Testimony of Clete D. Johnson

Senior Fellow,
Center for Strategic and International Studies

Partner,
Wilkinson Barker Knauer, LLP

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Communications and Technology

Hearing on

Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era

January 11, 2024

Chairman Latta, Ranking Member Matsui, Chair McMorris Rodgers, Ranking Member Pallone, Members of the Committee, thank you for the opportunity to join you to discuss the defense of our nation's communications capabilities against sophisticated cyber threats.

This Committee's bipartisan approach to these issues is a welcome and compelling continuation of decades of cybersecurity policymaking across multiple Congresses and Presidential Administrations. Your leadership has never been more urgent, as our most dangerous adversaries are growing more violent, destructive, and disruptive in both the physical world and in cyberspace.

Russia's invasion of Ukraine in 2022 – with the support of China, Iran, and North Korea – shattered any illusion that the "post-Cold War" peace among great powers still exists.

Likewise, Hamas's October 7 massacre of innocent civilians – with the acquiescence or even affirmative support of China, Russia, and Iran – shattered any illusion that our adversaries had moved beyond murderous terror.

Make no mistake, there is a nascent military alliance among these aggressive autocracies and the criminal organizations that serve as their proxies. In addition to their physical aggression, their cyber armies and criminal syndicates possess extremely sophisticated offensive cyber attack capabilities, ranging from theft and espionage to disruption and destruction to misinformation operations.

The stakes could not be higher for the United States and our free market democratic allies, because the battlefields of today's and tomorrow's conflicts are in cyberspace and the information arena as much as in the physical world.

As we progress further into the 5G era of near-ubiquitous wireless mobile connectivity, the physical world will converge with cyberspace in ways that we have never imagined. This means great advances arising from connectivity – but it also means bad actors can attack American citizens and critical infrastructure, even if they and their keyboards are physically located on the other side of the world.

We have to ensure that American and allied cybersecurity capabilities are stronger, faster, and more capable than those of our autocratic and criminal adversaries. The private companies that make up the communications sector – Internet Service Providers, other infrastructure providers, and suppliers and partners – have long been and will always be indispensable to these capabilities.

The Committee should therefore orient its legislative and oversight activities around maximizing the capabilities of this U.S. national security asset and promoting the uniquely American approach to cybersecurity policy, deriving from several core principles:

1. Implementing dynamic and flexible cybersecurity practices that innovate and adapt even faster than cyber threats;

2. Harnessing powerful market drivers for security, reliability, and resiliency that align directly with government interests; and

3. Building effective and accountable partnerships based on deep and ongoing collaboration between government and industry.

The roots of this uniquely American legal, policy, and operational framework go back to the height of the nuclear era six decades ago, when the Cuban Missile Crisis prompted the government to partner with industry to ensure that telecommunications functions would survive a nuclear attack. This partnership from the early 1960s served as the foundational model for all subsequent critical infrastructure security activities after 9/11, the creation of the Department of Homeland Security, and the advent of the cybersecurity era.

For instance, the Communications Sector Information Sharing and Analysis Center, or Comm-ISAC, is the organization where – like other critical infrastructure sectors' ISACs – companies actively share information about cyber threats, operations, response, and resiliency.

However, *unlike* every other sector's ISAC, the Comm-ISAC is physically co-located with the U.S. government, housed in the National Coordinating Center for Communications at CISA. Since decades before DHS even existed, communications network operators have been working literally side-by-side with government officials through hurricane seasons, wildfires, cyber-attack campaigns, and routine day-to-day challenges to maintain communications security and resiliency through all hazards.

The Comm-ISAC is just one example of the highly capable strategic and operational partnership between government and the communications sector, which is so deeply ingrained in our nation's network defense that it often goes unnoticed.

One good example is early March 2020, when Covid-19 shifted almost our entire society to a remote school and work environment overnight. At the time, videoconference capabilities like Zoom were niche services that were not ready for secure and widespread use by hundreds of millions of Americans. But ISPs ensured that their networks met the security and high bandwidth demands of these videoconferencing apps to enable us to communicate securely and reliably. ISPs also worked furiously behind the scenes with the government and other industry partners to secure America's networks during this massive shift in how people worked and learned, outperforming European counterparts in allowing our society to function online.[1]

This unique American framework is the right approach because dynamic, proactive, collaborative accountability for security prompts an ever-improving "race to the top" – as distinct from traditional prescriptive checklist compliance regulation, which leads to complacency at the lowest common denominator of security. I want to highlight four areas in which this Committee can continue to advance these principles.

[1] *See* NSTAC Report to the President on Communications Resiliency, October 6, 2020, *available at* https://www.cisa.gov/sites/default/files/publications/NSTAC%20Letter%20to%20the%20President%20on%20Communications%20Resiliency%20.pdf.

First, IoT security and the Cyber Trust Mark. This new program can leverage extraordinarily powerful global market drivers to ensure security throughout the product development and operation of consumer IoT devices. The criteria for the Cyber Trust Mark have been developed – and will be regularly updated – through rigorous NIST processes involving hundreds of engineers and other security experts, so devices earning the Mark will gain significant legal protections and security credibility. The resulting accountability will drive adoption, and I believe that the Mark will dramatically advance the security of IoT in the United States and worldwide – and very quickly, at the speed of the market.

To maximize the dynamism and scale of the global IoT market and the potential global reach of this policy initiative, it is crucial that the U.S. government maintain the Mark as an opt-in program and work with industry partners to promote adoption. This approach will bring successive advances in security, more broadly and more quickly, than a regulatory mandate.

Second, internet routing security. Immediately following Russia's invasion of Ukraine, the FCC initiated a proceeding to address vulnerabilities in the Border Gateway Protocol (BGP), the technical standard that serves as the internet's traffic routing function to enable internet traffic to arrive at its intended destination. Bad actors exploit BGP vulnerabilities to misroute or "hijack" internet traffic for nefarious purposes.

The various stakeholders in the internet routing ecosystem are diverse, complex and global, including entities such as cloud providers and enterprise network operators that are outside the reach of the FCC or other U.S. government agencies. Routing security is not conducive to one-agency oversight, so last year leading ISPs proposed that the U.S. government should undertake a broader collaborative approach to ensuring accountability in routing security. This process, underway now and convened by the Office of the National Cyber Director and the FCC, includes multiple federal agencies such as NTIA, NIST, CISA, and the Dept. of Justice, along with a wide variety of internet stakeholders. It is a "whole of government" and "whole of the internet" approach to security that has shown significant positive impact in its early months.[2]

As with the Cyber Trust Mark above, this collaborative effort on routing security represents an especially effective approach to security. I believe this approach is more dynamic and effective than a prescriptive compliance approach, which I fear would lead to companies replacing proactive solutions-oriented engineers with skittish lawyers hedging against regulatory risk.

Third, cybersecurity performance and risk management. In 2013, when President Obama directed NIST to develop a framework of cybersecurity risk management, communications sector companies led industry's engagement. In 2014, when NIST published Version 1.0 of the Cybersecurity Framework, the sector responded with the deepest analysis and recommendations for Framework implementation in any sector, working with NIST and DHS to develop recommendations through the FCC's Communications Security, Reliability, and

[2] *See* Internet Engineering Task Force, "RPKI's 2023 Year in Review - growth, governments, and innovation," *available at* https://mailarchive.ietf.org/arch/msg/sidrops/BKf57q5YIhxM30Yq8tvoOfw6Jyc/; and Communications Sector Coordinating Council, "ISP Internet Routing Security Practices and Partnerships," Communications Sector Coordinating Council, *available at* https://www.comms-scc.org/2024/01/02/isp-internet-routing-security-practices-and-partnerships/.

Interoperability Council (CSRIC). These CSRIC recommendations from 2015 provided a foundation for real-world implementation of the Framework that is valuable today in a variety of settings.[3] Further, CSRIC's recommendations for using the Framework for collaborative cybersecurity engagements with the FCC, CISA, and other important U.S. government agencies remain a visionary model for accountability and dynamic, adaptable risk management. In many ways, the collaborative approach to routing security discussed above is an example of how those landmark CSRIC recommendations might work more broadly.

The communications sector has continued to work closely with NIST to update the Cybersecurity Framework, and with Version 2.0 expected to be released next month, the Committee could explore new ways to harness network operators' leadership on these issues.

Fourth, supply chain security and trusted suppliers. From the Secure Networks Act and the Secure Equipment Act to the CHIPS and Science Act and multiple initiatives to free up spectrum for commercial uses, this Committee's work is crucial to establishing a secure ICT supply chain from trusted vendors. The Committee should continue to ensure that the Administration and the FCC identify untrusted suppliers and help eliminate them from our market, with clear government processes that are as transparent as possible and provide appropriate transition periods for affected U.S. industries. Of course, this must also include full funding of the "rip and replace" program to reimburse smaller networks for replacing untrusted equipment designated on the FCC's Covered List.

The Committee should also promote innovation among trusted suppliers. First, it should ensure that grants from NTIA's Wireless Innovation Fund are issued in a timely fashion – including the game-changing large grants that will meet Congress's intent to accelerate the trusted supplier market for open and interoperable Radio Access Network deployments. Second, as we discussed in March, it is imperative that Congress restore the FCC's spectrum auction authority and replenish the U.S. spectrum pipeline for commercial 5G. In short, if the United States lags China in spectrum availability for 5G, China's "national champion" companies – not trusted U.S. and allied-based companies – will supply the 5G services of the future. A shortage of commercial spectrum means a shortage of trusted suppliers.

* * *

In each of these areas, we have the potential to advance a policy path toward dynamic, proactive, collaborative accountability for ever-improving security. The stakes are high for the United States, and for free market democracy more broadly. I commend the Committee's focus on these issues, and I look forward to your questions.

[3] *See, e.g.,* the cybersecurity and supply chain security attestations required of sub-grantees under the Broadband Equity, Access, and Deployment program administered by NTIA, and the FCC's recent proposed updates to the E-RATE funding for cybersecurity for schools and libraries.