



PROTECTING CRITICAL SUPPLY CHAINS

Risks from Foreign Adversarial Exposure



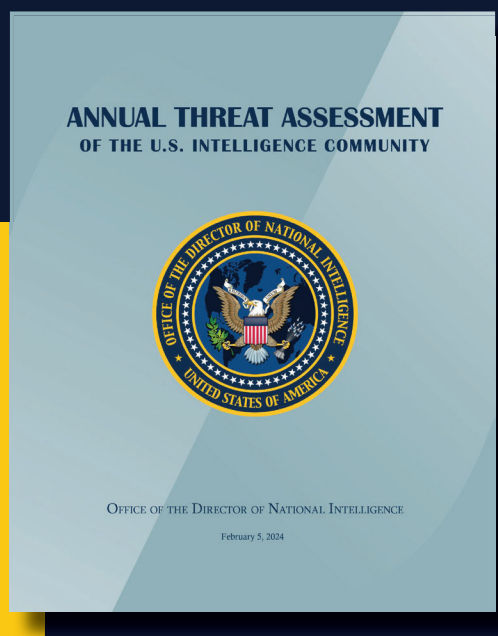


Protecting Critical Supply Chains: Risks From Foreign Adversarial Exposure

OVERVIEW

Cyber supply chain challenges are intensifying with profound implications for U.S. national security and economic resilience. Collaboration with all corporate security stakeholders and disciplines is essential to counter these challenges and reduce foreign adversarial exposure and access to the business operations of vital supply chains.

The U.S. Government has broad efforts to highlight areas, including in the Information, Communication, and Technology Services (ICTS) marketplace, for organizations that may not know their business operations are exposed to risks from nation-state adversaries exploiting the supply chains they rely upon every day.



“China will continue to expand its global intelligence posture to advance the CCP’s ambitions, challenge U.S. national security and global influence, quell perceived regime threats worldwide, and steal trade secrets and IP to bolster China’s indigenous S&T sectors.”

- Annual Threat Assessment of the U.S. Intelligence Community (2024)

When a cyber-attack vector proves unsuccessful or insufficient, nation-state actors may move to other threat vectors, including third party supplier relationships, investment arrangements, or witting and unwitting insiders. Corporate security stakeholders with an understanding of foreign adversaries’ intentions and ongoing efforts to exploit standard business operations require a more holistic view of enterprise risk.

This integrated risk approach protects corporate assets, employees, critical technology, and intellectual property. This guidance outlines significant foreign adversarial supply chain attack methods utilized by the People’s Republic of China (PRC), critical lessons learned, and suggested mitigations that corporate security stakeholders can tailor for their own risk management strategy.

CHINA'S DUAL USE INITIATIVE: PUBLIC & PRIVATE RISKS

In 2002, the PRC identified Military-Civil Fusion (MCF) as a national priority to develop its "dual-use" technology projects to rapidly advance its critical technology sector. In addition, the Central Military Commission, under Xi Jinping's leadership, codified MCF as an official military strategy in 2015, which signified an intensified push to innovate and advance MCF implementation. Since then, China's science and technology enterprise has been reorganized to ensure new innovations simultaneously advance economic and military goals. MCF strategy is

intended to move China towards its goal of military dominance; it will also reduce China's dependency on foreign technology in those sectors. Currently, the MCF strategy targets technologies such as quantum computing, semiconductors, 5G, nuclear technology, aerospace technology, and artificial intelligence. This PRC strategic focus may challenge U.S. businesses in these technology sectors seeking to protect their corporate data and minimize exposure from PRC sponsored companies from being in their supply chains.



U.S. INITIATIVES TO HIGHLIGHT & COUNTER DUAL USE RISKS

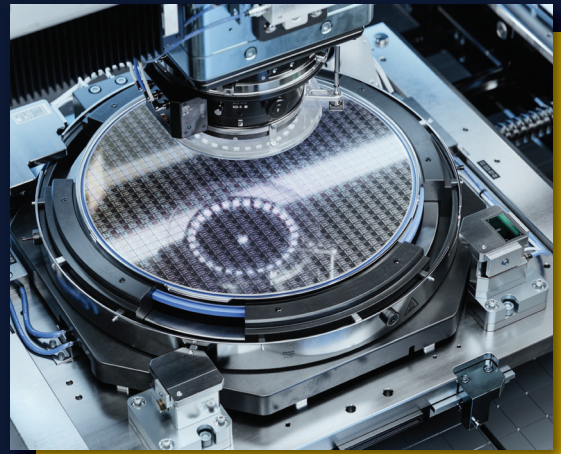
To mitigate China's MCF strategy and its efforts to acquire advanced technologies, the United States Government continues to update its export control regulations and continues to engage private industry on the risks to its critical technology and supporting supply chains. Corporate security stakeholders are keen to monitor various U.S. government export controls, regulations, and

entity lists as they pertain to critical technologies. These regulatory practices are well known, and corporations have a practiced "playbook" on how and when to engage with Federal officials. However, recent policy developments may require new actions or closer review to ensure incorporation into existing corporate risk management strategies.

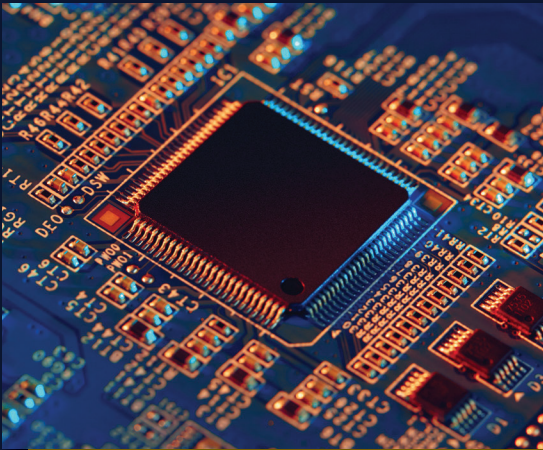
Specifically, the following initiatives focus on supply chain protections against foreign adversarial exposure. They can also be leveraged to enhance an organization's corporate and personnel security posture.

SECTION 1260H OF THE NDAA ACT FOR FISCAL YEAR 2021 (PUBLIC LAW 116-283) directs the Secretary of Defense to annually (until the end of 2030):

- Identify each entity the Secretary determines, based on the most recent information available, is operating directly or indirectly in the United States or any of its territories and possessions, that is a Chinese military company.
- Identify, among other things, Military-Civil Fusion contributors operating directly or indirectly in the United States.



While Section 1260H does not implement any supply chain prohibitions, other statutory provisions incorporate the 1260H listed companies into existing prohibitions, which prevent DoD from entering into a contract, directly or indirectly, with an entity on the 1260H list.



SECTION 5949 OF THE CHIPS AND SCIENCE ACT FOR FISCAL YEAR 2022 (PUBLIC LAW 117-263) directs the Secretary of Commerce to:

- Prohibit executive agencies from procuring or contracting with entities to obtain any electronic parts, products, or services that include covered semiconductor products or services from certain Chinese companies, specifically Semiconductor Manufacturing International Corporation ("SMIC"), ChangXin Memory Technologies, Yangtze Memory Technologies Corp, or any subsidiary or affiliate of these entities.

EXECUTIVE ORDER (E.O.) 13873. SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN allows the Secretary of Commerce to review ICTS commercial transactions within six product and services categories involving suppliers associated with a "foreign adversary."

- Currently, the list of designated foreign adversaries includes China, Cuba, Iran, North Korea, Russia, and the government of Nicolas Maduro in Venezuela ("Maduro Regime").





Protecting Critical Supply Chains: Risks From Foreign Adversarial Exposure

TAKEAWAY

Section 1260H, the CHIPS and Science Act, and E.O. 13873 all seek to address the growing national security threat in the global supply chain risks created by foreign adversaries attempting to obtain U.S. critical technology. While these regulatory and policy enhancements address specific technologies and industries, the collective impact aims to reduce the risks from foreign adversarial exposure; to bolster supply chain risk management information sharing; and to enhance supply chain protections around U.S. critical technologies.

“Beijing is implementing a whole-of-government effort to boost indigenous innovation and promote self-reliance, and is prioritizing advanced power and energy, AI, biotechnology, quantum information science, and semiconductors. Beijing is trying to fast-track its S&T development through investments, intellectual property (IP) acquisition and theft, cyber operations, talent recruitment, scientific and academic collaboration, and illicit procurement.”

- Annual Threat Assessment of the U.S. Intelligence Community (2024)

As the United States continues to mitigate national security risks to critical supply chains, U.S. private corporations may mirror similar security and risk mitigation measures to secure its supply chain and limit the risk of foreign adversarial exposure and access to its technology and intellectual property.

REPORTING AN INCIDENT

If you believe your company has been targeted or is at risk of compromise, contact the Private Sector Coordinator at your local FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>

REFERENCES

Section 1260H of the National Defense Authorization Act for Fiscal Year 2021
Section 889 of the National Defense Authorization Act for Fiscal Year 2019
Section 5949 of the National Defense Authorization Act for Fiscal Year 2024
Executive Order 13873 Securing the Information and Communications Technology and Services Supply Chain
2024 Annual Threat Assessment of the U.S. Intelligence Community
FBI: The China Threat
China: Military-Civil Fusion
The CCP Cyber Threat to the American Homeland and National Security
Federal Acquisition Regulation (F.A.R)

THIS INFORMATION IS CURRENT AS OF 1 APRIL 2024. THIS DOCUMENT
CONTAINS A GENERAL REVIEW OF NON-EXHAUSTIVE PROHIBITION
LISTS TO CONSIDER IN A PERSONNEL SECURITY PROGRAM.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

For more information on supply chain security, please visit [ncsc.gov](https://www.ncsc.gov)