Prepared Statement of:
Robert L. Strayer
Deputy Assistant Secretary of State for
Cyber and International Communications and Information Policy

Hearing before the:
Senate Committee on Homeland Security and Governmental Affairs
on
Supply Chain Security, Global Competitiveness, and 5G

October 31, 2019

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you for today's opportunity to testify.

As the world becomes more interconnected, the security of our information communications technology (ICT), including the fifth generation of wireless technology (5G), is becoming increasingly important for our national security and economic prosperity, as well as the protection of human rights globally. The Department of State, under Secretary Pompeo's leadership, is in charge of the United States' international engagement on ICT security and our campaign to convince our allies and partners of the importance of 5G security.

Our mission is to engage our allies and partners to advance our shared vision for an open, interoperable, reliable, and secure digital environment, including for 5G.

5G will be transformative, as it will provide consumers and businesses with speeds up to 100 times faster than 4G, delay times of less than a millisecond, and networks capable of handling millions of new devices.

These advantages will empower a vast array of new critical services – from autonomous vehicles and transportation systems, to telemedicine, to automated manufacturing and traditional critical infrastructure, such as electricity distribution. The massive amounts of data transmitted by devices on 5G networks will also advance artificial intelligence.

With all these services relying on 5G networks, the stakes for safeguarding these vital networks exponentially increases.

As countries around the world upgrade their communications systems to 5G technology, we are urging them to adopt a risk-based security framework. To this end, the Department is executing a global campaign on 5G security that includes strategic bilateral and multilateral engagements to convince our allies and partners of the importance of adequately securing these networks.

An important element of this risk-based security approach is a careful evaluation of hardware and software equipment vendors and the supply chain. The evaluation criteria should include the extent to which vendors are subject to control by a foreign government with no meaningful checks and balances on its power to compel cooperation of these vendors with its intelligence and security agencies. While this should apply to vendors from all countries, our current concern is primarily with equipment vendors from the People's Republic of China (PRC) for multiple reasons.

Our assessment of the problem is that the PRC could compel Chinese equipment vendors to act against the interests of U.S. citizens and citizens of other countries around the world. If allowed to construct and service 5G networks, Chinese equipment vendors will have access to critical networks and understanding of network vulnerabilities. This information could be exploited, as outlined in China's National Intelligence Law, for the Chinese Communist Party to disrupt critical infrastructure, intercept sensitive transmissions, and acquire sensitive technology and intellectual property.

Specifically, the National Intelligence Law compels Chinese citizens and organizations to cooperate with Chinese intelligence and security services and to keep such cooperation secret.

In addition, the Chinese Communist Party does not have any meaningful checks or balances on its powers. As President Xi Jinping told security officials in January, China does not walk the "Western road" of constitutionalism, separation of powers, or judicial independence.

Chinese technology firms are already working with authoritarian regimes – often hand-in-hand with the Chinese government – to suppress freedom of expression and other human rights through arbitrary surveillance, censorship, and targeted restrictions on Internet access. If Chinese companies build the underlying 5G infrastructure, they will be in an even better position to facilitate these activities.

Moreover, the PRC and Chinese firms have a long history of intellectual property theft to benefit its interests. In December 2018, the United States announced that since at least 2014, Chinese cyber actors associated with the Chinese Ministry of State Security hacked multiple U.S. and global managed service and cloud providers. These cyber intrusions allowed the PRC to compromise the networks of the providers' clients, including global companies located in at least 12 countries. Countries must not allow 5G to be another vector for the PRC to steal their intellectual property.

Furthermore, Chinese companies, such as Huawei have benefited from subsidized financing and currency manipulation for their equipment sales. Countries should adopt the best practices in procurement, investment, and contracting, and require that financing be commercially reasonable, conducted openly and transparently, and based on free market competition, while taking into account trade obligations.

To manage and address the risks posed by 5G, the entire U.S. government is taking an interagency approach to this issue, led by the Director of the National Economic Council at the White House. The National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) - 4 process. These meetings are an opportunity to discuss and come to decisions on key 5G issues, such as participation in standards bodies, as well as to provide updates on interagency 5G activities. The Department of State is mobilized to continue its bilateral and multilateral engagements and to coordinate with its interagency partners.

That said, the United States is a leader in 5G deployment, and we will do so using trusted vendors to build our networks. Through our engagements, many other countries are now acknowledging the supply chain risk and beginning to strengthen their information and communications technology security alongside the United States.

For example, in August 2018, Australia issued 5G security guidance to Australian carriers to protect their networks from unauthorized access or interference by "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law."

Japan has also taken measures to address supply chain risks using existing and new authorities. Most recently, in April, Japan announced spectrum awards conditional on 12 criteria, including one on network security that requires operators to "take appropriate cyber security measures including measures to respond to supply chain risks."

Likewise, Taiwan had previously adopted measures to protect 4G networks from untrusted equipment vendors and has extended these measures to protect all 5G government networks and critical infrastructure.

In May, the Czech Republic hosted more than 140 representatives of 32 countries from around the world, as well as the European Union and NATO, to build consensus on a common approach to 5G security. This effort produced the Prague Proposals -- a set of recommendations on how to build secure and resilient 5G networks based on free and fair competition, transparency, and the rule of law.

We have been working to advance the principles envisioned in the Prague Proposals by encouraging other countries to endorse the Proposals and by signing joint declarations or memorandums of understanding on 5G security with like-minded countries, including Romania and Poland.

Most recently, the European Commission and member states released their coordinated risk assessment of 5G security. We welcomed the assessment and how it clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances in place.

The assessment also highlighted the corporate ownership structure of 5G suppliers as a potential risk factor, which aligns with the U.S. assessment and the Prague Proposals' call for transparency.

In addition, the assessment recognized that the "edge" and "core" of networks will blur in 5G networks, requiring increased security measures be applied to all parts of the network. This aligns with the U.S. assessment that you cannot mitigate the risk of untrusted suppliers by limiting them to certain parts of a network. Untrusted suppliers anywhere in the network could be exploited by authoritarian governments for espionage, traffic disruption, data manipulation, and/or theft of sensitive information and intellectual property.

The EU risk assessment itself is a sign of progress in our 5G campaign as it demonstrates that our allies and partners are recognizing the risk of untrusted vendors, but our work is far from over.

Next, the European Commission and member states will use this assessment to develop and agree upon "a toolbox of possible risk mitigating measures" by the end of the year. This toolbox will outline specific, albeit non-binding, actions that member states can take to secure their 5G networks. It is important that this toolbox address the vulnerabilities and risks identified in the EU's risk assessment, including from untrusted suppliers, and that member states then implement binding national measures to safeguard their networks.

Thank you for the opportunity to appear before the Committee today. I look forward to your questions.