

National Security Risks Dependence Foreign Manufacturing

The national security risks of America's dependence on foreign manufacturing extend well beyond the economy. They include military readiness, cybersecurity, espionage, medical supply shortages, infrastructure vulnerabilities, and dependence on foreign governments during international conflicts.

The central concern is that the United States could become dependent on another country for products, materials, or technologies essential to its defense and civilian population.

Seven major national security risks

Risk	How it could threaten the United States
1. Military supply shortages	Foreign supply disruptions could delay production or repair of aircraft, ships, weapons systems, and military equipment.
2. Cybersecurity and espionage	Compromised hardware, firmware, or software could expose sensitive information or provide unauthorized access to critical systems.
3. Dependence on China for critical minerals	Restrictions on rare earths and other processed minerals could disrupt defense manufacturing, electronics, and energy technology.
4. Medical supply shortages	Interruptions involving pharmaceuticals, medical ingredients, or protective equipment could weaken emergency preparedness.
5. Electrical grid vulnerabilities	Foreign-manufactured equipment with insufficient security controls could introduce vulnerabilities into critical infrastructure.
6. Economic coercion	A foreign government could restrict exports of essential materials to pressure the United States during a diplomatic or military dispute.
7. Loss of industrial capabilities	The closure of domestic factories and loss of specialized workers could make it harder to increase production during wartime or emergencies.

These risks depend on the particular product, supplier, country, and security safeguards. Foreign manufacturing is not inherently unsafe, and American manufacturing does not automatically guarantee security.

What the U.S. government has documented

Two federal reports provide particularly strong evidence.

1. Government Accountability Office, July 2025

The GAO found that the Department of Defense relies on more than 200,000 suppliers and has limited visibility into much of its supply chain. The report identifies risks involving foreign suppliers cutting off critical materials or introducing technological backdoors.

U.S. GAO

[Read the GAO report: Defense Industrial Base](#)

2. National Institute of Standards and Technology (NIST)

NIST identifies cybersecurity supply chain threats including counterfeit components, tampering, malicious hardware or software, and unauthorized production. These vulnerabilities can be introduced at different stages of a product's life cycle.

CSRC

[Read NIST's cybersecurity supply chain guidance](#)

How this relates to your country-of-origin petition

Your proposed Amazon petition addresses one part of a much larger issue: supply chain transparency.

Country-of-origin labels would help consumers understand where products are manufactured. But national security assessments also require knowing where components originate, who controls the suppliers, and whether products have been independently tested for security vulnerabilities.

For example, a laptop assembled in the United States could still contain chips, batteries, or networking components manufactured overseas.

The important distinction is between ordinary consumer goods, such as French sweaters, and strategically critical products, such as military electronics, pharmaceuticals, and telecommunications equipment.

The national security concern is not simply buying foreign goods. It is becoming so dependent on a limited number of foreign suppliers that the United States cannot maintain essential services or defend itself when those suppliers become unavailable or compromised.