wiley

ALERT

BIS Requests Comments on ICT Supply Chain Risks

September 21, 2021

On September 20, 2021, the U.S. Department of Commerce's (DOC) Bureau of Industry and Security (BIS) published a *Notice of Request for Public Comments (RFC) on Risks in the Information Communications Technology (ICT) Supply Chain*. The RFC calls for comments on cybersecurity and supply chain challenges for the ICT sector and will inform a federal report on ICT supply chain resiliency. Comments are due on **November 4, 2021**.

BIS issued the RFC pursuant to the *Executive Order (EO) on American's Supply Chains*. Specifically, as covered in a previous Wiley Alert, the EO charged the Secretary of Commerce and the Secretary of Homeland Security, in consultation with other agencies, to submit "a report on supply chains for critical sectors and subsectors of the [ICT] industrial base."[1]

Who Is Affected?

According to the RFC, for purposes of the report, the scope of the ICT industrial base consists of:

- hardware that enables
  - terrestrial distribution,
  - broadcast/wireless transport,
  - satellite support,
  - data storage to include data center and cloud technologies, and
  - end-user devices including home devices such as routers, antennae, and receivers, and mobile devices;

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Practice Areas

International Trade
National Security
Privacy, Cyber & Data Governance
Strategic Competition & Supply Chain
Telecom, Media & Technology

- "critical" software (as defined by the National Institute of Standards and Technology (NIST) in relation to EO 14028); and
- services that have direct dependencies on one or more of the enabling hardware.

Request for Comments

The RFC seeks comments on a host of issues and topics, including, among others:

- "critical goods and materials," as defined in section 6(b) of EO 14017 and related manufacturing capabilities;
- supply chain risks and information and cybersecurity practices and standards of the ICT sector with specific regard to the risks;
- resilience and capacity of American manufacturing supply chains, including ICT design, manufacturing, distribution, and the industrial base;
- specific policy recommendations important for ensuring a resilient supply chain for the ICT industrial base;
- U.S. ally and partner actions, and whether they have identified and prioritized ICT capabilities; and
- policy and possible legislative recommendations that are important for ensuring a resilient supply chain for the ICT industrial base.

What Does This Mean for Industry?

Industry has already provided extensive input to the U.S. government on a related EO entitled *Securing the Information and Communications Technology and Services (ICTS) Supply Chain* issued in May 2019, which proposes to restrict certain ICTS transactions that pose significant national security risks. Here too, companies, manufacturers, and suppliers in the ICT sector should consider submitting comments to inform policymakers at the DOC. The ICT industrial base encompasses a wide array of hardware, software, and service suppliers.

Industry should expect additional action from government agencies to address supply chain security risks. ICT sector suppliers ought to evaluate the constraints on their ability to secure crucial goods, materials, and services. Affected industries should also turn a critical eye on their supply chains, searching for any points of failure. Early advocacy can set the tone for the Administration's regulatory stance on ICT supply chains. Feedback could shape future regulatory burdens, raise coordination problems, address unfair trade policies, encourage alternative supply chains, and incentivize domestic ICT investments.

****

Wiley has a robust Supply Chain practice, as well as unparalleled experience and expertise in International Trade, National Security, Government Contracts, Telecom, Media & Technology, and Trade Analytics, and can help clients navigate evolving supply chain developments. For more information about the EO and notice requesting comments, please contact one of the attorneys listed on the alert. Wiley's multidisciplinary team

has been helping companies with shifting export controls, entity listings, various DOC ICTS supply chain regulations, the Federal Acquisition Security Council, Federal Communications Commission (FCC) supply chain activities, and procurement restrictions such as Section 889 of the 2019 National Defense Authorization Act (NDAA), and other NDAA restrictions.

---

[1] See EO on American's Supply Chains, "Sec. 4. Sectoral Supply Chain Assessments. (a) Within 1 year of the date of this order, the specified heads of agencies shall submit the following reports to the President [...] (iii) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the heads of appropriate agencies, shall submit a report on supply chains for critical sectors and subsectors of the ICT industrial base (as determined by the Secretary of Commerce and the Secretary of Homeland Security), including the industrial base for the development of ICT software, data, and associated services."

Scott Bouboulis, a Law Clerk at Wiley Rein LLP, contributed to this alert.