OFFICE of PRIVATE SECTOR
Liaison Information Report (LIR)

CROSS-SECTOR

12 JUNE 2026 LIR 260612012

Chinese Intelligence Officers Manage Private Sector Staffing Agency

References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.
The FBI does not and will not target people based on their race or ethnicity.

The FBI prepared this Liaison Information Report (LIR) to inform the private sector about the presence and role of Chinese intelligence officers in the management of the Foreign Enterprise Human Resources Services Company (FESCO), a company that staffs China-based branches of foreign businesses with local Chinese national employees. FESCO is headquartered in Beijing and has branches throughout China and the world. The FBI has information indicating senior officials at both FESCO headquarters and FESCO regional offices are intelligence officers from the Ministry of State Security (MSS),[a] an agency responsible for covert intelligence collection and counterintelligence to support the Chinese Communist Party's policy priorities.

According to FBI information, FESCO offices throughout China are staffed with senior-level MSS officers. These officers work undercover as corporate executives and oversee FESCO's day-to-day business. Lower-level FESCO employees and workers whom FESCO places in foreign businesses are less likely to be undercover MSS officers, though some are, and some non-MSS employees receive training in surveillance and elicitation techniques from the MSS. Non-MSS employees may also wittingly or unwittingly carry out MSS taskings. Not all Chinese nationals employed at FESCO, or whom FESCO has placed in foreign businesses in China, work for the MSS.

FESCO a Longstanding Staffing Agency for Foreign Businesses in China

Established in 1979, FESCO has offices in over 400 cities and provides services to thousands of businesses, according to its public website. For decades, foreign businesses have used FESCO to identify and place local Chinese nationals as employees for their China-based branches because the Chinese Government requires most non-Chinese businesses to use local employees rather than employees from abroad. Some of its purported customers are large, industry-leading US companies with proprietary technologies. As a Chinese staffing agency and employer of record for local hires, FESCO helps foreign businesses navigate many of the complexities of Chinese labor laws when seeking new workers.

The presence of its officers embedded throughout FESCO provides the MSS with the opportunity to use FESCO-placed employees in US companies to gather non-public information about US businesses operating in China. The MSS may order the workers it places to collect proprietary data on sensitive technology and personal information about other employees or to provide information about US business practices that the Chinese Government may see as a security threat.

[a] The MSS is China's primary civilian intelligence agency. With responsibilities roughly comparable to both the FBI and the CIA, the MSS conducts counterintelligence and counterespionage as well as domestic and foreign intelligence collection, including economic espionage and cyber espionage. Like FESCO, the MSS is headquartered in Beijing, and it has provincial and municipal offices located across China.

FESCO is just one tool the Chinese Government uses to collect foreign business information. In addition to China's aggressive and well-documented cyber activities, the US Department of Justice has indicted multiple Chinese intelligence officers and their agents inside US companies for stealing proprietary US business information. US businesses in China have been subject to coercive regulations and raids by Chinese authorities that have led to the loss of confidential information. In 2017, China passed a law requiring Chinese citizens and private organizations to cooperate with any request from an intelligence service like the MSS in service of "national intelligence efforts."

The following suspicious activities are potential indicators a FESCO-placed employee is attempting to collect sensitive US business information. An indicator alone does not accurately determine whether such an employee is an insider threat; organizations should evaluate the totality of potentially suspicious behavior before notifying security or law enforcement personnel.

- A FESCO-placed employee takes work—especially sensitive work—home;
- A FESCO-placed employee asks questions about sensitive information without a need-to-know;
- A FESCO-placed employee suggests or otherwise indicates that the employee works for the Chinese Government;
- A FESCO-placed employee does not promptly report contact with Chinese law enforcement or security services encountered in the course of the employee's work;
- On company computers, a FESCO-placed employee possesses or uses removable media outside of the employee's job responsibilities or otherwise uses unauthorized removable media;
- On company networks, a FESCO-placed employee engages in unusual activity or communications with suspicious contacts;
- Chinese law enforcement or security services ask US company representatives questions about situations or information about which they have no clear way of knowing;
- A FESCO-placed employee accesses or attempts to access information outside of the employee's job responsibilities;
- A FESCO-placed employee attempts to give an unauthorized individual physical access to the business or its information technology system; and
- A FESCO-placed employee conducts suspicious activities on company networks, such as accessing sensitive files, conducting large data transfers, engaging in off-hours network activity, bypassing security protocols, or uploading or downloading unauthorized software.

US companies who do business in China and have a relationship with FESCO, including hosting FESCO-provided personnel, may be positioned to provide information about that relationship and help the FBI understand more about this potential threat. The FBI encourages US private sector organizations to work with their China-based offices to identify indications of FESCO-related suspicious activity and report it to their local FBI Field Office.

Organizations operating in China that use FESCO or other human resources (HR) firms to hire local employees are encouraged to take the following actions, which align with best practices for mitigating insider threats:

- Conduct background checks on personnel hired through China-owned HR companies, including to identify a family history of Chinese Government employment.
- Ask direct questions to the HR company about their association with Chinese intelligence services.
- Audit and monitor foreign employees' access to computer networks, systems, and US business information.
- Implement procedures for reporting suspicious incidents, including record keeping to track trends over time.
- Establish a clear standard of conduct for foreign employees working in your China-based locations.
- Revamp or modernize any non-disclosure agreements or hiring contracts for locally sourced workers to provide your organization greater flexibility to fire, replace, or monitor them.
- Provide insider threat awareness training to US citizens managing locally hired employees.
- Ensure any communication with the FBI takes place from US-based offices rather than China-based offices.

The FBI's Office of Private Sector disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP: RED  For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.
TLP: AMBER  Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP: AMBER+STRICT** restricts sharing to the organization only.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP: AMBER+STRICT.
TLP: GREEN  Limited disclosure, recipients can spread this within their community.	Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.