Timeline of Federal U.S. Actions on Tech Supply Chain Risk Management

Over the past few years, the United States has seen an emergence of new laws, agency actions, and public-private partnerships all with the goal of securing the information and communications technology (ICT) supply chain. This timeline maps the most significant policies and provides an overview of each policy's scope and implications.

Key Acronyms:

DHS: U.S. Department of Homeland Security
DOD: U.S. Department of Defense
DOJ: U.S. Department of Justice
DOC: U.S. Department of Commerce
FCC: Federal Communications Commission
ICT: Information and communications technology
NDAA: National Defense Authorization Act
NIST SP: National Institute of Standards and Technology Special Publication
NSF: National Science Foundation

Agency Specific

2014: Section 515 of the Consolidated Appropriations Act of 2014

Requires the DOC, 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 telecommunications equipment or services for high-priority missions.

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's supply chain risk management approach for the defense industrial base.

'14 '15 '16 '17 '18 '19 '20

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 Operational Directive 17-01

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: 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

A public-private partnership that provides recommendations to identify and manage risks to the global ICT supply chain.

2019: Executive Order on Securing the ICT Supply Chain

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

Government–Wide

Inventory of Federal Supply Chain Risk Management Programs

Compiled by the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force Coordination Tiger Team

1. Department of Homeland Security Cybersecurity and Infrastructure Security Agency ICT Supply Chain Risk Management (SCRM) Task Force
2. Outsourcing of Network Services Assessment Tool (ONSAT) Tool (formerly "Risk Management of Outsourced Network Services (RMONS)" – Out of the Enduring Security Framework (ESF)
3. Federal Acquisition Security Council (FASC)
4. Department of Commerce Bureau of Industry and Security (BIS) – Entities List
5. Bureau of Industry and Security (BIS) – De Minimis Regulation
6. Bureau of Industry and Security (BIS) – Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List
7. National Telecommunications and Information Administration (NTIA) Software Bill of Materials (SBOM)
8. National Institute of Standards and Technology (NIST) Internal Report (IR) 8276 - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
9. NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management
10. NIST Special Publication (SP) 800-161 Rev. 1 - PRE-DRAFT Call for Comments: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
11. NIST Special Publication (SP) 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
12. NIST National Cybersecurity Center of Excellence (NCCoE) – Supply Chain Assurance Project
13. Executive Order (EO) 13873 Securing the Information and Communications Technology and Services Supply Chain
14. Protecting Against National Security Threats to the Communications Supply Chain Through FCC [Federal Communications Commission] Programs (FCC 19-121)
15. Supply Chain Notice of Proposed Rulemaking (NPRM)
16. Final Designation Proceeding for Huawei Technology Company
17. Final Designation Proceeding for ZTE Corporation
18. Communications Security, Reliability, and Interoperability Council (CSRIC)
19. Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector
20. Department of Defense Cybersecurity Maturity Model Certification (CMMC)
21. National Defense Authorization Act (NDAA) Section 889 Federal Acquisition Regulation (FAR) Rule Implementation
22. Alliance for Telecommunications Industry Solutions (ATIS)/DOD 5G SCRM
23. Department of Energy SCRM Plan
24. Executive Order 13920: Securing the United States Bulk-Power System
25. Telecommunications Industry Association (TIA) SCRM Efforts
26. Solarium Commission
27. New Committee on Foreign Investment in the United States (CFIUS) Legislation
28. National Strategy to Secure 5G of the United States
29. Public Law 116-124: Secure and Trusted Communications Networks Act of 2019
30. Public Law 116-129: Secure 5G and Beyond Act of 2020
31. Utilizing Strategic Allied (USA) Telecommunications Act (Introduced in Senate)