with AI technology, we also want to emphasize that AI and machine learning can be leveraged to improve cybersecurity. Indeed, defensive cybersecurity technology should embrace machine learning and AI as part of the ongoing battle between attackers and defenders. The threat landscape constantly evolves, with cyberattacks that are complex, automated and constantly changing. Attackers continually improve their sophisticated and highly automated methods, moving throughout networks to evade detection. The cybersecurity industry is innovating in response: making breakthroughs in machine learning and AI to detect and block the most sophisticated malware, network intrusions, phishing attempts, and many more threats. Other examples include using AI to identify unknown IoT devices as well as suspicious device behavior, to uncover suspicious Domain Name System (DNS) activity, and to stop incoming threats.

Because of this, we encourage the U.S. government to develop policies that support the use of AI for cybersecurity purposes. Cybersecurity tools and capabilities should incorporate AI to keep pace with the evolving threat landscape, including attackers who are constantly improving their highly automated methods to penetrate organizations and evade detection. Defensive cybersecurity technology can use machine learning and AI to more effectively address today's automated, complex, and constantly evolving cyberattacks. When combined with cloud, AI can help to scale cyber efforts through smart automation and continuous learning that drives self-healing systems. To support and enable the use of AI for cybersecurity purposes, policymakers must carefully shape (or reaffirm) any policies related to privacy to affirmatively allow the use of personal information, such as IP addresses, to identify malicious activity.

Securing the Internet of Things

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. To reap the benefits of connected devices and to minimize the potentially significant risks posed by malicious actors seeking to exploit them, these devices need to be secure and resilient. Unfortunately, as the number of connected people, businesses, and devices grows, so does the potential for malicious attacks. Today, the destructive potential of cyber attacks, can increase exponentially when such attacks leverage massive quantities of connected IoT devices. As risks to the global digital ecosystem, including IoT, continue to grow, so does our need to restore trust and confidence in connected devices and the IoT and larger ecosystems to advance not only security but economic growth and innovation. To help policymakers and stakeholders better ensure the security of the IoT ecosystem, ITI developed a set of IoT Security Policy Principles, which we encourage

Congress and policymakers more broadly to use as a guide.[5] Below are several suggestions relevant to the issues being discussed today.

It is imperative that all stakeholders collaborate to take a thoughtful, holistic approach to securing the various parts of networks and complex ecosystems that make up the IoT, and not only focus on the device. An inclusive process must focus on end-to-end security, including security-by-design techniques and secure development lifecycles. As global concerns regarding IoT security — including concerns about sophisticated automated and distributed threats such as botnets that exploit insecure IoT devices — have continued to grow, policymakers have disproportionately focused on IoT product security without addressing the broader issues related to securing the IoT ecosystem. Many policy proposals have only targeted individual components of the ecosystem, rather than focusing on ecosystem security as a whole. For instance, some policies propose that internet service providers (ISPs) should simply shut down all botnets, or that manufacturers of billions of devices should make them universally secure. Such overly simplistic solutions fail to address the fundamental need to secure the ecosystem. Regardless of which security measures are taken at the device, network, or software level, if these components of the ecosystem are addressed in isolation, efforts will ultimately fail. Taking a holistic view is therefore a superior approach.

While ecosystem-wide security is important, industry-driven consensus around baselines and standards is essential for IoT devices. Developing a common set of best practices and secure capabilities that are broadly applicable across all IoT devices with varying levels of complexity and are driven by market demand will help to improve all new IoT devices' cybersecurity. Building broad industry consensus around an IoT security baseline will also facilitate more effective government-industry collaboration on this issue, helping to drive interoperable IoT security policies worldwide. In addition, establishing a core baseline will promote globally interoperable standards and advance innovation worldwide to improve IoT security. Governments should continue to encourage open and international security standards to maintain the long-term viability of the IoT and to foster solutions that are interoperable and reusable across a variety of use case deployments, vendors, sectors, and geographies

To fully realize the benefits offered by IoT, governments should promote policies that help break down barriers to connecting devices and correlating data while protecting privacy and security. Government bodies should examine the technologies underlying the IoT and assess where current authority, oversight, and regulation already exist and avoid siloed, sector-specific regulatory approaches. Policymakers and regulators should reinforce private-public cooperation on IoT issues to help identify cybersecurity solutions and better coordinate the many IoT security-related policy efforts currently in progress across the U.S. government and globally. In the United States, the National Institute of Science and Technology's (NIST) ongoing commitment to industry outreach in developing an IoT security framework provides an excellent example of such cooperation.

The U.S. government should promote global harmonization of any mandatory IoT requirements published by individual states, sector-specific agencies, or countries in order to prevent

[5] ITI IOT Security Policy Principles, https://www.itic.org/policy/ITIIoTSecurityPolicyPrinciples.pdf.

unhelpfully fragment the global IoT security landscape. Such fragmentation would ultimately limit the growth of a secure IoT by reducing the efficiencies of scale in development, manufacturing, support, training, assessment, and identification of secure IoT products. It will also make it more difficult for industry to comply with such divergent requirements, hampering global business and trade. The long-term security and resilience of the internet and communications ecosystem requires a global and holistic approach involving the adoption of baseline security practices by stakeholders in many different countries, industries, and segments of the ecosystem.

To combat an increasingly divergent policy environment, policymakers should prioritize global harmonization and regulatory cooperation to support a voluntary, industry-driven consensus around core baseline capabilities for IoT security that are grounded in global standards. Finally, stakeholders and consumers must understand that connecting IoT devices or equipment to the Internet is a long-term commitment, not a one-time design and manufacturing cost. IoT security demands dynamic, flexible market-driven solutions that are nimble and adaptable to evolving cyber threats, including those specific to the proliferation of IoT devices, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.

Cybersecurity

As this Subcommittee has recognized, cybersecurity is one particular type of security issue impacting all digital technologies, and it is certainly vital for the security of emerging technologies. For ITI members, facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally. Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity.

As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy, and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

The NIST Cyber Security Framework (CSF) has provided immense value to users, within critical infrastructure, and beyond. ITI has been engaged in NIST's CSF efforts for the better part of a decade, working to provide constructive input and shape the Framework to make it as useful as possible. The CSF has been a highly useful tool for cybersecurity risk management, offering a baseline approach for organizations seeking to institute such a process. Indeed, to the extent the goal of the Framework was to provide a common language for organizations, it has certainly achieved that, proving useful for communicating about cyber risk both within and between organizations. This is one of the major benefits of using the Framework. Mapping to consensus standards and control sets helps to provide a common, international understanding of the intention of the categories and subcategories, and the Implementation Tiers provide a reference

point for organizations to evolve their ability to cybersecurity programs. The CSF has also provided for a risk-based, flexible approach, allowing organizations to develop a cyber risk management program that is appropriate for their level of risk and desired outcomes.

Even though the original target audience for the CSF was critical infrastructure owners and operators, it is now widely adopted, and companies and institutions developing and commercializing emerging technologies can certainly employ the CSF for their cybersecurity – some of which may be part of critical infrastructure supply chains. Small- and medium-sized businesses and institutions, however, may face resource constraints or have a lack of personnel with the skills and/or knowledge needed to digest, understand, and apply the Framework. This is an area worth further inquiry.

Recommendations

1) **Congress should finalize negotiations on the Bipartisan Innovation Act.** Both the House and Senate in their respective bills have embraced bold new investments in foundational technologies that are critical for American competitiveness, including $52 billion to incentivize American production and design of semiconductors and $1.5 billion for the Public Wireless Supply Chain Innovation Fund to support the deployment of 5G and next-generation network hardware and software utilizing radio access network open architecture. Both chambers' bills also reinvigorate federal research & development in key technology areas, including cybersecurity specifically. This legislation is urgently needed to strengthen our national innovation ecosystem and translate new research into commercialized technology, which when coupled with the bills' investments in manufacturing will result in high-tech jobs and new firms in communities across the country.

2) **Congress should use its oversight authorities to help coordinate and streamline federal policymaking efforts to address cybersecurity and emerging technologies.** ITI supported the recently passed, Cyber Incident Reporting legislation, and appreciated the collaborative approach this Committee took to developing the bill and its regulations. Since the beginning of the current Congress on January 3, 2021, there has been a plethora of bills on cybersecurity and emerging technologies. We encourage this Subcommittee and other relevant committees to focus on the driving power of Congressional oversight to help federal agencies successfully and completely implement these new requirements and various lines of effort.

3) **Congress should encourage CISA to leverage the IT Sector Coordinating Council (IT SCC) to better understand the scope of threats related to emerging technologies.** The Information Technology Sector Coordinating Council (IT SCC) serves as the principal entity for coordinating with CISA and the government generally on a wide range of critical infrastructure protection and cybersecurity activities and issues. The IT SCC brings together companies, associations, and other key IT sector participants, to work collaboratively with the Department of Homeland Security and CISA, as well as

other government agencies and partners. Through this collaboration, the IT SCC works to facilitate a secure, resilient, and protected global information infrastructure. Of note, the IT SCC has launched an Emerging Technologies Working Group, aimed at helping CISA better understand cybersecurity threats and vulnerabilities related to emerging technologies, including those that may stem from AI, 5G, and quantum information sciences. The IT SCC recently published a set of AI Policy Principles, based upon ITI's *Global AI Policy Recommendations,* which offer guidance to policymakers around how to best leverage this emerging technology to counter threats. Congress should encourage CISA to continue to leverage the IT SCC, and the Emerging Technologies working group, to understand how it should appropriately scope its work to address potential threats to critical infrastructure moving forward.

4) **Beyond CISA and the IT SCC, Congress should encourage robust and continuous cooperation between the U.S. government and industry.** Policymakers and companies each have important and distinct roles to play in addressing technology-related national security risks. The U.S. government has information that companies do not have about national security threats. Companies have information that governments do not have about their network operations and how they detect, manage, and defend against risks to data, systems, networks, and supply chains. Both policymakers and industry should communicate regularly and robustly about relevant risks (consistent with limitations relating to classified information and business confidentiality), including through opportunities for industry input in regulatory rulemaking processes, public-private task forces and other collaborative mechanisms, and informal relationships between policymakers and companies.

5) **Avoid overbroad regulatory approaches, which may not serve to mitigate security risk, and which could instead hamper innovation.** As the U.S. government is considering how to best harness emerging technologies while simultaneously mitigating security risks, we urge it to carefully evaluate the costs and benefits of any regulatory approach before adopting it. Indeed, many of these technologies are nascent, and overbroad, ill-scoped approaches may serve to hinder innovation without demonstrably improving cybersecurity. As such, any approach should be appropriately targeted, proportionate, and tied to discrete security (or other) risks. We elaborate on this suggestion in our *Principles for Improved Policymaking and Enhanced Cooperation on National Security, Technology, and Trade.*[6]

6) **Congress should continue to fund and support NIST work on Artificial Intelligence, IOT security, 5G security, post-quantum encryption, and other emerging technologies.** As referenced in our testimony above, NIST is undertaking work in many areas that will be vital to harnessing emerging technologies while also ensuring that risks are appropriately managed. Indeed, NIST is developing a framework to better manage risks to individuals, organizations and society that may be posed by specific uses of AI. It

[6] ITI's Principles for Improved Policymaking and Enhanced Cooperation on National Security, Technology, and Trade, available here: https://www.itic.org/policy/us-national-security-policymaking

is also undertaking work to cultivate trust in AI technologies, including by conducting fundamental and applied AI research, as well as establishing benchmarks and developing metrics to help evaluate AI technologies. NIST is also undertaking helpful work on post-quantum cryptography and is seeking to standardize quantum-resistant public-key cryptographic algorithms, which will be important if large-scale quantum computers are built as they can break traditional public-key cryptography systems currently in use. We therefore encourage continued support of these NIST efforts. Aside from NIST, private-sector-led standardization activities, such as in the International Standardization Organization – International Electrotechnical Commission Joint Technical Committee-1, are also focused on AI risk management and interoperability of quantum-resistant cryptography.

7) **Continue to implement the recommendations stemming from the National Security Commission on Artificial Intelligence (NSCAI).** The NSCAI report offers a plethora of recommendations for the U.S. government to advance trustworthy AI in different domains. Particularly useful in this context are those recommendations pertaining to countering adversarial AI, as well as those related to establishing confidence in AI systems. We encourage the U.S. government to continue to make progress on implementing these recommendations in order to enable innovation and protect against malicious uses of the technology.

Conclusion

Future United States economic and national security depends on continued leadership in emerging technologies. It is possible for the U.S. government to ensure that those technologies are secure, while continuing to promote leading-edge innovation. A track record exists involving AI, 5G, and IOT security of using risk-based frameworks to address potential vulnerabilities, with significant involvement of NIST in those efforts. The active collaboration among the government, especially NIST and CISA, the private sector, and other stakeholders is essential for the evolution of frameworks that will protect and enhance emerging technologies. As new digital technologies emerge, malicious actors will seek to compromise them, so new frameworks will need to be developed to address those challenges.