OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Cross Sector

LIR 180705001

5 July 2018

FBI's Recent Espionage Arrests Highlight Hostile Foreign Intelligence Services Targeting of Former US Government (USG) Clearance Holders

Why Are Foreign Intelligence Services Targeting Former USG Clearance Holders?

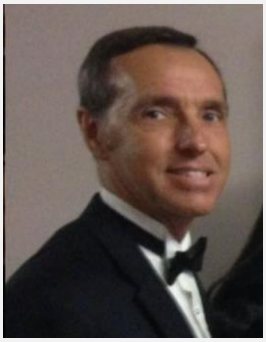
The arrests of three former US Intelligence Community (USIC) case officers on espionage charges in the past year highlight the threat posed by hostile foreign intelligence services to former USG clearance holders. The FBI assesses hostile foreign intelligence services are seeking to recruit former USG clearance holders likely for the following five reasons.

1. Former clearance holders likely remember classified information still of interest to hostile foreign intelligence services, such as USIC sources and methods, insights regarding the functioning of specific USG agencies, and vulnerabilities of current USG personnel.
2. They often have indirect access to classified information and can elicit it by maintaining contact with former colleagues who still hold clearances.
3. They can easily regain direct access to classified information by seeking re-employment with the USG, especially as a contractor.
4. They often market their previous USG experience on social media which hostile foreign intelligence services scour for potential targets.
5. They are no longer subject to security reporting requirements, such as the need to report foreign travel and foreign contacts.

How Are Foreign Intelligence Services Targeting Former USG Clearance Holders?

The FBI assesses foreign intelligence services likely primarily use commercial recruitment techniques to target former clearance holders, such as posing as headhunters seeking to hire "consultants" on innocuous-sounding issues like USG relations with foreign governments and counterterrorism cooperation. Foreign intelligence services primarily use two methods to approach former clearance holders. The first method is online via a professional networking site. The second method is contacting former clearance holders who reside in or regularly travel to their countries. Many former clearance holders are likely identified from cyber intrusions into USG unclassified networks, such as Office of Personnel Management databases.

Recent Espionage Arrests of Former Clearance Holders



Kevin Mallory

Ron Hansen

Jerry Lee

(U) *Source:* Undated photographs from Google images.

OFFICE of PRIVATE SECTOR

Recent Examples of Foreign Intelligence Services Targeting of Former US Government (USG) Clearance Holders

- On 8 June 2018, a federal jury convicted former CIA case officer Kevin Mallory on charges related to his transmission of classified documents to an agent of China. As shown in evidence in Mallory's trial, he was contacted by a Chinese headhunter on LinkedIn in February 2017, and traveled in March and April 2017 to China where he met a Chinese intelligence officer (IO). The Chinese IO represented himself as working for a Chinese think tank and provided Mallory a customized smartphone to electronically transmit classified documents using steganography.[a] Mallory was arrested in June 2017.

- On 3 June 2018, the FBI arrested former DIA officer Ron Hansen for attempted transmission of national defense information to China. Between 2013 and 2017, Hansen regularly traveled to China, where he allegedly received at least $800,000. He provided the Chinese intelligence services with information he learned at military and intelligence conferences in the United States and improperly sold export-controlled technology to China.

- On 8 May 2018, former CIA case officer Jerry Lee was indicted for conspiracy to gather or deliver national defensive information to aid the Chinese Government. After Lee left the CIA in 2007, he resided in Hong Kong and was approached in 2010 by Chinese IOs who offered to pay him for information. Lee prepared documents responsive to the IOs' taskings, made numerous unexplained cash deposits, and kept two books containing handwritten notes containing classified information regarding the true names of CIA assets and employees.

What Should Current and Former Clearance Holders Do About This Threat?

Based on their past success, hostile foreign intelligence services will almost certainly continue to target former clearance holders. Although foreign intelligence services likely have been targeting former clearance holders for decades, social media and professional networking sites have allowed them to easily identify and target both current and former clearance holders on a mass scale.

The FBI strongly encourages current clearance holders to report potential elicitation attempts by former colleagues who no longer have an active clearance.[b] The FBI also strongly encourages current and former clearance holders to conduct basic vetting of foreign contacts on professional networking sites and to report suspicious approaches, such as headhunters seeking consultants to foreign governments or foreign think tanks.

Potential Indicators of Foreign Intelligence Service Targeting

Below are potential indicators that a foreign contact or company on a professional networking site might be affiliated with a foreign intelligence service:

• No other current or former employees on the professional networking site.
• No website or limited company presence on the internet.
• No listed phone numbers or executives on the web site.
• Request to travel overseas and interview outside of a commercial location, such as in a hotel.

[a] Steganography is the technique of hiding a file within a picture.
[b] Concerns can be reported via the FBI's Public Access Line, 1-800-CALL-FBI, or via the Field Office Private Sector coordinators.