Telecommunication and Video Surveillance Equipment Introducing Risk

Tribal Consultation

December 03, 2020

Agenda

- Overview of importance of supply chain risk to Tribal nation cybersecurity
- Describe types of risk and identify banned foreign nation commercial vendors
- Describe Federal coordination on supply chain risk
- Provide overview of Federal authorities, with focus on prohibition of use of Federal funds for prohibited foreign national vendors
- Address engagement with Tribes to assess supply chain risks, reduce risks to Tribal cybersecurity, and ensure compliance with Federal requirements

Presenters

- Jason Freihage, Deputy Assistant Secretary for Management
- Joseph Austin, Associate Chief Information Officer for Indian Affairs
- Jack Donnelly, Chief Information Security Officer, Department of the Interior
- James Anderton, Chief Financial Officer for Indian Affairs

What are the risks?

- Supply Chain Risk is the probability of an incident associated with buying equipment from suppliers that cause cybersecurity threats, data breaches, or nonfunctional equipment.
- Commercial marketplace is increasingly filled with products from foreign vendors and some present risks to cybersecurity.
- Assessing Supply Chain Risk is increasingly important to ensuring cybersecurity of your valuable data and applications for government services and businesses.
- Risky equipment can allow foreign nations to:
  - Monitor your activity and communications; and
  - Collect data on your people, businesses and government activities, and Tribal nation priorities.
- Basically, if you are using this equipment, you should assume all information will be public.

Who are we most concerned about now?

- As a result of supply chain risk assessments, the following Chinese technology and surveillance companies are of concern and are banned in the United States:
  - Huawei, ZTE Corporation, Hytera Communications Corporation, and Dahua Technology Company, and Hangzhou Hikivision Digital Technology

- Generally these companies have products/services in two areas of concern
  - Cellular Services
    - Huawei manufactured Cell Phones and Cellular Towers
  - Surveillance equipment
    - Hikvision Cameras

Intelligence Community and Law Enforcement

Interior regularly coordinates with DHS and FBI to ensure all bureaus are aware of the latest threats and can take actions to mitigate risk.

For example, in an intelligence/law enforcement brief on Huawei:

- Interior was contacted about supply chain risks associated with 5G telecommunication equipment, specifically Huawei was:
  - Offering 5G solutions at or below cost
  - Advancing a strategy to lock organizations into long term contracts
- Intelligence/law enforcement asserted Huawei contacted Tribal nations with lucrative technology deals
- Indian Affairs asked to assist in public outreach and communication to increase awareness among Tribes of supply chain risks, and specifically the prohibited Chinese vendors

Authorities requiring actions to address risks

- National Defense Authorization Act of 2019, Section 889
  - Banned Chinese technology and surveillance companies, including the following:
    - Huawei, ZTE Corporation, Hytera Communications Corporation, and Dahua Technology Company, and Hangzhou Hikivision Digital Technology
  - Prohibits Interior from directly procuring any equipment, system or service that uses covered equipment or services
  - Prohibits Interior from entering into contracts or agreements with any entity that uses covered equipment or services

- National Counterintelligence Strategy of the United States of America of 2020
  - Requires efforts to identify risks to critical infrastructures
  - Provides process and procedure for securing the supply chain
  - Changed federal acquisition regulations to prevent purchases of covered equipment and services

Next Steps

- DASM/OIMT, working through Regions and Office of Self Governance, will engage Tribes and Tribal Organizations to assess current level of risk across Indian Country.
- Continue engagement with Tribes and Tribal Organizations on strategies to:
    - Reduce risk by eliminating use of equipment from prohibited vendors;
    - Ensure compliance with the NDAA section 889 prohibition; and
    - Identify paths forward for impacted Tribes.
- Following initial assessment with Tribes, DASM/OIMT will conduct follow-up consultations with Tribes and Tribal Organizations.

Tribal Input

- Types of Tribal feedback needed:
  - To what degree is this already a major concern for Tribal entities?
  - What tools would help you assess risk?
  - Do you have any recommendations on a preferred method to conduct the assessment of risk?
- Written input to: consultation@bia.gov
  - Or if email not possible, mail to: Joseph Austin, Associate Chief Information Officer (ACIO) – Indian Affairs, 1849 C Street, NW, MS 4660, Washington, DC 20240
- Questions: Joseph Austin, ACIO, joseph.austin@bia.gov, (202) 515-6827

Q&A