Laura Galante
Principal, WestExec Advisors
Former Director, Cyber Threat Intelligence Integration Center
Office of the Director of National Intelligence

August 5, 2025

Noah Jackson
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Jackson:

Thank you for the opportunity to appear before the Subcommittee on Communications and Technology on Wednesday, April 30, 2025, to testify at the hearing entitled, "Global Networks at Risk: Securing the Future of Communications Infrastructure."

I am submitting the following answers below to Member questions submitted after my testimony.

Sincerely,

Laura Galante

Questions for the Record:

The Honorable Robin Kelly

1. Ms. Galante, Recent breaches have shown that vulnerabilities in our communications networks can stem not just from telecom infrastructure, but also from compromised end devices including IT hardware. How should Congress address the risk posed by companies controlled and owned by the People's Republic of China that make critical devices, such as computers, given their potential as threat vectors into critical communications systems?

There is significant and well-documented risk in incorporating PRC-manufactured devices in US telecommunication networks. In 2020 Congress passed the Secure and Trusted Communications

Networks Act which established the FCC-managed "covered list" of communications services and products that pose an unacceptable risk to national security. Numerous Chinese companies are included on the list including Huawei and ZTE.

Congress can take steps to strengthen the FCC's covered list work. This could include expanding the definition of 'risk' to include supply chain components, pursue accelerated removal timelines ("rip and replace") for covered list tech still in use and fully fund the program, and also coordinate with allies (i.e. EU, Japan, Australia) to develop shared covered lists that promote trusted network alliances to establish an ecosystem of trusted vendors in 5G/6G, edge, and critical infrastructure.

The Honorable Kathy Castor

1. *Ms. Galante, can you please elaborate for this committee what government-industry collaboration looked like in response to this attack? How is the government able to help companies identify Salt Typhoon activity into their networks, and what can we do to be more effective in the future?*

In response to the discovery of a multi-victim PRC-sponsored campaign against multiple US telcos, industry-government collaboration occurred primarily through law enforcement (FBI victim assistance and investigative support) and the sector risk management agency for the telecommunications sector–CISA (including the relevant ISAC). Intelligence agencies coordinated their support of these efforts primarily through the Unified Coordination Group which was established to respond to these breaches. Conducting a thorough review–such as the review process designed by the recently disbanded Cyber Safety Review Board–will identify a more effective intelligence sharing process between telecoms' security and intelligence teams and US government.

2. What vulnerabilities or gaps did Salt Typhoon's intrusion demonstrate to us regarding the US telecommunications structure?

The PRC-sponsored campaign against US telecoms highlighted the need for improved identity management practices in complex, critical networks. It also demonstrated the PRC's increasing willingness to target Americans' communications at both a personal level (for intelligence gathering purposes) and an ability to hold major parts of American telecommunications networks at risk for wider disruption.

3. What actions can we anticipate the PRC to be taking next to grow their own capabilities, and what should we be doing to combat this and enhance our national security?

The PRC's intelligence operations against US telecoms and the People's Liberation Army (PLA)'s deep access to US water, energy and transportation networks–both demonstrate President Xi's focus on developing digital leverage points against the US. We can expect this activity to continue as the PLA, Ministry of State Security and other PRC government entities seek options and intelligence that can have military, political, and economic consequences on US decision making.

4. Can you speak to what cybersecurity risks Elon Musk's so-called "efficiency" operations, specifically its unlawful access of personal data, have on our national security? What signal and opportunity does it present to adversaries like the CCP?

I do not have firsthand knowledge of these activities. As a general matter, PRC cyber actors closely follow the coverage of specific databases, systems, and vendors associated with government networks and will use any information they can gather to inform their reconnaissance efforts for future operations.

5. *What do these actions indicate to our allies? How will it impact our cybersecurity partnerships with them?*

As a general matter, our allies' cyber partnerships provide critical tactical and strategic intelligence about our common adversaries. Efforts that appear to undermine the information security or integrity of these relationships will undermine these partnerships and negatively impact US national security.