



Center for Development of Security Excellence  
**CDSE**  
Learn. Perform. Protect.

# COUNTERINTELLIGENCE AWARENESS **JOB AID**



## Counterintelligence Awareness Case Study: Attempted Acquisition of Technology – Illegal Export to Iran

### Alireza Jalali

- 39 year-old citizen of Iran.
- March 20, 2018: Sentenced to 15 months in a U.S. prison for conspiracy to defraud the United States by illegally exporting sensitive military technology to Iran.

### What Happened?

- Between 2009 and December 2015, Jalali was a part-time employee of Green Wave Telecommunication, Sdn Bhn, a Malaysian company located in Kuala Lumpur, Malaysia.
- Green Wave Telecommunication operated as a front company for Fanavar Moi Khavar (Fana Moj), an Iran-based company that specialized in both broadcast communications and microwave communications.
- Green Wave Telecommunication was used to unlawfully acquire sensitive export-controlled technology from the United States on behalf of Fana Moj. In order to accomplish these acquisitions, Jalali and his co-conspirators concealed the ultimate unlawful destination and end users of the exported technology through false statements, unlawful financial transactions, and other means.
- The defendant's co-conspirators would contact producers and distributors of the sought-after technology, solicit purchase agreements, and negotiate the purchase and delivery of the goods with the seller. When the goods were received by Green Wave Telecommunication in Malaysia, Jalali repackaged and unlawfully exported the items from Malaysia to Fana Moj in Tehran, Iran.

### Impact

- In 2017, Fana Moj was designated by the United States Department of the Treasury as a Specially Designated National for providing financial, material, technological or other support, or goods or services in support of the Islamic Revolutionary Guard Corps (IRGC).
- The U.S. Treasury Department has sanctioned the designated end users of this technology for their ties to Iran's nuclear and ballistic missile programs and as dual-use technology reported to be used in weapon guidance systems.



**Specially Designated Nationals:** As part of its enforcement efforts, the U.S. Department the Treasury, Office of Foreign Assets Control (OFAC) publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called Specially Designated Nationals (SDN). Their assets are blocked and U.S. persons are generally prohibited from dealing with them. To access the SDN list, please visit [www.treas.gov/ofac](http://www.treas.gov/ofac) and click on the link for the SDN list under the OFAC mission statement.

**Export Controlled:** This case study address one example of how individuals bypassed the Export Control regulation to acquire and ship export controlled technology to embargoed countries by falsifying the true end user and destination. Your awareness is key to protecting our national security. To learn more about recognizing and reporting suspicious activities, visit the CDSE Counterintelligence Awareness Toolkit at:

<https://www.cdse.edu/toolkits/ci/index.php>