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 the Judiciary
5G: The Impact on National Security, Intellectual Property, and Competition

May 14, 2019

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

As the world becomes more interconnected, international cyber policy issues are becoming even more critical to national security, human rights, and economic prosperity. The State Department promotes U.S. foreign policy interests in cyberspace by engaging with our allies and partners to advance our vision for an open, interoperable, reliable, and secure digital environment.

The Fifth Generation of wireless technology, or 5G, will be transformative by providing consumers and businesses with up to 100 times faster connections than 4G networks provide, and with very low latency – which is the time devices need to communicate with one another. Tens of billions of new devices will be connected to the Internet in the next few years.

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

With all of these services relying on 5G networks, the stakes for safeguarding these vital networks could not be higher.

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 seriousness of the need to adequately secure 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.

For example, because of the essential role that vendors play in networks and their maintenance, they could be ordered to undermine network security—to steal personal information or intellectual property, conduct espionage, disrupt critical services, or conduct cyber attacks.

Under Chinese law, most notably its National Intelligence Law, Chinese citizens and organizations are required to cooperate with Chinese intelligence and security services.

In addition, the Chinese government 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.

Therefore, we are concerned that China could compel actions by network vendors to act against the interests of U.S. citizens and citizens of other countries around the world.

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.

In addition, China has a long history of undertaking intellectual property theft to benefit its commercial interests. Last December, 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 China to compromise the networks of the providers' clients, including global companies located in at least 12 countries. Countries should not allow 5G to be another vector for China to steal their intellectual property.

Chinese companies, such as Huawei, appear to have benefited from subsidized financing 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 competitive principles, while taking into account trade obligations.

The United States will be 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 of last year, 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."

In March, the European Commission released a set of recommendations to improve the cybersecurity of 5G networks, noting that evaluations of equipment suppliers should include the "risk of influence by a third country, notably in relation to its model of governance." This principle should be applied rigorously.

Two weeks ago, 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. Moving forward, the Prague Proposals will help guide our engagements with our partners and allies to build secure 5G networks.

We will continue our bilateral and multilateral engagements to ensure that telecommunications, the Internet, and all the critical services that 5G will enable are secure and reliable.

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