Stop Buying Huawei Equipment?

National policy is muddled, contradictory and almost certainly more drastic than security needs require. But facts don't really seem to matter these days.

By Steven S. Ross / *Broadband Communities*

This year, the rumors and accusations about Huawei's potential or real security risk finally emerged into public debate. But the muddle continues. On November 25, the Federal Communications Commission (FCC) banned use of Universal Service Fund (USF)/ Connect America Fund money to purchase Huawei or ZTE equipment. The FCC also issued a notice of proposed rule-making that would force removal of such equipment in networks already built or maintained with USF money.

A week earlier, however, the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce issued a third Temporary General License allowing Huawei to buy certain U.S.-sourced components for 90 days. The issue at BIS is not, strictly speaking, network security. However, BIS says Huawei sold equipment to Iran built with U.S.-sourced components, despite the Iran embargo.

As I noted in the July Hawk column, Huawei denies these charges. What's more, the BIS exemptions allow Huawei to build equipment for sale to American carriers, typically in rural areas. It will be a tough sell. I suggested a compromise – that Huawei allow third parties in the United States to develop and sell software updates for existing equipment. But BIS pressure motivated Huawei to look beyond American technology for chips. That will complicate any third-party software vendors' task, as new generations of Huawei technology will diverge from the rest of the world's chip standards. Despite that, Huawei has signaled that it might be open to licensing its software to American and other third parties. A possible deal is pending but hardly a sure thing.

Say you work at a carrier that uses Huawei equipment – or wishes to. Obviously, it would be wise to find, or at least consider finding, alternative suppliers. It would be wise to create a plan for ripping out existing Huawei (and ZTE) equipment or finding an alternative software supplier for the equipment you have. And, again, worry about software updates, too. For details, see sidebar for links to two earlier Hawk columns, in the May/June and the July 2019 issues of this magazine.

SECURITY, TECHNOLOGY, POLITICS, MONEY

What do you tell your management or board of directors? Where do you find the money to take action if you so choose?

Start with policy: Again, strictly speaking, the FCC security action and the Commerce BIS embargo violation action are separate matters. But it seems that Commerce and the FCC are not talking to each other. Past administrations would have looked to the intelligence community and to the White House Office of Science and Technology Policy (OSTP) for clarity and coordination. But OSTP never had a chief White House science adviser under President Trump, and Trump hasn't displayed much trust in the intelligence community.

The odor of politics permeates the FCC move, as the FCC has little security expertise in-house. Folks at the FCC do note, correctly, that Chinese law requires Huawei and ZTE to help with espionage missions, and that the Chinese military partially owns ZTE.

You could be pardoned for thinking all of this is just a bargaining chip to use as trade talks finish between China and the United States. But does that really matter? Will the trade talks actually result in an agreement, or are they close to collapse anyway?

Now, about the money: Back in June, Congress was quick to propose $700 million in new funds to help rural carriers pay for replacing Huawei equipment. CoBank's experts – folks who wrote the mortgages on many loans to rural carriers to buy (usually with federal aid) the equipment in the first place – say the cost would be well over $1 billion. By the way, the money would be paid through the Rural Utilities Service at the U.S. Department of Agriculture (USDA). Coordination between the USDA and FCC has not been a model of efficiency and transparency.

Considering the many ways U.S. networks can be disrupted without touching Huawei equipment or anyone else's at the network level – and considering that there is a much smaller level of unease about equipment at the network edge, compared with the network core – you may be pardoned for thinking that this all will blow over. Don't think that way. ❖

Contact the Hawk at steve@bbcmag.com.

READ MORE

Hawk May/June 2019 – To Protect Network Security, Regulate Software, Not Hardware https://tinyurl.com/w7gv6ec

Hawk July 2019 – Huawei: So Many Pronouncements, So Little Change https://tinyurl.com/umgthu6