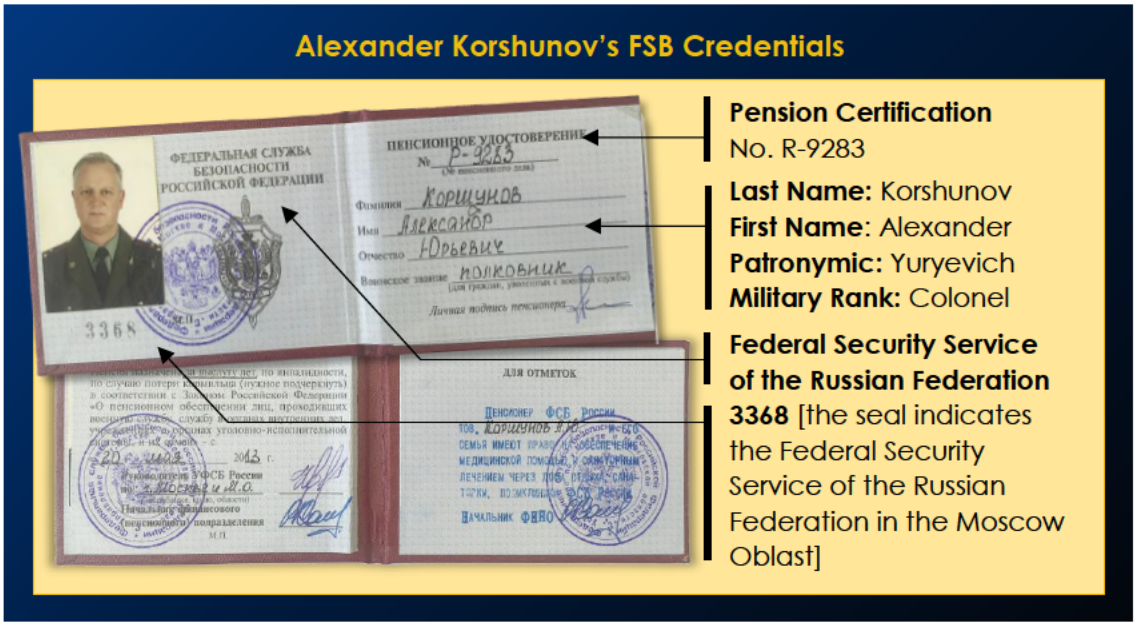
FBI COUNTERINTELLIGENCE BULLETIN

March 31, 2021

Case Study: Undercover Russian Intelligence Officer Targeted US Aviation Technology

Russia's intelligence services attempt to steal US science and technology (S&T) information using intelligence officers working undercover in Russian businesses and recruiting foreign nationals with access to US S&T. The recent case of Alexander Yuryevich Korshunov, a Russian intelligence officer arrested in Italy for theft of US trade secrets, illustrates why it is critical for US companies to make their employees aware of Russian S&T collection efforts and methods.

Russia has a long history of using its intelligence services to acquire foreign S&T. Underestimating the threat of Russian theft of technology and expertise could cause irrecoverable financial losses to US companies, damage our nation's security, and undermine US technological leadership.



An FBI investigation revealed Korshunov's ties to Russia's Federal Security Service (FSB) and Foreign Intelligence Service (SVR)—the primary successor agencies of the Soviet KGB. For his intelligence work, Russia decorated Korshunov with the medal of The Order "For Services to the Fatherland" second class, one of Russia's top awards.

The SVR awarded Korshunov a 25-year service medal in 2011, which suggests Korshunov began his intelligence career as a KGB officer in the mid-1980s.

Alexander Korshunov's SVR Service Medal

Identification Document
For the Medal of SVR of Russia
"Veteran of the Services"
[medal image]
Personal Number R-510098

Foreign Intelligence Service of the Russian Federation
Korshunov Alexander Yuryevich

By the Order of SVR of Russia
From December 1, 2011
No. 2584-ls

Is awarded the Medal of SVR of Russia
"Service Veteran"
[Seal of Foreign Intelligence Service of the Russian Federation]
Director of SVR of Russia [signature]

On August 30, 2019, in response to a US provisional arrest warrant, Italian authorities arrested Alexander Korshunov in Naples, Italy. At the time of his arrest, Korshunov, a long-time Russian intelligence officer, worked undercover as the director of marketing and sales in the Russian state-owned aviation company United Engine Corporation (UEC). Korshunov's assignment was to partner with Western aviation experts to fill Russian aviation S&T shortfalls.

From 2009, when he began his undercover assignment at UEC, until the time of his 2019 arrest, Korshunov used his position at the company to travel to the United States and abroad, meeting with US aerospace representatives, attending conferences, and targeting Western aviation technology and expertise for illicit transfer to Russia.

The US government charged Korshunov with two counts of attempting to steal trade secrets (18 USC 1832) for his work with an Italian accomplice to hire engineers employed by a former Italian subsidiary of GE Aviation. Korshunov paid these individuals to meet with him in Paris and Italy and provide consulting work on the re-design of the Russian PD-14 aero engine. GE Aviation has invested substantial resources over several decades to develop its jet engines. By operating through an Italian accomplice and various subsidiaries, Korshunov was able to acquire GE Aviation's expertise for the Russian engine, including proprietary information for advanced engine drive assemblies and jet engine accessory gearbox designs.

In August 2020, despite US efforts to extradite Korshunov to the United States, Italy returned him to Russia based on a competing extradition request from the Russian government.

Risk Mitigation Practices

Korshunov and his Italy-based accomplice offered GE Aviation employees money in exchange for work on a side project. Their offers of compensation, along with escalating requests for meetings and secrecy, are indicative of Russian espionage methods to collect S&T from Western scientists and experts. Employees should be wary of offers to pay for consulting work outside of the scope of their regular employment, especially offers involving virtual or in-person correspondence. US companies can take steps to sensitize their employees and minimize the risk of intellectual property loss and, as a result, guard US national security. These steps may include:

- Policies on accepting foreign government grants or money for work outside the scope of employment
- Reporting mechanisms for suspicious interactions outside of work with individuals who probe for information or offer money for expertise
- Monitoring foreign travel
- Providing regular CI awareness briefings
- Debriefing employees who travel overseas
- Implementing cyber security procedures that monitor suspicious network activity and flag unsolicited requests for information from Russian IP addresses

The FBI is dedicated to thwarting foreign government attempts to steal US innovation and gain an unfair advantage threatening US national security. The FBI welcomes any information you have that could assist with disrupting possible Russian economic espionage.

Report Suspicious Activity
(U) Report potential insider threats to your facility security office, insider threat program, local FBI Field Office, or Counterintelligence Task Force representative.

Administrative Note
For comments or questions related to the content or dissemination of this document, please contact the FBI National Counterintelligence Task Force by e-mail at FBI_NCITF@fbi.gov.