OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

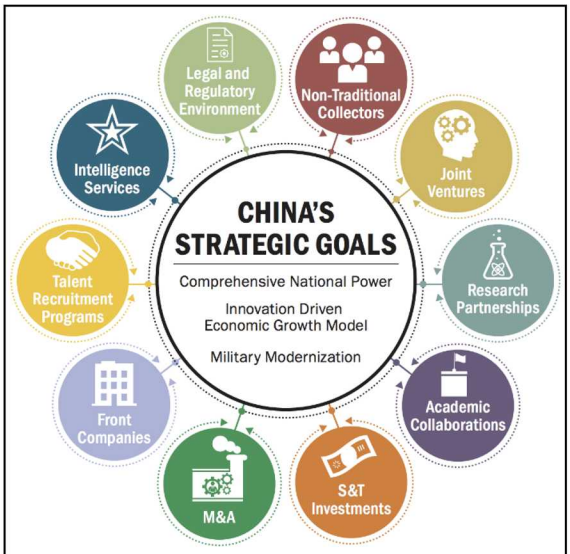
TRANSPORATION SYSTEMS SECTOR
PASSENGER AND FREIGHT RAIL

09 June 2020 **LIR 200709006**

Economic Risks to Rail Emerging Technology Companies from Chinese Joint Ventures and Investments

The FBI's Los Angeles Field Office, in coordination with the Office of Private Sector, prepared this LIR for rail industry partners to address ongoing risks to U.S. intellectual property arising from Chinese joint ventures and investments. As China continues to pursue joint and direct investments, research opportunities, and partnerships in emerging rail technology, U.S. companies should be aware of warning signs and risk factors in contracts and business decisions, as well as how to identify decision points where proprietary information might be at an increased risk of compromise through contractual technology transfer mandates.

Although joint work with Chinese companies may offer benefits to the U.S. rail industry, China could use the terms of these legitimate business arrangements to force U.S. rail companies to transfer proprietary technology or industry know-how to China to curb U.S. economic competitiveness and bolster China's global standing in the rail industry. As outlined in China's 25 Year Plan, "Made in China 2025," China uses joint ventures and direct or venture capital investments into emerging U.S. rail technology companies, as one means to achieve its growth and technology objectives through legal business practices. The Chinese Government pushes its own private sector to gain maximum advantage from these arrangements in order to drive national objectives. China could leverage the access gained from licit business relationships with U.S. companies to obtain and reconstruct U.S.-originated rail technology to modernize their trains for domestic use, secure patents, and mass produce next generation trains for foreign markets, to include the United States, at prices that could undercut competitors. Chinese investments in start-ups could give China access to the respective company's underlying technologies.



China's Strategic Goals
Source: Online Report | National Counterintelligence and Security Center | *2018 Foreign Economic Espionage in Cyberspace* | July 2018 | https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace | Accessed 26 June 2020

In late 2019, the U.S.-China Economic and Security Review Commission warned that state-subsidized Chinese companies with operations in the United States may seek to advance China's political or industrial policy goals by undercutting prices to take the market share from their U.S. competitors. The Commission further flagged Beijing's ongoing efforts to advance its economic and military goals by encouraging Chinese companies to invest in U.S. start-ups specializing in technologies in several key industries including autonomous vehicles/smart transportation and computer vision/visual intelligence.

Other emerging rail technologies potentially at risk include:

- Wayside equipment safety and data processing software and equipment
- Braking systems, including automatic and safety-related braking controls
- Locomotive car designs, engine schematics, and fueling improvements
- Trip optimization, shipment tracking, and scheduling software
- Industrial control software

The FBI identified the following indicators that foreign actors may be targeting or attempting to access intellectual property and technologies through joint ventures or direct and venture capital investments. These activities/indicators include, but are not limited to, any individual, group, or activity (*these indicators should be observed in context and not individually*).

- Increasing unsolicited offers from individuals or firms located overseas to purchase intellectual property, enter into joint ventures, or provide seed money to emerging U.S. technology companies
- Increasing efforts by overseas corporations or individuals involved in establishing joint ventures with, or investments into, U.S. technology companies mandating technology or intellectual property transfers as a part of the contractual agreements
- Increasing pressure from overseas joint venture or investment firms on U.S. emerging technology to move operations overseas
- Increase in anomalous network activity, particularly around remote connection, email systems and key data locations

The following proactive measures may help emerging technology companies, including those producing devices for next generation rail cars, protect their intellectual property from nation-states or criminal actors seeking to acquire their protected information.

- Prior to entering into joint ventures, ensure your organization knows if the business is owned by a nation-state or has a decision-making board or committee that has direct ties with, or is directed by, a nation-state.
- Prior to accepting venture capital or direct investments, ensure your company knows if the funds are subsidized by a nation-state or a state-owned entity.
- Prior to entering into agreements, ensure your intellectual property is protected from technology transfer clauses, especially to nation-state controlled or subsidized entities.
- Be wary of joint venture agreements that include job shadowing requirements, which could provide direct access to process engineering methods that would enable replication of entire industrial processes.
- Develop and maintain a network baseline that can be used to help detect anomalous activity. Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities. Strengthen credential requirements and implement multi-factor authentication to protect individual accounts, including those associated with any Managed Service Provider accounts.

- Train personnel in insider threat warning signs and ensure employees only have access to information and systems required to do their jobs. When an employee's job role changes or the employee leaves the position or company, immediately remove access, both physical and virtual.

In the early 2000s, China's former Railway Minister Liu Zhijun instituted a "technology transfer for market access" strategy to overcome China's unsuccessful attempts to develop indigenous high-speed railway (HSR) technology. In 2004, China began soliciting bids from foreign firms and contracts were awarded on the condition that the foreign companies assembled the trains through local joint ventures. Through these agreements, China successfully transferred their technical knowhow by negotiating access to train blueprints and securing training for Chinese engineers. By 2011, Chinese state-owned rail companies were participating in high-speed rail projects in Venezuela and Turkey, while bidding for contracts in Brazil, Russia, Saudi Arabia, and the United States.

In 2019, an identified U.S. company announced a partnership with CRRC, a Chinese state-owned rolling stock manufacturer, to deploy customized long-range visual perception modules, which is a key component for producing semi-autonomous locomotives. Partnerships such as these may create unintended risks including the loss or transfer of intellectual property and corporate proprietary information. Separately, subsidies from the Chinese Government enabled CRRC to consistently underbid its competitors in U.S. markets winning four out of five major contracts for new rail cars for transit systems in Chicago, Illinois; Boston, Massachusetts; Philadelphia, Pennsylvania; and Los Angeles, California. CRRC was looking to bid for contracts in New York as well.[a] When CRRC underbid domestic competitors in Australia, CRRC put two of Australia's three primary rail companies out of business and acquired the third. China will likely continue to engage in widespread efforts to transfer technology and undercut foreign competitors in the global rail market, activity consistent with China's industrial policy goal to introduce, digest, and absorb a foreign technology and "re-innovate" it with improvements.

For additional information about the risks private sector partners face from China, please visit the FBI's website at https://www.fbi.gov/file-repository/china-risk-to-corporate-america-2019.pdf/view. To report suspicious activity other incidents that may compromise emerging rail technology companies' intellectual property, go to Internet Crimes Complaints Center at www.ic3.gov and/or the National Intellectual Property Rights Coordination Center at www.iprcenter.gov. If you believe your company's intellectual property has been targeted or is at risk of compromise, please contact your local FBI Field Office.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office www.fbi.gov/contact-us/field-offices.

[a] (U) Congress signed the National Defense Authorization Act for Fiscal Year 2020 into law in December 2019 which forbids the use of federal grants to buy new subway trains or buses from Chinese state-owned rail company CRRC. Legislatures were concerned that subway cars made by a Chinese company might make it easier for Beijing to spy on Americans and could pose a sabotage threat to American infrastructure. (*Source.* Report | Congressional Bill, 116th Congress, 1st Session, House of Representatives | NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020 | December 2019 | https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf | pp. 2672-2677.)

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.