Summary of Statement of Clete D. Johnson
Partner, Wilkinson Barker Knauer, LLP

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

Hearing on Telecommunications, Global Competitiveness, and National Security
May 16, 2018

Supply chain security issues are crucial for American technology leadership and the future of our economic and national security. My testimony today reflects lessons from my experience with these issues in multiple government and private sector positions, including as counsel for the Senate Select Committee on Intelligence, the FCC, the Dept. of Commerce, and private practice.

The supply chains for the global internet and communications technology ecosystem raise complex national security, strategic, economic, business, and technological concerns. The United States has played the leading role in advancing these tech developments, and we must address these security concerns in a way that further advances innovations and U.S. leadership.

The capability of bad actors to use these technologies – and to leverage supply chains – for intellectual property theft, cyber espionage, sabotage, and even warfare presents acute threats. There are well-funded, purposeful, sophisticated adversaries, spies, criminals and others who are working hard to find openings for their nefarious purposes. These threats and vulnerabilities manifest in different ways at all levels of the global supply chain, beginning with the Chinese and Russian companies that have been identified in recent government actions.

The public actions that Congress and the Administration have taken in recent months to address these concerns constitute a significant, and welcome, intensification of policy activity.

We need to do this right. These issues are highly complex, and solutions must take root in the global market. These challenges call for private sector leadership, in close, collaborative engagement with government partners through clear and effective processes.

Perhaps the most important of recent actions is the FCC proposal to prevent government funds from purchasing technology or services from companies that pose a national security threat to the U.S. communications infrastructure. This will advance the policy discourse on these difficult issues and can be a lever to move the whole government, and the market, in the right direction.

The market needs clear practical guidance that derives from coherent, well-informed processes that include input from experts throughout the government, as well as from the private stakeholders who know this complex market best. This should be led by DHS, and the confidentiality of sensitive private sector information should be protected.

The FCC's actions in the future should derive from, and further advance, processes that are built on principles of industry leadership and government-industry partnership in cybersecurity and supply-chain risk management.

Statement of Clete D. Johnson
Partner, Wilkinson Barker Knauer, LLP

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

Hearing on Telecommunications, Global Competitiveness, and National Security

May 16, 2018

Chairman Blackburn, Ranking Member Doyle, distinguished Members of the Subcommittee, thank you for holding this hearing. These issues are crucial for American technology leadership and the future of both our economic and national security, and I thank you for the opportunity to share my perspective on this critical bipartisan policy activity.

My testimony today reflects insights and lessons from my experience with supply chain security issues in multiple government and private sector positions since I was a logistics officer in the U.S. Army in the late 1990s. Over the past dozen years, these experiences have focused on promoting private sector leadership in cybersecurity and national security-based export controls in the global market for internet and communications technology, including through crafting legislation and conducting congressional oversight as counsel for the Senate Select Committee on Intelligence and working through regulatory proceedings and interagency National Security Council processes as counsel at the Federal Communications Commission and the Department of Commerce.

Now at Wilkinson Barker Knauer, I advise a number of clients on how to navigate this dynamic, complex and fast-changing global market and security environment – particularly through partnership with the federal government in advancing our collective security. I would

like to note that while the advice I provide clients also draws from these same experiences, the views I am expressing today are my own.

As this Committee well knows, the global supply chains for the diverse and innovative hardware, software and services that make up the world's internet and communications technology ecosystem raise a complex mix of national security, strategic, economic, business, and technological concerns. The United States and its innovative companies and people have played the leading roles in creating and advancing these world-changing tech developments, and addressing security concerns in a way that further advances these innovations is absolutely crucial to maintaining that U.S. leadership role and our society's prosperity. As we advance to a thoroughly connected 5G world, the capability of bad actors to use these technologies – and to leverage their supply chains – for intellectual property theft, cyber espionage, sabotage, and even warfare presents acute threats. There are well funded, purposeful, sophisticated nation state adversaries, spies, criminals and other malicious actors who are working hard to find openings for their nefarious purposes – and many such openings are there to be found.

These threats and vulnerabilities are very real, and they manifest in different ways at all levels of the global supply chain, ranging from the Chinese and Russian companies that have been identified in recent government actions all the way down to small startups in Silicon Valley or elsewhere that few have even heard of.

The public actions that Congress and the Administration have taken in recent months to address these concerns constitute a significant, and welcome, intensification of policy activity that has been percolating for a decade. We are at a policy inflection point on these issues, for good reason, and we need to do this right. These issues are highly complex, and solutions must take root in multiple arenas of a global market in which rapid business developments and the

practical realities of the supply chain can challenge or blur traditional boundaries and legal jurisdictions. These challenges call for private sector leadership – in close, collaborative engagement with government partners through clear and effective processes.

In recent months, more than a dozen new government actions on these issues have either taken place or are presently pending. Perhaps the most important of these activities is the FCC Notice of Proposed Rulemaking, championed by Chairman Pai and unanimously adopted last month. This proposal, which would prevent government funds from purchasing technology or services from companies that pose a national security threat to the U.S. communications infrastructure, will significantly advance the policy discourse on this difficult set of issues. Moreover, I believe this proposal can serve as a lever to move the whole government, and the market, in the right direction. Put simply, the market needs clear practical guidance that derives from coherent, well-informed processes that include input from experts throughout the government, as well as from the private stakeholders who know this complex market best.

Prohibitions or restrictions on the Chinese and Russian companies identified in last year's National Defense Authorization Act and cited in the FCC's Notice are perhaps the easy step. The more difficult questions over the longer term have to do with how these policies will be implemented and updated – or possibly expanded – in the months and years to come.

With this in mind, I would like to offer a few high-level thoughts on the FCC proposal. While the FCC has targeted its action to address supply chain security issues pertaining to networks supported by public funds, the implications of the FCC's precedent-setting proposal are potentially far-reaching. The identification of national security threats is fundamentally a function of the intelligence, law enforcement, defense and homeland security agencies of the Executive Branch, so as the FCC implements this rule, there is a need for thorough coordination

throughout the federal government in order to ensure that the supply chain security requirements or prohibitions for recipients of public funds are fully aligned with national security policy decisions by the Administration and/or Congress. Over the long term, the FCC should ensure that any further requirements or prohibitions derive directly from broader interagency policy processes or statutory requirements.

The Department of Homeland Security, as the Sector Specific Agency for the communications and information technology sectors, should coordinate these efforts, with input from the Departments of Commerce, State, Justice, Defense and others. The recently-begun Telecommunications Supply Chain Risk Assessments by DHS's Office of Cyber and Infrastructure Analysis could provide the basic foundation of such a process. To promote candor and collaborative partnership with industry leaders, sensitive private sector information provided by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits disclosure of protected information under the Freedom of Information Act or state transparency laws, and use in civil litigation or regulatory rulemaking or enforcement actions.

In short, the FCC's actions in the months and years ahead should derive from, and further advance, processes that are built on principles of industry leadership and government-industry partnership in cybersecurity and supply-chain risk management. I look forward to further fleshing out these thoughts in answers to your questions.