



**OFFICE of
PRIVATE SECTOR**
LIAISON INFORMATION REPORT (LIR)



INFORMATION TECHNOLOGY SECTOR

1 April 2019

LIR 190401001

US Adversaries Exploit Social Media Information to Target US Individuals and Government Clearance Holders

The FBI's Washington Field Office, in coordination with the FBI's Office of Private Sector (OPS), is informing private sector partners regarding foreign intelligence services' (FIS) exploitation of social media platforms^a and data to target corporate and US government (USG) clearance holders. FIS and US adversary intelligence officers are using popular US-based social media platforms to identify, recruit, and conduct operations against USG clearance holders, to include private sector employees or contractors supporting the USG. FIS officers will use popular US-based platforms and their respective countries' social media platforms for personal and intelligence gathering/operations purposes.

The FBI reminds US clearance holders and/or individuals with access to US sensitive/proprietary information to remain vigilant, and adhere to strict operational security protocols in their physical and online presence. Increasing physical and online operational security awareness, using best practices, and training may limit FIS solicitation attempts/activities. Visit the FBI's Domestic Security Alliance Council, InfraGard, and the FBI's Counterintelligence homepage for information and brochures related to FIS, as well as, material on insider threat awareness:

- www.fbi.gov/investigative/counterintelligence
- www.dsac.gov
- www.infragard.org

FIS Primary Targets: Former/Active USG Clearance Holders

In 2017, an FIS used a popular professional networking website to contact a former USG employee who held an expired Top Secret level clearance. The employee listed their intelligence/national security background on their website profile. A separated but recruited individual later acted as the "middleperson" who introduced the employee to the FIS. In February 2017, the employee traveled overseas to meet the FIS and established a covert communication channel. That communication channel served as a mean to pass Secret and Top Secret information to a US adversary. In mid-2017, the USG arrested and charged the employee for conducting espionage against the United States.

FIS Private Sector Targets: USG Contractor Clearance Holders

A known FIS front company used a publically available employment website to target USG defense contractors who posted their resume online. The FIS used the website to target, assess, and recruit

^a The term **social media platform** refers to as a broad range of private to public communication, employment networking, interaction, and file sharing featured tool via websites, as well as, applications on smart-devices and/or computer systems.



employees of US-based defense contracting companies supporting the USG who have specialized skills in the aviation technology.

Social Engineering Method: FIS use Fictitious Social Media Accounts to Obtain Access to Sensitive and Classified Data from USG and Corporate Employee

An FIS created a fictitious US military social media profile on several platforms. The FIS used the profile to establish online relationships/social network with a wide range of USG, US military personnel, and multiple US-based cleared defense contractors. The FIS used the social network to develop and assess a targeted pool of profiles.





Bridging the Physical and Online Introductions Gap: FIS Used Physical Events and Online Research for Social Media Usage to Establish Relationships

In early 2018, a US-based cleared defense contractor with a Top Secret level clearance attended a technical trade show conference in the United States. An FIS who operated a vender booth at the conference approached the contractor several times and offered sales of products/services. As a means to deter the aggressive sales pitches, the contractor indicated to the FIS his/her affiliation with the USG and offered the FIS a business card. A week after the conference, the FIS located the contractor on a popular professional linking website. The FIS sent an online request to the contractor via the website. The FIS is likely associated with an identified US adversarial military unit.

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](#):
<https://www.fbi.gov/contact-us/field-offices>



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>