Cross-Sector

5 August 2026 LIR 260805012

Case Study: China's Intelligence Services Recruited Insider to Obtain Sensitive, Non-Public US Economic Information

The FBI prepared this Liaison Information Report (LIR) to provide the financial services sector and academic community a case study illustrating how China's intelligence services (CIS) spot, approach, develop, and task people to provide sensitive, non-public information.[a] This study is intended to sensitize readers to concerning behaviors and suspicious activities that could be indicative of CIS intelligence gathering.[b] CIS are very interested in acquiring US sensitive, non-public information and frequently target individuals who can provide that information, regardless of where they work. Such information could provide the Chinese Government with key insights into high-level US decision-making processes and policies.

On 31 January 2025, the FBI, in coordination with the Federal Reserve Board of Governors (FRB), Office of the Inspector General (OIG), arrested John Rogers, a former Senior Adviser for the FRB, on charges of conspiracy to commit economic espionage on behalf of China and making false statements to federal law enforcement. Rogers exploited his employment with the FRB by soliciting colleagues for sensitive non-public information regarding proprietary economic datasets, deliberations about tariffs targeting China, briefing books for designated FRB governors, and sensitive information about Federal Open Market Committee (FOMC)[c] deliberations and forthcoming announcements. During a February 2020 interview with FRB OIG, Rogers claimed he never provided or shared any FRB restricted information with anyone outside the FRB. On 3 February 2026, a jury convicted Rogers of making false statements to federal law enforcement based in part on his claims in that interview.

Initial Approach

In May 2013, Rogers, representing the FRB, presented on US monetary policy at a conference at Fudan University in Shanghai, China. After the presentation, a CIS intelligence officer using the alias Hummin Lee[d] approached Rogers and identified himself as a PhD student from Shandong University (SDU).

---

[a] See Appendix A: CIS Recruitment Process.

[b] See Appendix B: CIS Recruitment Indicators.

[c] The FOMC is the decision-making body of the Federal Reserve that determines future US monetary policy actions, such as adjusting the federal funds rate. The FOMC consists of 12 members, drawn from the Federal Reserve Banks and the FRB.

[d] Lee, as referenced in this case study, is CIS intelligence officer Jin Chuan (金川), who used the aliases "Hummin Lee" and "Li Haiming" (李海明) when interacting with Rogers.

Development

Between 2013 and 2018, Lee provided Rogers gifts and personal favors and paid for Rogers's international travel. During this time, Lee developed Rogers as a source for sensitive, non-public FRB information—including interest rate marketization, US monetary policy, asset bubbles, exchange rates, and commodity prices—and utilized academic exchanges to compensate Rogers for sharing this sensitive information.

- Between 2013 and 2016, Lee sent Rogers several gifts, including handmade embroidery, a decorative copy of *The Art of War*, commemorative stamps, four silk scarves, a hand-painted folding fan, and a traditional Chinese painting.

- Between 2017 and 2019, Lee paid for at least five trips that Rogers made to China for conferences at Chinese universities and one trip to Seoul, South Korea, including Rogers's airfare, in-country transportation, meals, and hotels.

- Lee helped Rogers obtain his ten-year Chinese visa, set up bank accounts for him in China, fostered the relationship between Rogers and his second wife (including serving as their translator), and secured housing for his second wife and in-laws. In February 2020, Rogers said of Lee, "I owe everything to him. The…baby wouldn't have happened, the relationship with my wife wouldn't have happened…without him. And I love him like a brother."

CIS Taskings and Tradecraft

Beginning in May 2018, Rogers became responsive to Lee's taskings for sensitive, non-public FRB information about the US economy and monetary policies. Rogers obtained the sensitive information, including non-public FRB and FOMC information, on his own or from his FRB colleagues. Rogers gave Lee the information via email or WeChat,[e] as well as through purported "classes" he taught to Lee, a CIS intelligence officer using the alias Ricky,[f] and their associates in hotel rooms in China. Rogers went to great lengths to hide this activity from the FRB, using coded language such as "teaching" and "class" when setting up the meetings and identifying ways to increase their perceived legitimacy to the FRB.

- **May 2018:** Via WeChat, Lee asked Rogers to "collect answers from [his] colleagues" to a list of questions about the US dollar and China and further requested Rogers "teach" about it at their next meeting. Rogers emailed multiple FRB employees, one of whom was a China expert in the International Finance Division, asking for information about US-China trade imbalances, how FRB staff think about exchange rates, and the value of China's

[e] WeChat is a mobile messaging, payments, and social media application owned by the Chinese technology company Tencent. As of 2025, WeChat had approximately 1.4 billion monthly users, the vast majority of whom resided in China.

[f] Ricky, as referenced in this case study, is CIS intelligence officer Du Bin.

currency (the Renminbi). In response, Rogers received two documents, one of which was a portion of an April 2018 Designated Governors Book.[g] The email banner was “NONCONFIDENTIAL//FRSONLY.”[h] Rogers emailed this document to his personal email account and then forwarded it to Lee with the revised banner “NONCONFIDENTIAL//EXTERNAL.”

- **September 2018:** Lee rented a hotel suite for Rogers to "teach" Lee, Ricky, and a purported PhD candidate how the United States or FRB addresses risks from an emerging economy. Via WeChat, Rogers advised they needed to make the “class” appear legitimate by creating a course title, syllabus, student roster, and grading system.

- **September 2018:** Via WeChat, Lee asked Rogers to teach "classes" on US and FRB assessments of Japan’s economy and the European Union’s economy and monetary policy.

- **October 2018:** Rogers emailed an FRB employee asking for FRB information that could be shared externally related to trade policy uncertainty and US investment. Rogers also requested information that could not be shared externally, but which would enhance his understanding of the material. The employee gave Rogers two documents, including one related to the effects of washing machine tariffs, and requested he not share them outside the FRB. The next day, Rogers sent these documents to his personal email account and then to a Chinese professor at Fudan University. The following day, Rogers forwarded the document related to washing machine tariffs to Lee.

- **November 2018:** Via WeChat, Lee requested Rogers teach a class in Shanghai on US monetary policy trends in 2019. Lee told Rogers to find FRB statements or FOMC member presentations and analyze them in class. Rogers emailed multiple FRB employees in the International Finance Division, asking for relevant presentation materials and information about FRB forecasting, claiming they were for a talk to Chinese master’s students. Additionally, after requesting and receiving the October 2018 digital Designated Governors Book from an FRB employee, Rogers forwarded the book to his personal email account.

- **December 2018:** Rogers agreed to meet Lee and an identified individual for dinner in Shanghai. Approximately ten days later and after an FOMC announcement, Rogers sent Lee an email about the announcement, noting changes in the FRB’s forecast for US economic growth and planned interest rate hikes. Lee replied, “Aha, just like what we talked about at dinner."

---

[g] A Designated Governors Book is a briefing created by senior FRB staff for a newly nominated FRB member. The book is intended for an audience of one and is accompanied by a cover sheet stating, “Nonpublic Information, FOR YOUR USE ONLY, DO NOT DISSEMINATE.”

[h] “NONCONFIDENTIAL//FRSONLY” is an internal designation for materials intended solely for use within the Federal Reserve Board or the broader Federal Reserve System.

- **June 2019:** Lee and Rogers discussed arrangements for the next "class" in Beijing. On 13 June 2019, Rogers printed two documents related to a June FOMC briefing and flew to Beijing the next day. On 15 June, Rogers met Lee and Ricky in a hotel room for "class." On 19 June, Rogers sent Lee a WeChat message with a screenshot of a public FOMC statement from June 2019. Lee responded the statement was the same as Rogers had predicted, with only slight changes, like deleting the word "patient." Lee's reference to this deletion from the June 2019 FOMC statement appeared to indicate he saw a version of this statement before it was made public.

Rogers's Recommendations to Lee for Possible Recruitment

Rogers recommended several individuals to Lee as sources of information or possible recruitment.

- In December 2016, Rogers recommended a junior colleague accompany him on a May 2017 visit to the Research Institute of International Politics and Economics at Shandong University Finance and Economics, where Lee claimed to be an intern.

- In February 2018, Lee emailed a US-based economist and expressed interest in "learning" from the economist. Lee claimed his friend, Rogers, had mentioned the economist multiple times.

- In April 2019, Rogers recommended one of his students to Lee, touting how the student "could monitor all of the FOMC members [*sic*] public announcements, and keep you up to date with analysis of Fed policy." In June 2019, Lee stated he had paid the student $1,000 the previous month for information about the state of the US economy in the first half of 2019.

Post-FRB Employment and Continued "Classes" and Taskings for FRB Information

In May 2021, Rogers was forced to retire from the FRB for personal misconduct unrelated to his relationship with CIS, and he began teaching International Finance and Economics at Fudan University just three months later. In February 2022, Lee invited Rogers to Qingdao, China, to teach a "class" and meet "Director Zhang" from China's State Council. Lee offered to cover all expenses and pay Rogers for the "class." Rogers declined to meet with Director Zhang, citing retirement stipulations, but agreed to meet with Lee and Ricky before flying back to the United States. Rogers continued to seek internal FRB information. In an August 2023 email, he asked an FRB employee for a non-public Monetary Financial Market Analysis dataset.

Recommendations to Combat CIS Intelligence Gathering

Employees across the US Government, the financial sector, and academia have ideal placement and access to sensitive, non-public US information that likely fulfills CIS information needs. Employees are encouraged to abide by the following best practices to safeguard their organizations' sensitive information:

- Conduct all official business using hardware and software issued and approved by your employer's IT department and follow all relevant information security policies. Employees should not conduct official business using personal accounts or devices unless directed by their employer.
- Do not accept cash, gifts, or reimbursement for expenses in exchange for work or information from anyone other than your employer without prior notification and approval.
- While on personal travel, do not engage in work-related seminars, conferences, trainings, "brown bag" sessions, presentations, or workshops. Engaging in these activities could reveal you have privileged access to desirable information.
- Use all available resources to validate an individual's or company's bona fides before committing to a personal or professional relationship.
- Employers should consider instituting travel reporting procedures for employees related to personal and business travel to mainland China and Hong Kong, preferably with pre- and post-travel security discussions.

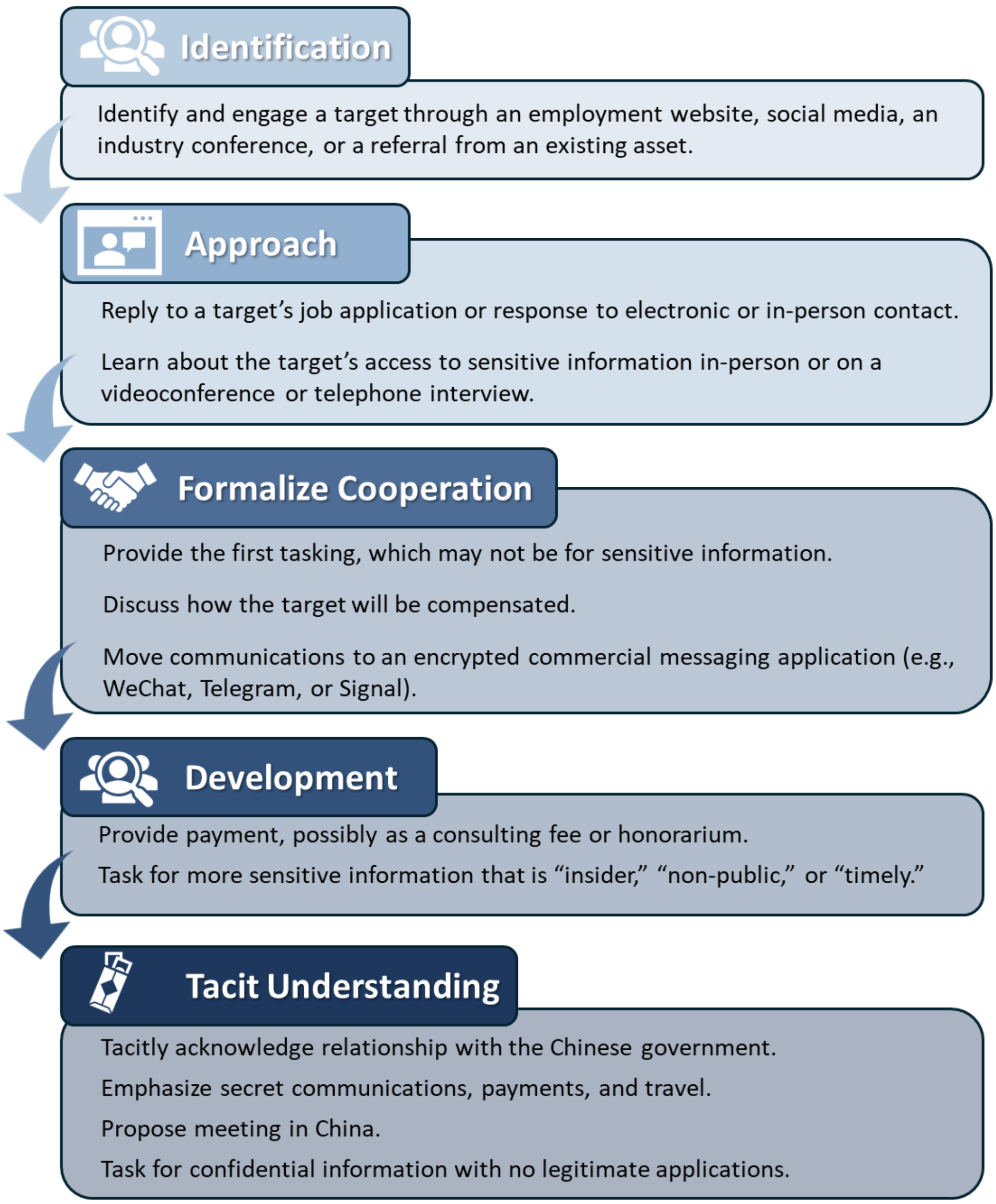
If employees encounter suspicious activity while in the United States or while traveling to China or Hong Kong, please contact the global security element of your organization and your local FBI Private Sector Coordinator to discuss any concerns. To report any leads, threats, and suspected criminal activity, you may also visit https://tips.fbi.gov. Any information you share may help the FBI more effectively address threats to the US Financial Services and academic sectors.

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.

This product was prepared by the FBI's Washington Field Office and Counterintelligence and Espionage Division, in coordination with the Office of Private Sector and the Federal Reserve Board of Governors' Office of the Inspector General.

Appendix A: CIS Recruitment Process

CIS use similar tactics to recruit people of all professional and academic backgrounds. Many US financial services and academic professionals have ideal placement and access to inform CIS about US financial operations, policies, and plans. While the precise steps a CIS officer takes to recruit a person can vary widely, the below graphic outlines common stages in the CIS source recruitment process.



Appendix B: CIS Recruitment Process

The following are common CIS tradecraft features that could indicate a Chinese national or entity is collecting intelligence for CIS from your organization or employee. A single indicator is not necessarily determinative of CIS involvement or otherwise malicious activity. However, the FBI encourages your organization and employees to report suspicious activity that exhibits any of the following indicators.

Funding and Travel

- Invites target to apparent professional or academic exchanges
- Represents meetings as presentations, lectures, or briefings
- Pays cash stipends or honoraria for minimal services

Online Presence

- Lacks history of operations, publications, or other bona fides
- Copies online information from an established organization
- Impersonates a legitimate organization
- Claims to be based in a US-partner country

Soliciting Sensitive Information

- Solicits sensitive information in a non-alerting manner
- Initially requests white papers or opinions on general topics
- Transitions to detailed requests for privileged information

Employment Opportunities

- Employment contracts
- Academic appointments
- Sabbaticals
- Research funds
- Grants
- Talent plan awards

Building Personal Relationships

- Flatters target and builds rapport around common interests
- Handles administrative tasks for travel to China
- Facilitates travel to and within China
- Assists with Chinese translations and communications
- Pays for meals and entertainment

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.