

# What FAR Case 2019-009 Means for Tech

Meeting with Office of Information and Regulatory Affairs

April 6, 2020

Global Headquarters 700 K Street NW, Suite 600 Washington, D.C. 20001, USA

+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90





# About the Information Technology Industry Council (ITI):





### 2015: NIST SP 800-161 Published

Provides guidance to federal agencies on identifying, assessing and mitigating ICT supply chain risks at all organizational levels.

## 2017: DHS Binding Operation

Directive

Bans Kaspersky Lab products from all government agencies.

## 2018: Sec. 889 of FY19 NDAA

Bans federal procurement of telecommunications and video surveillance equipment and services from selected Chinese entities.

Bans agencies from contracting with companies that use covered equipment or services in any capacity with limited waiver authority.

2018

## 2018: SECURE Technology Act of 2018

Creates a Federal Acquisition Security Council tasked with creating uniform guidance around supply chain risk management of federal systems.

Allows agency heads to remove technology from federal networks once a supply chain risk is found while offering due process for impacted companies.

## 2018: ICT Supply Chain Risk Management Task Force Established

This public-private partnership, led by IT and communications industry experts, will develop consensus recommendations to identify and manage risks to the global ICT supply chain.

2019

## 2019: Executive Order on Securing the ICT Supply Chain

Authorizes the Commerce Secretary to regulate the acquisition and use of ICT products and services from a foreign adversary. In consultation with other agencies.

2015

 $\overline{\phantom{a}}$ 

## 2014 2017

## 2014: Section 515 of the Consolidated Appropriations Act of 2014

Requires the Commerce Department, DOJ, NSF and NASA to review, evaluate and mitigate the supply chain risk associated with any acquisition of high or moderate-impact IT systems.

#### 2017: Sec. 1656 of FY18 NDAA

Bans DoD procurement of Huawei or ZTE telecommunicati ons equipment or services for high-priority missions.

# U.S. ICT SCRM Policy

# **Timeline**



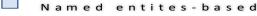
## 2019: FCC-19-121

Bars the FCC from using Universal Service Fund dollars for Huawei and ZTE products.

#### 2019: Section 845 of FY20 NDAA

Requires the Defense Secretary to streamline and digitize the DoD supply chain risk management approach for the defense industrial base.







# Contracting provisions in Sec. 889 of FY19 NDAA

- Subsection(a)(1)(A): Direct prohibition
  - Restricts federal government from contracting with Huawei, ZTE, Hytera, Dahua, Hikvision and any other company determined by the Secretary of Defense to be owned or controlled by, or otherwise connected to, the People's Republic of China
  - o In effect as of August 13, 2019; Addressed through FAR Case 2018-017
- Subsection(a)(1)(B): Indirect prohibition
  - Restricts federal government from contracting with entities that use covered equipment as a substantial or essential component of any system or as a critical technology as part of any system
  - o Will go into effect on August 13, 2020; Addressed through current FAR case



# Key terms remain undefined in statute

**Key Terms** 

"Entity"

Clarity Needed

 Will the definition cover a company's subsidiaries and affiliates?

"Use"

"Substantial or essential component"

"Critical technology"

"Owned or controlled by"

- Will the definition cover commercial use or merely use in the performance of a federal contract?
- FAR Case 2018-017: "Any component necessary for the proper function or performance of a piece of equipment, system or service"
- Export Control Reform Act of 2018 and North American Industry Classification System codes
- 2014 Commerce, Justice, Science appropriations law
- Proposed FIRRMA regulations



# Waiver process is unclear

- Statute provides limited waiver authority
  - Agency heads can issue a two-year waiver under limited circumstances
  - After two years, Director of National Intelligence has sole waiver authority
- Rule should lay out clear process
  - Micropurchases
  - GWACs
- Lack of alternative equipment options should be considered a mitigating factor



# Bottom Line: Unintended consequences of this law could erode U.S. technological dominance

- Compliance almost impossible for global companies
- Options very limited in certain geographies
- Increased costs from switching suppliers and damages from canceling contracts



- Compliance
- Economics



 A strict interpretation of this law may result in limited government ability to procure innovative IT goods and services and best-in-class warfighting technology



# National security threat is already being addressed

- Companies are using tools at their disposal to mitigate risk
  - NIST SP 800-161 <u>Appendix D, Threat Scenario 2</u>
  - DHS Information and Communications Technology Supply Chain Risk Management (SCRM) Task Force
- Agencies have authority to remove problematic equipment from federal networks
  - SECURE Technology Act of 2018



# Our asks

- Clearly define and scope key terms
- Simplify waiver process as to not interrupt government use of innovative technologies
- Look to pre-existing risk-based authorities to combat present and future cyber supply chain threats



# Questions?

Kelsey Kober, Manager of Policy, Public Sector <a href="kkober@itic.org">kkober@itic.org</a>
202-570-1177

