Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Secure America's Wireless Future"
September 27, 2019

Ms. Bobbie Stempfley, Managing Director, CERT Division
Software Engineering Institute, Carnegie Mellon University

The Honorable Anna G. Eshoo (D-CA)

1. **Please explain the role encryption plays in protecting the American people from potential vulnerabilities in telecommunications equipment. To what degree does the encrypting of calls and internet traffic mitigate risks related to potential vulnerabilities in telecommunications equipment?**

Response: Encryption technologies are an important part of protecting the content of the communications passing across telecommunications equipment, enabling confidentiality of the message in transit. While encryption solutions can be employed to reduce the risk of eavesdropping, they are limited in their ability to reduce the risks of other vulnerabilities in the supply chain. Vulnerabilities within the supply chain could allow for attacks that alter the way the telecommunication equipment accepts, routes, and processes communications (calls, messages, video, and data). This would enable an adversary to interject content into the message stream, disrupt the transmission of content, and/or affect the timing of the distribution of content. Further, impacting the routing would also facilitate the collection of routing information, as meta-data this provides rich insight into the relationships between individuals in the communication stream and can provide insights into the nature of the communications and possible transactions.

Attachment—Additional Questions for the Record

Ms. Bobbie Stempfley, Managing Director, CERT Division
Software Engineering Institute, Carnegie Mellon University

The Honorable Tim Walberg (R-MI)

1. **We recognize the concerns that rural carriers like Pine Belt, with their limited budgets, have when it comes to complying with the reimbursement program while also trying to deploy new, or upgrade existing, networks.**

   a. **Are there certain types of network equipment or services that are particularly vulnerable that should be prioritized for removal?**

Response: If the focus is to provide risk reduction, prioritization should not be on type of equipment, i.e. replace all routers before the switches, etc., rather it should be on the key places and roles of the equipment in the infrastructure. In any telecommunications architecture the equipment that provides the core management and infrastructure sits in a privileged place in the architecture. In this instance the elements of the transport that support the radio access network and the services that are required to provide the routing and peering point services should be prioritized.