



February 16, 2010

Middleman Arrested for Allegedly Directing Malaysia-Based Iranian Illicit Procurement Scheme

By David Albright, Paul Brannan, and Andrea Scheel Stricker

In March 2009, Majid Kakavand, an Iranian citizen, was arrested in France on fifteen counts of conspiracy to export U.S.-made items to Iran, money laundering, smuggling, making false statements, and fraud. Beginning in January 2006 until around December 2008, Kakavand and two associates who are also under indictment allegedly ran a front company in Malaysia called Evertop Services Sdn Bhd, which illicitly bought electronic equipment from firms in the United States and Europe. The accused allegedly operated the company from Iran, directing at least 30 known shipments of U.S.-made items worth more than \$1 million to a freight forwarder in Malaysia, and then re-exporting the items on IranAir to Iranian military entities flagged on U.S. watch lists. The alleged exports violated the U.S. embargo against Iran and Office of Foreign Assets Control (OFAC) licensing requirements.¹

Based on a tip from a U.S. company, U.S. authorities began investigating the activities of Evertop Services in October 2007. This investigation led to Kakavand's indictment and arrest on a provisional arrest request while in France. The United States is seeking extradition of Kakavand from France to stand trial.² If successfully extradited and convicted of the crimes, Kakavand could face multiple years in prison per count and millions of dollars in fines.

Simple Malaysia-Based Procurement Network

Kakavand and his two associates, Amir Ghasemi and Alex Ramzi, established Evertop Services Sdn Bhd in Kuala Lumpur, Malaysia in 2005. This company also maintained a small office in Singapore, but Kakavand was not indicted on any charges relating to shipments through Singapore. It also allegedly attempted to use other company names and aliases for company officials. Evertop Services allegedly targeted both United States and European companies, but U.S. legal documents relating to the Kakavand case do not indicate information regarding European purchases. Kakavand, 37, was an electrical engineering employee of an oil company in Iran who took a second job procuring items through Evertop Services (though reports differ).³

¹ United States District Court of the Northern District of California, San Jose Division, *Indictment, United States of America v. Evertop Services Sdn Bhd, Amir Ghasemi, Majid Kakavand, and Alex Ramzi*, Case No. CR 09-0357 RMW (HRL), Filed April 7, 2009.

² *Affidavit of Candace Kelly, Assistant U.S. Attorney, Northern District of California, in Support of Extradition of Majid Kakavand before United States Magistrate Judge, Northern District of California*, April 20, 2009.

³ Angela Doland, "Engineer's Arrest Exposes U.S. Pursuit of Iranians," Associated Press. January 22, 2010.

He was co-director of Evertop Services, and Amir Ghasemi was also co-director. Both resided in Iran. Kakavand was previously investigated by the U.S. Immigration and Customs Enforcement (ICE) agency on suspicion that he was a procurement agent for the Iranian military. In 2006, ICE investigated a tip that Kakavand attempted to procure High Capacity Line of Sight military radio communication systems from a U.S. company.⁴ Alex Ramzi was the purchasing supervisor for Evertop Services.⁵ The U.S. indictment of Kakavand and his associates does not indicate where Ramzi resided.

The U.S. companies allegedly targeted by Evertop Services were located all over the continental United States in states such as Alabama, California, Florida, New Jersey, and Washington, and manufactured or sold electronic items usable in military, avionic, and aerospace programs. Evertop Services allegedly procured electronic items such as connectors, capacitors, resistors, measurement systems, reflectometers, rivets, and pressure sensors by telling the U.S. companies that the final destination of the items was Malaysia or that items would not be diverted to a country under U.S. trade sanction. Evertop Services sent its purchase requests to companies exclusively via email, through which it allegedly claimed to be a fully-functional trading company that sold electronic and electrical component parts to clients such as telecommunications firms located in the Middle East and Southeast Asia.⁶ According to the U.S. indictment of Kakavand and his associates, Evertop Services was a phony end destination, or front company, whose purpose was to divert items to the Iranian military.⁷

According to affidavit of an Immigration and Customs Enforcement agent assigned to Kakavand's case, authorities obtained a February 2006 correspondence from Kakavand's e-mail account to an unspecified recipient which described the *modus operandi* of the company: "Our company is a small business office only. There are two directors for this company both resident in Iran....This is just a small private company stablished(sic) in Malaysia for the sake of shipment purposes only...Now we have a small office in Singapore that is being managed by one employee there."⁸ A March 2006 communication with an unnamed freight forwarding service, possibly K Line Logistics, indicated, "We have recently established this company in Malaysia. Before this we handled our works in Singapore...We are Iranian. We have also got an office in Tehran. Of course as you know, our company has been registered in Malaysia."⁹

Kakavand and his associates allegedly routinely signed certifications for U.S. companies stipulating that items would not be transshipped to embargoed or sanctioned countries. Once

⁴ *Affidavit of Todd Harris, Special Agent, United States Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, in Support of a Criminal Complaint and Arrest Warrant before United States Magistrate Judge, Northern District of California, March 6, 2009, p. 8.*

⁵ *Indictment, United States of America v. Evertop Services, p. 2.*

⁶ *Affidavit of Todd Harris, p. 10.*

⁷ *Indictment, United States of America v. Evertop Services, p. 5.*

⁸ *Affidavit of Clayton Wright, Special Agent, Immigration and Customs Enforcement, in Support of the Request for Extradition of Majid Kakavand before United States Magistrate Judge, Northern District of California, April 20, 2009, pp. 4-5.*

⁹ *Ibid, p. 5.*

items were purchased and sent to Malaysia via unspecified U.S. freight forwarders, Evertop Services allegedly used an international freight forwarding company called K Line Logistics to receive and ship the items from Malaysia to Iran on IranAir. K Line Logistics is headquartered in Tokyo, Japan and has offices in Malaysia and the United States.¹⁰

Evertop Services' customers in Iran allegedly included Iran Electronics Industry (IEI) and Iran Communications Industries (ICI), two key suppliers to the Iranian military that in September 2008 were added to OFAC's Specially Designated Nationals (SDN) and Blocked Persons List based on evidence that they procure items for Iran's ballistic missile and nuclear programs. The SDN list specifies entities and individuals that work to procure sensitive items for sanctioned countries, and entities and persons on this list are prohibited from doing business with U.S. companies. For many years, IEI and ICI also have appeared prominently on German warning lists, which are confidential memos provided to German companies by the government, warning them about doing business with companies or entities on the lists.

IEI manufactures and offers "a diversified range of military products" including missile launchers, electronic warfare equipment, and manufactured night vision systems and laser range finders.¹¹ IEI was a well-known buyer for the Iranian Ministry of Defense Armed Forces and Logistics section on German government warning lists. ICI is Iran's "leading manufacturer of military and civilian communication equipment and systems," producing tactical communications and encryption systems.¹² E-mails obtained by U.S. authorities revealed that ICI in particular pressured Kakavand in meetings to quickly acquire needed items.¹³

Kakavand and his associates allegedly transferred payments for purchases from Maybank in Malaysia to the bank accounts of U.S. companies. The money supply for at least one of these alleged payments might have originated at the Shiraz branch of Bank Melli, Iran's state-owned bank that is sanctioned by the United States and European Union and included in United Nations Security Council Resolution 1803 as a bank whose activities states should "exercise vigilance over."¹⁴ Transactions originating from Bank Melli or any other Iranian financial institutions would have been laundered through Malaysia's Maybank, or made to appear as though they were originating in Malaysia so that U.S. banks would accept the alleged transfers.

At Least 30 Illegal Procurements Alleged

In total, from 2006 until 2008, Evertop Services allegedly made at least 30 illegal procurements of U.S.-made electronic items, garnering \$1,187,212 in equipment purchases from U.S. companies.¹⁵ Three of these alleged procurements are indicative of the tactics used by the

¹⁰ Ibid, p. 9.

¹¹ *Affidavit of Todd Harris*, pp. 10-12.

¹² Ibid.

¹³ *Indictment, United States of America v. Evertop Services*, p. 7.

¹⁴ "U.S. Slaps Broad New Sanctions on Iran," Associated Press. October 25, 2007; UNSCR 1803 (2008), March 8, 2008, p. 4; *Affidavit of Todd Harris*, p. 16.

¹⁵ *Affidavit of Candace Kelly*, p. 5.

Iran-based procurement agents to acquire items from U.S. companies. The accused have not yet been convicted of any crimes.

In December 2006, Evertop Services contacted a Northvale, New Jersey company on behalf of Iran Electronics Industries (IEI) for the purchase of 1000 capacitors and 400 resistors, valued at \$7,046. Amir Ghasemi allegedly signed a certification stating that the items would not be transshipped from Malaysia in violation of U.S. law, and the New Jersey company did not apply for an export license when it shipped the items to “Evertop K Line” since they were not controlled for shipment to Malaysia. In March 2007, K Line Logistics shipped the items to IEI in Iran via IranAir. Iran’s Bank Melli location in Shiraz was notified of the delivery.¹⁶

In August 2007, Evertop Services contacted a Morgan Hill, California company to purchase 85 pressure sensors. Evertop Services sent a request for quote (RFQ) to the company suggesting a sale price of \$17,000 for the 85 pressure sensors. At some point following this, the Morgan Hill company notified an agent from the U.S. Bureau of Industry and Security (BIS) that it had received a transfer of \$16,960 from Evertop Services for sensors, which it had shipped in November 2007 without a license to Malaysia. Ghasemi e-mailed K Line Logistics in Malaysia to urge haste in shipping the items to Iran, and K Line Logistics then shipped the items on IranAir to a location called “Farazeh Tajhiz Gostar” in Tehran. The nature of this entity is unclear from the U.S. indictment, and the entire name does not appear in internet searches (though “Tajhiz Gostar” appears in several variations of Iranian company names that are medical supply or engineering firms).¹⁷

A third procurement indicative of the alleged scheme was made in January 2008 of 2,500 inductors from a Milpitas, California company on behalf of Iran Communications Industries (ICI). Ghasemi signed an end-use statement from the company indicating that the shipment would not be sent to a country under sanction by the United States. The Milpitas company did not apply for a license for the \$17,855 shipment before shipping the items, and received payment for items sold from Evertop Services’ Maybank bank account. The items were scheduled for delivery to Malaysia, and K Line Logistics was instructed to ship them to ICI on the next available IranAir flight once they arrived. However, in July 2008, the Northern District of California obtained a federal search warrant that led to the seizure of the 2,500 inductors from an unnamed U.S. freight forwarder that was apparently preparing or in the process of shipping the items to Malaysia.¹⁸

In May 2008, Kakavand allegedly attempted to create a new company in Malaysia for receiving and shipping purposes, and investigated the availability of registering one of four different innocuous-sounding company names: Vertex Technology Sdn Bhd, Zenith Technology Sdn Bhd, Summit Technology Sdn Bhd, and Microsun Technology Sdn Bhd.

¹⁶ *Affidavit of Todd Harris*, pp. 15-22; *Indictment, United States of America v. Evertop Services*, p. 8-11.

¹⁷ *Ibid.*

¹⁸ *Ibid.*

Evertop Services' activities continued following the July 2008 shipment disruption. In November 2008, a New Jersey company informed the BIS agent assigned to Kakavand's case that its Australian representative had received enquiries from Evertop Services about purchasing items, with the claimed end destination of goods being Malaysia.¹⁹ In June 2008, Kakavand indicated in an e-mail communication to an unspecified individual that Evertop Services was also using an Armenian alias to procure items: Armen Vartanyan. He instructed the individual to take messages for Armen, an alias which his "friend" was using.²⁰

Extradition Pending

Kakavand was arrested on March 20, 2009 while arriving in France at Paris' Charles de Gaulle International Airport while traveling to Paris on a tour of Europe with his wife. The U.S. Magistrate Court of the District of Northern California made a provisional arrest request, and French authorities identified him as he passed through customs. According to the BIS special agent who investigated the sales requests of Evertop Services to California companies, officials from ICE began investigating Evertop Services' activities in October 2007, which later led to the arrest request and indictment of Kakavand.²¹ According to this time frame, the ICE investigation may have begun following suspicions reported about Evertop Services by the Morgan Hill, California company.

Kakavand was released from prison in August 2009 but is not allowed to leave France. The matter of Kakavand's extradition will be decided on February 17 following extradition hearings that took place in France. Iran has denounced the detention and extradition proceedings over Kakavand. Iranian foreign ministry spokesperson Ramin Mehmanparast said that Kakavand was innocent and that the United States and France were seeking to pressure Iran for unspecified reasons, even using forged evidence concocted by the United States.²² According to the Associated Press, French media reports have claimed that Iran offered to release two French women being held in Iran on charges of supporting the government opposition in return for Kakavand's release, and other reports said that France proposed the deal.²³ Authorities in both countries denied the reports.

Kakavand and his lawyers maintain that the items he allegedly bought and exported to Iran could not be used in military programs and were exported without violating licensing requirements to Malaysia.²⁴ A U.S. Department of Justice official, speaking anonymously to the Associated Press, said that trading companies and agents doing business with many nations "have an obligation to follow the laws of each of those countries, not just those they see fit."²⁵

¹⁹ *Affidavit of Clayton Wright*, pp. 21-22.

²⁰ *Affidavit of Todd Harris*, pp. 22-23.

²¹ *Affidavit of Todd Harris*, p. 8.

²² "Iran Urges France to Free Engineer Wanted by U.S.," *Agence France Presse*. January 19, 2010.

²³ "Engineer's Arrest Exposes U.S. Pursuit of Iranians."

²⁴ Nasser Karimi, "Iran Says France Using Iranian's Trial to Pressure," *Associated Press*. January 19, 2010.

²⁵ "Engineer's Arrest Exposes U.S. Pursuit of Iranians."

Lessons and Observations

Malaysia remains an important point of transshipment for U.S.-made items heading to Iran. Malaysia has resisted international pressure, particularly its obligations under U.N. Security Council Resolution 1540, to create and implement export controls and monitor the activities of companies on its territory. The United States should pressure Malaysia to implement export control laws as it did with the UAE in 2007. Unless Malaysia creates and implements export control laws, the United States government should add licensing requirements to the export of a wide range of dual-use items to Malaysia, requiring Malaysian companies to provide verified assurances that the goods will not be secretly transshipped elsewhere.

This case study reveals that Iran successfully used a relatively uncomplicated procurement scheme to acquire vast quantities of electronic items for Iranian military entities. In this instance, a single front company operated remotely from Iran purchased items from the United States and sent them to a freight forwarding location in Malaysia. The simplicity of this scheme shows that U.S. companies need to exercise more caution when doing business with acknowledged Malaysian trading companies and middlemen, especially in this case where an Evertop Services official admitted to being an Iranian with a Malaysia-registered company. Companies also should do more to verify the legitimacy of the buyer of the items' physical address. Companies might have been able to determine that the shipments were headed to a freight forwarding address if this were not already obvious from shipping destination names such as "Evertop K Line," the name given for the procurement from the New Jersey company. A simple internet search on the second part of the company name, "K Line", would have shown that it is a major global freight forwarder, if they weren't already known by reputation. Shipments to Malaysian freight forwarders should raise red flags for responsible company export compliance officials given Malaysia's well known status as a transshipment point for Iran, Pakistan, and other countries. Simple checks can often reveal potential illicit procurement schemes before sales are made and companies face potential fines and prosecution for export control noncompliance.

Companies need more information from the U.S. government about the latest illicit procurement schemes and attempts, including up-to-date individual and entity names that often only intelligence agencies have. Too often, U.S. companies rely on outdated and incomplete lists of entities and individuals when authorizing foreign sales. The fact that Kakavand was previously investigated for illicit procurements, for example, was likely not information available to company compliance officials. This may have been useful knowledge for companies that perform simple screening checks of potential clients against lists of names, associates, and companies suspected of illicit trading by the U.S. government.

Germany and Britain routinely provide their domestic companies with more information about which Iranian companies and entities to avoid. The United States needs to share more information about companies and entities discovered to be working for Iran's military or nuclear programs. In the Kakavand case, U.S. authorities were slow to alert companies about the risk posed by Kakavand and Iranian entities such as IEI and ICI. If notified, U.S. suppliers

could have avoided Kakavand's enquiries or requests for quotes. In the end, prevention of a sale is more valuable than punishment after the fact.

More than \$1 million in military-usable electronic equipment was diverted to Iran through Malaysia in a simplistic scheme that was missed for nearly a year by both company compliance and U.S. government export enforcement systems. It is clear that the system has not worked optimally, and U.S. government and U.S. companies, as well as the U.S. government and its foreign partners, need to work together more effectively to ensure that the illicit procurement schemes of sanctioned countries are detected and thwarted.