

**Small Entity Compliance Guide for the
Securing the ICTS Supply Chain Final Rule**

Basics	<p>This final rule, often referred to as “the Supply Chain Final Rule,” implements regulations for the Bureau of Industry and Security (BIS) to carry out Executive Order (E.O.) 13873 and E.O. 14034 authorities.</p> <p>The Supply Chain Final Rule is set out in 15 C.F.R. Part 791 Subparts A-C and governs the investigatory process for review of individual transactions or types of transactions, as opposed to sector- or class-based rulemakings which appear in the later subparts of Part 791. This rule establishes definitions and the scope of reviewable information and communications technology and services (ICTS) transactions, as well as the processes for ICTS transaction reviews, including: (1) how the Secretary will evaluate and assess transactions involving ICTS to determine whether they meet the criteria of E.O. 13873; (2) how parties to transactions reviewed by the Secretary can engage with the Office of ICTS (OICTS) within BIS and their responsibilities while under investigation; (3) how the Secretary will reach, and how parties may respond to, a preliminary decision (Initial Determination) regarding ICTS transactions under review; (4) how the Secretary will reach a final decision regarding ICTS transactions under review (Final Determination), including whether the Secretary will prohibit the transactions or mitigate the risks posed by the transactions; and (5) penalties for non-compliance. The rule became effective on February 4, 2025.</p> <p>This Small Entity Compliance Guide, issued under the Small Business Regulatory Enforcement Fairness Act of 1996, provides a plain language overview of the rule, but you should refer to the final rule directly for details, as well as the Office of Information and Communications Technology and Services (OICTS) website for further guidance that applies to all entities, including small entities, impacted by the rule. By its terms, this rule does not treat small entities differently than other regulated parties, so all guidance should be considered. There is no small business exception for this rule; however, OICTS has provided the below</p>
--------	--

	resources to help small business navigate this rule’s compliance process.
Who may be affected by this rule?	<p>Any person, including any small entity, that is participating in an ICTS transaction that OICTS has determined to review, prohibit, or mitigate through a Final Determination may be affected. Parties to ICTS transactions under review who have obligations or responsibilities during the review process will be notified directly by OICTS. Parties to ICTS transactions that are identified in a Final Determination will be notified directly of the Secretary’s decision to prohibit, not prohibit, or mitigate. Final Determinations that prohibit ICTS transactions will also be published in the Federal Register.</p> <p>U.S. persons, including small entities, may have obligations pursuant to Final Determinations. In such cases, these Final Determinations will be published in the Federal Register.</p> <p>OICTS would also like to remind small entities that certain ICTS transactions or classes of transactions with a foreign adversary nexus may be covered by separate ICTS- or sector-based OICTS rulemakings, such as the final rule on connected vehicles, so OICTS recommends small entities stay current on OICTS rulemaking through the Federal Register and OICTS website.</p>
What action must I take if I am covered by the rule?	<p>If contacted pursuant to an investigation, persons, including small entities, must follow the obligations listed in 15 C.F.R. Part 791 Subpart B. These obligations include, but are not limited to, furnishing records on demand and under oath, retaining any and all records related to the transaction(s) under review for no less than ten (10) years, and meeting thirty (30) day response timelines to Initial Determinations.</p> <p>Entities, including small entities, subject to an ICTS transaction review under 15 C.F.R. Part 791 Subpart B are typically provided the opportunity to respond to an Initial Determination before the Secretary reaches a Final Determination. In such a response, entities may attempt to refute the basis for the initial decision or assert that the circumstances resulting in the initial decision no longer apply and seek to have the Initial Determination rescinded or mitigated.</p>

	<p>Persons subject to an OICTS Final Determination must follow the prohibition or mitigation specifications of the Final Determination.</p> <p>In the event you are contacted by OICTS due to an ICTS transaction that poses a suspected national security risk, OICTS will provide specific instructions to comply with this rule.</p> <p>Please refer to Final Determinations or final rules published in the Federal Register by OICTS as well as updates and publications on the OICTS official website for further information.</p>
What if any alternatives are there to this rule for small businesses?	<p>OICTS considered regulatory alternatives to reduce the burden on small entities. However, such alternatives would not achieve the goal of protecting U.S. national security or U.S. persons from undue or unacceptable risk stemming from ICTS transactions with a nexus to foreign adversaries.</p> <p>Final Determinations issued under this rule may describe alternatives or exceptions, if any, related to a specific prohibition or mitigation measure for small entities.</p>
Enforcement concerns?	<p>The National Ombudsman resolves concern of uneven or excessive federal regulatory enforcement. Reviews are confidential and do not waive the right to pursue administrative appeals or any other legal action. Contact 888-REG-FAIR or Ombudsman@SBA.gov.</p>
How do I find this rule?	<p>The official text of the “Securing the Information and Communications Technology and Services Supply Chain” final rule appears in 89 Federal Register 96872.</p>
Background	<p>E.O. 13873 authorizes the Secretary of Commerce to prohibit transactions that involve ICTS with a nexus to a foreign adversary and that pose certain risks to U.S. national security, technology, or critical infrastructure, or U.S. persons. E.O. 14034 builds upon E.O. 13873 to explicitly include transactions that involve connected software applications with a nexus to a foreign adversary that pose undue or unacceptable risk to U.S. national security or U.S. persons within the purview of the Secretary’s review. Foreign adversaries</p>

	include China, Cuba, Iran, North Korea, Russia, and the Maduro Regime. The rule is administered by OICTS within BIS.
If you have any questions about this rule, contact	OICTS's Policy and Engagement Division Email: OICTSregs@bis.doc.gov
For additional OICTS Information, visit	OICTS Website 15 C.F.R. Part 791 E.O. 13873 E.O. 14034 Compliance Application and Reporting System