R Street

Free markets. Real solutions.

R SHEET ON
SUPPLY CHAIN SECURITY

May 2019

BACKGROUND

American national security depends upon supply chain integrity. In today's world, America's adversaries often advance their goals by exploiting technological weaknesses, engaging in a range of malicious cyber activities targeted at U.S. government agencies and critical industries. Insufficient protection against the possibility of devastating cyberattacks—against the American electrical grid or command-and-control communications systems during a crisis—could have disastrous consequences for society. Yet, until recently, the United States has lacked a unified strategy to deal with supply chain vulnerabilities.

Companies whose products are incorporated into our supply chains must be carefully vetted to ensure supply chain integrity. Last year's John S. McCain National Defense Authorization Act demonstrated a growing awareness of the importance of supply chain security by banning federal government use of certain products from Chinese firms Huawei and ZTE.

However, Huawei and ZTE are not the only companies that pose a threat to the federal government's supply chain. Other companies, such as Lenovo and Kaspersky Lab, may also threaten American national security, given their countries' problematic legal structures and histories of cyber espionage.

CURRENT DEBATE

Supply chain security is highly context-dependent, and requires a realistic appraisal of threats and vulnerabilities on a case-by-case basis. No federal department or agency is solely responsible for addressing the risk that the federal government faces, and at present, no national body effectively addresses the supply chain risks faced by state and local governments and the private sector. Instead, various federal actors—including the Commerce Department, the State Department, the Department of Homeland Security and the FBI—each play partial roles in addressing supply chain risk. This fragmentation of responsibility makes cross-departmental cooperation all the more imperative.

SUMMARY

- Ensuring supply chain integrity is vital to American national security.
- Huawei and ZTE are not the only risky foreign companies. Other companies from China and Russia (like Lenovo and Kaspersky Lab) should also be investigated.
- If the United States' approach to supply chain security is not transparent, American citizens will be put at risk.

There is often debate about whether or not a given supplier is, in fact, a national security threat. In general, international trade and foreign direct investment are highly beneficial to U.S. economic growth. However, there are times when a business deal can have a negative impact on American security. Mergers and acquisitions that might threaten American national security are sometimes blocked by the Committee on Foreign Investment in the United States (CFIUS). Unfortunately, CFIUS findings are classified. Similarly, other government intelligence regarding the threats posed by specific companies is not always made public, leaving individuals in the private sector confused or ignorant.

Even when a company is deemed a legitimate national security threat, there is often debate about the best way to mitigate such threats. While the United States has chosen to ban Huawei and ZTE from the federal government's supply chain, other allied countries, such as the United Kingdom and Germany, have pursued strategies to contain and manage risks without resorting to outright prohibitions, though the success of these strategies has yet to be proven.

ACTION ITEMS

The recent creation of a new Federal Acquisition Security Council is an opportunity to develop a more comprehensive approach to supply chain security. However, there are several additional actions we recommend:

Transparency: Between now and the end of 2020, the Federal Communications Commission should conduct a series of public hearings to discuss the supply chain threat to the telecommunications infrastructure of the United States and its foreign partners, how best to mitigate those threats and how best to recover from malicious activity directed against such infrastructure.

Focus on Likely Threats: To date, threats have arisen primarily from state-controlled companies from Russia and China. Therefore, the president should request that the U.S.-China Economic and Security Review Commission conduct an evaluation of supply chain risk from all Chinese-owned manufacturers.

Congressional Support: Congressional leaders should immediately designate one committee in each house of Congress as the lead for conducting oversight of the federal government with respect to supply chain risk management, to hold hearings on the topic with input from a broad range of witnesses in the public and private sectors, and propose legislation to address identified gaps in the law.

CONTACT US

For more information on this subject, contact the R Street Institute, 1212 New York Ave. N.W., Washington, D.C. 20005, 202-525-5717.

Paul Rosenzweig
Senior Fellow, National Security & Cybersecurity
prosenzweig@rstreet.org
202-738-1739

Kathryn Waldron
Research Associate, National Security & Cybersecurity
kwaldron@rstreet.org
202-900-8242

Jim Baker
Director, National Security & Cybersecurity
jbaker@rstreet.org
202-525-5717