Security Vulnerabilities Within Communications Networks: Find It, Fix It, Fund It

Jeff Johnston, Lead Economist, Communications

CoBank

June 27, 2019

Before I begin I want to thank Commissioner Starks for the opportunity to participate in today's workshop to address the national security threats posed by banned equipment within our communications networks.

My name is Jeff Johnston and I am the Lead Economist in CoBank's Communications division.

CoBank is a $125 billion cooperative bank that provides loans and other financial services to rural America. Our customer base includes farmers, ranchers, energy and water infrastructure companies, and communication network providers. CoBank, and its commercial banking partners have $4.5 billion in loan commitments to the telecommunications industry. CoBank serves a broad range of industry verticals including; wireless, wireline, broadband, datacenters and cable infrastructure.

As a mission based organization, CoBank is committed to serving rural America. We know we have to be more than just a senior debt lender to support rural communities. In addition to the financial services we offer to rural America, we publish articles and present our research findings to industry stakeholders, customers, and the farm credit and commercial banking system.

Rural wireless operators play a critical role in ensuring residents of sparsely populated, high cost areas have access to wireless communication services. Through their roaming agreements, these operators also serve as a critical partner to national network providers such as AT&T and Verizon by providing service where the aforementioned does not have network coverage.

Chinese-made equipment is being used in a number of rural communications networks. Huawei, the largest telecom equipment manufacturer in the world, is widely recognized as the price leader and has established itself as a major provider of telecom equipment to rural wireless operators. Purchasing equipment from Huawei has enabled rural operators to serve high cost areas at reasonable rates where few, if any, options exist for residents in these markets.

The recent executive order banning US companies from buying telecommunications equipment from designated foreign companies deemed a national security risk is problematic to rural operators.

From a financing perspective, many rural operators lack the balance sheet strength to take on additional debt to fund the capital expenses associated with replacing banned equipment. Nor do they generate enough cash flow to cover the costs associated with the executive order. We estimate that a system-wide rip and replace of unauthorized RF, core and optical related equipment could cost the industry over $1B. Without significant government support, the lion's share of rural operators would not be able to secure the necessary funding to meet this requirement.

Further, some rural operators have struggled to do business with equipment vendors outside of the executive order's scope, which has left them with very few options. Telecom equipment manufacturers have been cutting staff in response to a softening market, and in some cases they have failed to respond to tenders issued by rural operators.

By banning the purchase of telecom equipment from designated foreign companies deemed a national security threat, it's imperative that the government ensures other options are available to rural wireless operators.

Even if operators who have banned equipment in their networks are not required to rip and replace, they may eventually have to do so anyway. Running multiple vendor platforms in a network can increase operating expenses, which is something these companies can ill afford. For example, when new products and services are introduced they would need to be developed and tested against multiple platforms. This increased operational complexity will put pressure on operating margins, and could negatively impact network access.

Even in the best of times, funding such a program would be a major challenge for rural operators. The wireless industry is entering the maturity phase of the product lifecycle which is characterized by slowing growth and margin compression. Capital and operating expenditures are being scrutinized and operators are challenged to find new revenue streams. We think it's important that all these factors be taken into account when determining how to address national security threats posed by banned equipment within our communications networks.