Updates
December 26, 2024
Department of Commerce Adopts Final Rule Restricting Tech and Telecom Supply Chain Transactions With Foreign Adversaries

The U.S. Department of Commerce's Bureau of Industry and Security (BIS), issued its much anticipated Final Rule under Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain* (EO 13873), on December 5, 2024. The Final Rule formalizes the federal government's framework for identifying, reviewing, and prohibiting transactions involving information and communications technology and services (ICTS) that may pose undue or unacceptable risks to U.S. national security, critical infrastructure, or the safety of U.S. persons. Unless the Department of Commerce changes course after the Trump administration begins or Congress "disapproves" the Final Rule, the new regulation will become effective February 4, 2025.

Issued originally in 2019, EO 13873 gave BIS broad authority to regulate ICTS transactions with ties to foreign adversaries, including China and Russia, as part of a broader effort to counter evolving threats to the U.S. ICTS supply chain. The Interim Final Rule (IFR) published in January 2021 established the initial framework but drew substantial public feedback regarding its scope, definitions, and review processes. Over the last three years, BIS has incorporated this input while also expanding its regulatory focus to specific technologies, such as connected vehicles and unmanned aerial systems. Notably, the Final Rule reflects BIS's implementation experience, stakeholder concerns, and the Biden administration's prioritization of supply chain security.

Key Updates in the Final Rule

The Final Rule significantly refines the scope and focus of ICTS transaction reviews, addressing both substantive and procedural aspects. By prioritizing the type of data involved and broadening categories subject to scrutiny, the rule reflects an evolved approach to safeguarding national security. It also enhances clarity for businesses through updated definitions, a streamlined review process, and detailed enforcement mechanisms. These changes aim to ensure a more precise and effective regulatory framework for ICTS transactions.

Specifically, the Final Rule introduces the following updates:

Expanded Scope

- **Threshold removal.** The rule eliminates the requirement that ICTS transactions involving sensitive personal data affect more than one million U.S. persons to trigger review. Risks are now assessed based on data type, not volume, to address potential national security implications regardless of scale.
- **Broader categories.** BIS clarified that ICTS transactions spanning critical infrastructure, sensitive personal data, and emerging technologies will receive heightened scrutiny.

Definitions Clarified

Key terms have been refined to provide businesses with greater clarity, including:

- **"Dealing in,"** which includes "buying, selling, reselling, licensing, or acquiring" ICTS.
- **"Importation,"** which covers ICTS brought into the United States through any means, including electronic transmission.
- **"Foreign adversary jurisdiction,"** which indicates that entities located, incorporated, or with a principal business in a foreign adversary country are subject to review.

Enhanced Review Process

- BIS clarified the initial determination process and extended the time for parties to respond to determinations to 30 days, with an optional 30-day extension for good cause.
- The Final Rule outlines the sources BIS will consider when making determinations, including interagency consultations.

Penalties

- The Final Rule clarifies that penalties apply to both direct participants in ICTS transactions and nonparties—such as subcontractors or intermediaries—who knowingly assist in violations. Prohibited activities include importing prohibited ICTS, evading mitigation agreements, aiding and abetting violations, or providing false or misleading information to the U.S. Department of Commerce.
- Penalties include civil fines up to the greater of $250,000 per violation (adjusted for inflation) or twice the value of the prohibited transaction, as well as criminal fines up to $1,000,000 and imprisonment for up to 20 years for willful violations.

Implications for Businesses

The Final Rule expands the regulatory landscape for ICTS providers, buyers, and users, particularly those operating in critical infrastructure sectors or handling sensitive personal data. With the removal of prior thresholds, even smaller transactions now risk triggering BIS scrutiny if they involve connections to foreign adversaries. U.S. businesses with global operations or foreign subsidiaries should evaluate their ICTS supply chains for potential risks, especially where there may be ties—direct or indirect—to jurisdictions BIS considers adversarial. To ensure compliance, businesses should conduct a thorough review of their ICTS supply chains to identify potential exposure to foreign adversaries, particularly in critical infrastructure or sensitive data sectors. Developing or updating internal compliance programs to include proactive risk assessments and regular monitoring of BIS updates and determinations is also essential.

As BIS continues to build on this authority—evident from recent rulemaking efforts targeting connected vehicles and unmanned systems—businesses must stay attuned to evolving regulatory priorities. BIS's approach is likely to remain selective, targeting high-risk ICTS transactions, but companies engaged in sensitive technologies or sectors should prepare for heightened scrutiny. Based on the first Trump administration's approaches to national security and regulation, as well as more recent statements by President-elect Trump and his advisors, it is difficult to predict how the incoming administration will balance an emphasis on national security with its expressed skepticism of regulation. The Trump administration's early approaches to Biden administration rules designed to enhance cybersecurity and infrastructure security will signal whether the incoming president intends to adopt, modify, or reject the regulatory scheme that emerged over the past four years.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security Communications

Related insights

Update

Salt Typhoon Cyberattacks: New Federal Cybersecurity Guidelines for Telecoms

Update

FCC Proposes New Internet Routing Security Rules for Telecoms