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

A Safe Wireless Future:
Securing our Networks and Supply Chains

June 30, 2021

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers, Members of the Committee, thank you for the opportunity to join you – in person! – today to share my views on the best path toward a future of secure and reliable wireless communications.

Having been in the policy trenches on these issues through many different Administrations and Congresses, I have special gratitude for the Committee's bipartisan approach to cybersecurity, supply chain security, and the bills that are the subject of this hearing. Thank you.

In my work in the Senate, at the Federal Communications Commission (FCC), in the Commerce Department, within the interagency processes of the National Security Council, and now in private practice and in the think tank arena, I have been personally involved in just about every major cybersecurity policy development since the end of the Bush Administration. Since cybersecurity became a prominent federal policy issue in the late 2000s – through the Administrations of Presidents Bush, Obama, Trump, and now Biden – the clear trajectory of cybersecurity policy is steady progress toward industry leadership and partnership with a well-coordinated federal interagency.

Successive Congresses and Administrations have put the foundational cornerstones of this policy approach in place:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Cybersecurity Enhancement Act that codified NIST's private sector engagement model;

- The Cybersecurity Information Sharing Act that provided new clarity and safeguards for operational sharing of cyber threat indicators;

- The Secure and Trusted Communications Networks Act and related appropriations, through which the FCC is reimbursing the replacement of untrusted equipment in subsidized networks;

- The Secure 5G and Beyond Act, which prompted the development of the National Strategy to Secure 5G;

- The provisions of last year's National Defense Authorization Act, which created the Public Wireless Innovation Fund, to be administered by the National Telecommunications and Information Administration (NTIA) to promote breakthrough advances in promising areas such as Open Radio Access Network (RAN) architecture;

- The Commerce Department's work with industry to secure the hardware and software supply chain; and

- The work of the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) on 5G security, and the FCC's related supply chain security proposals.

All of these are precedent-setting initiatives. They all have the promise of further advancing industry leadership and government-industry partnership.

Building on this foundation, and particularly following recent attacks on SolarWinds and Colonial Pipeline, we are now transitioning to an altogether new phase of cybersecurity and supply chain security policy. We are no longer establishing the foundations of this policy; now, we must fully implement, operationalize, and build on the policies and partnerships we have developed over the past fifteen years.

Perhaps the central "next step" question pertains to the crucial relationship between the Information and Communications Technology (ICT) industry and the federal government on cybersecurity and communications reliability. Will the future be prescriptive regulation or collaborative partnership?

I urge the Committee to consider that collaborative partnership across the ICT industry will produce superior outcomes against the common threats we face. Government and industry must be on the same team to defend against the sophisticated adversaries that target all of us, and I know from my time as the FCC's Chief Counsel for Cybersecurity that regulatory agencies can be extremely influential in enabling – or alternatively, in blocking – this necessary teamwork.

One of the lessons learned from the COVID-19 pandemic is that the network operators, trusted suppliers, and other stakeholders of the ICT industry collectively constitute our greatest national asset towards the goal of secure, reliable connectivity.

The ICT industry that serves the United States has the most sophisticated and well-resourced security operations in the world. As demonstrated during the unprecedented connectivity demands of the pandemic – when every single day was Mother's Day and New Year's Eve with regard to telecommunications traffic – the ICT industry's core interest in maintaining secure, reliable connectivity is an indispensable imperative.

This industry imperative not only fully aligns in every way with the U.S. government's interest in network security – it is in fact the foundation of defending that government interest.

That is why throughout the pandemic, particularly in those harrowing early months when our world changed completely, the FCC, NTIA, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and other government agencies turned to network operators and the broader ICT industry to keep our society connected and operating.

This collaborative effort was not a regulatory mandate or government otherwise telling the ICT stakeholders what they had to do. Instead, government stakeholders were asking ICT stakeholders how the government could help them keep our society connected during the crisis. It was a partnership that was as urgent as the life-saving and life-sustaining activities that depended on it. And it worked.

This is the model to follow in the future, because U.S. network operators and their trusted suppliers are the U.S. government's most important partners in securing our nation's networks.

Unlike other critical infrastructure sectors, the ICT industry has been working in close partnership with the government to maintain secure, reliable connectivity for decades, going back to the height of the Cold War when – under the threat of nuclear weapons disrupting our communications capabilities – President Reagan established the predecessors of today's public-private National Coordinating Center for Communications, a joint government-industry operation hosted at DHS CISA, and the Communications and IT Sector Coordinating Councils.

In short, the ICT industry knows how to work with the government to ensure the security and reliability of the nation's networks. New challenges and opportunities, from IoT to 5G security to Open RAN to incident detection and response, call for deeper and more efficient partnerships to help network operators and their trusted suppliers help the country.

The ICT industry needs the government to advance existing partnerships – particularly with the Commerce Department (both NTIA and NIST), the FCC, and CISA. They need coordinated interagency processes that leverage industry's strengths. They need careful U.S. government attention to minimize duplication and turf battles, and to maximize coordination and impact.

When I was at the FCC in 2015, the communications sector provided a path to this goal via its groundbreaking CSRIC recommendation that the FCC partner with DHS to engage in partnership with network operators. It was a "new paradigm" of industry-led cooperation with government – perhaps an idea before its time, as the idea bogged down in FCC-DHS turf wars. However, particularly given our nation's experience maintaining secure, reliable connectivity throughout the pandemic, I am confident we have grown past those turf battles at this point.

Given the maturation of interagency processes that have developed since that time, particularly the increasingly clear authorities of the Department of Commerce and CISA, as well as the FCC's recognition that its most meaningful role is in supporting interagency processes rather than taking unilateral actions, the time is now ripe for the U.S. government to work with the ICT industry to take the next big steps in securing our nation's networks.

The bills you are now considering can help make that happen, so long as we continue close partnership between industry and government.

Thank you for your time, and I look forward to answering your questions.