April 14, 2011

Man Charged with Exporting U.S. Goods to Pakistan’s Nuclear Program

David Albright and Andrea Stricker

Overview of Case

On March 9, the United States formally announced charges against a Pakistani man living in Maryland for illegally buying U.S. goods with nuclear dual-use applications between 2005 and 2010 and sending them to the Pakistani nuclear program. Nadeem Akhtar, 45, is in U.S. custody and charged with nine counts of export control, money laundering, and conspiracy related violations for exports of “items that are used directly or indirectly in activities related to nuclear reactors and the processing and production of nuclear-related materials,” according to a Department of Justice press release. According to the indictment, among the nuclear dual-use goods allegedly sent to Pakistan by Akhtar were calibration and switching equipment, resins for coolant water purification, surface refinishing abrasives, and radiation detection devices. The two Pakistani entities which received goods through Akhtar’s alleged illicit procurement operation were the Chashma nuclear power plant (CNPP) and the Space and Upper Atmosphere Research Commission (SUPARCO).

Lessons

This case study highlights:

- The need to improve U.S. government/industry cooperation and information sharing to detect illicit procurement networks. This cooperation should encourage more corporate diligence about checking the bona fides of a customer and include the U.S. government sharing more information about current illicit procurement schemes.

- It can take years for a smuggling network to make a mistake that authorities find suspicious enough to investigate, leading to the busting of the network.

- Improved corporate vigilance can detect suspicious enquiries. Regular communication with the U.S. government can help detect illicit procurement networks and prevent their success.

- The U.S. government should develop a procedure to tip companies about suspicious trading companies, as is done in Britain and German
Pakistan remains an active procurer of nuclear dual-use goods and utilizes highly sophisticated networks to obtain what it needs. Pakistan publicly claims to be a responsible nuclear nation and says it wants a civilian nuclear trade deal as a result. Yet, its illicit nuclear procurement efforts remain steadfast and belie its claims of acting like a responsible nation. As an ally, the United States should insist that Pakistan stop its illicit nuclear trafficking activities and prove it is truly committed to global non-proliferation norms and laws.

The Alleged Scheme

Akhtar, a Pakistani national and lawful permanent U.S. resident, operated an import/export company out of Silver Spring, Maryland called Computer Communication USA (CC-USA), which he represented to U.S. companies to be a subsidiary of the Pakistani company Computer Communication International (CCI). He allegedly operated this company from 2005 until 2010 for the purpose of deceiving U.S. suppliers about the end destination and use of goods he ultimately routed to the Pakistani nuclear program without applying for licenses. He allegedly obtained goods from seven different companies located in North Dakota, Pennsylvania, Maryland, Massachusetts, Tennessee, and Texas. He is also accused of making illegal financial transactions to arrange payment for the goods.

Akhtar allegedly worked with associates located in Dubai and Pakistan to arrange the procurements. Another individual who directed Akhtar’s alleged procurements from Pakistan is also indicted, but his name has been redacted from the publicly available U.S. indictment likely because he is still sought by law enforcement or remains under investigation. Other information is redacted from the indictment, such as the name of one of Akhtar’s Pakistani associates involved in running procurement operations and names of entities involved in the alleged scheme.

Because Pakistan is a non-signatory to the Nuclear Non-Proliferation Treaty (NPT), the United States bans on national security grounds the export of U.S. goods with nuclear applications to Pakistan, specifically to entities such as SUPARCO and the Pakistan Atomic Energy Commission (PAEC) and entities under its administration, such as the Chashma nuclear power plant and the Institute of Engineering and Applied Sciences (PIEAS), which conducts nuclear research and development and operates a research reactor in Pakistan. Among Akhtar’s exports to Chashma were products used for controlling electrical circuits and lighting in nuclear power and fuel reprocessing plants. In July 2010, ISIS published satellite imagery of the Chashma nuclear site, and speculated in a January 2007 report that, according to the available evidence seen in satellite imagery, a compound under construction to the southwest of the Chashma nuclear plants could be the site of the once-abandoned reprocessing facility intended for the production of plutonium for nuclear weapons. The report found that Pakistan may have resumed work around 2002 on finally bringing this reprocessing facility into operation.

Among the tactics Akhtar allegedly used to obtain the dual-use goods were using a U.S. company to buy goods from another U.S. company on his behalf, using a contractor of a U.S. company to buy goods, doing business with a U.S. company that knowingly or accidentally violated the U.S. ban on nuclear dual-use exports to Pakistan, and even lying to a Commerce Department official when asked about an end-user. He allegedly utilized a Dubai trading company as a claimed end-user of U.S. goods ultimately routed to Pakistan by an associate. He allegedly falsified shipping documents and invoices.
to misstate the contents and value of packages in order to deceive customs and shipping officials about the true nature of packages leaving the United States.

Akhtar will face trial and up to five years in prison for conspiracy to commit export violations, 20 years for unlawfully exporting U.S. goods, and 20 years for conspiracy to commit money laundering.

Of seven total alleged export control violations, four instances of alleged illicit trade are detailed below.

**Case 1: Domestic Company Allegedly Used as Front**

In October 2005, Akhtar allegedly obtained 100 dosimeters, a dual-use good used for radiation detection, from a U.S. company based in North Dakota on behalf of the Chashma nuclear power plant. Akhtar’s attempted procurement was directed by one of the Pakistani individuals whose names are redacted from the indictment. The individual instructed Akhtar not to inform the company about the end destination. Akhtar approached the North Dakota company stating he was seeking dosimeters from a company in the country of Georgia. The North Dakota company asked for the end-user information for the dosimeters and advised Akhtar that if the goods would go overseas or were destined for a nuclear plant, Akhtar would need to contact the Georgian company directly. Akhtar reported back to a Pakistani associate that he was having difficulty obtaining the dosimeters in the United States. In February 2006, an associate replied that Akhtar should try to buy the dosimeters in smaller quantities, such as 40 to 50 units at a time, and use different buyer names.

At this point, it appears that Akhtar gained the cooperation of a wireless company in Illinois to act as a middleman to front the purchase of dosimeters from the North Dakota company. The indictment does not indicate that the company was an entity owned or set up by Akhtar. In May 2006, Akhtar allegedly sent $5,000 to the wireless company for future purchases of dosimeters. That month, a Pakistani associate sent a letter to CNPP thanking them for their order and notified them that they should expect dosimeter deliveries in batches of 100 units. Chashma agreed to pay $330.75 per unit for a total of 300 units. In June, Akhtar allegedly transferred an additional $10,000 to the Illinois wireless company. A Pakistani associate instructed Akhtar to invoice future shipping expenses and to have the dosimeters sent to a “business associate” in Dubai.

In July, Akhtar allegedly sent a transfer of $30,350 to the Illinois company. The company allegedly then purchased 100 dosimeters from the North Dakota company for $282 per unit. Akhtar allegedly stated to the Pakistani individual a few days later that he would ship the 100 dosimeters to Dubai. In October 2006, Akhtar allegedly instructed the Illinois company to purchase an additional 200 dosimeters. Akhtar allegedly shipped the goods via a Virginian freight forwarder to Dubai with a false invoice attached stating the contents were digital calculators. A company called Shairook Scrap USP LLC received the goods in Dubai. In August, a Pakistani associate sent an e-mail to another business associate in Pakistan stating that he had possession of the dosimeters.

In September, a Pakistani associate instructed Akhtar to buy an additional 200 dosimeters. Akhtar allegedly transferred $25,000 to the Illinois company. In October, the Illinois company allegedly purchased 52 units and then another 74 units for $315 apiece. In November, the company allegedly purchased an additional 74 units for $307 each. That month, Akhtar allegedly shipped these units to
Dubai via the Virginia freight forwarder, marked with a false invoice indicating the contents were digital pagers.

**Case 2: Contractor of Domestic Company Used to Obtain Goods**

In December 2005, a Pakistani associate contacted Akhtar to let him know that he had a tender for nuclear-grade resins manufactured by a Pennsylvania company and directed him to obtain pricing information. In February 2006, the company asked about the end-user of the resins and noted that anything going to Pakistan would require a U.S. government license. A Pakistani associate instructed Akhtar to obtain a new price quote for the resins, but to change the quantities and add in “a few other non-nuclear resins.” That same day, Akhtar contacted the Illinois wireless company and asked it to request the quote. Later in March, a Pakistani associate warned Akhtar that they would be held responsible for the “stoppage of the plant” if the nuclear grade resins were not soon obtained.

A Pakistani associate e-mailed a business partner in Dubai to ask him to find a trading company they could use to import “chemicals” for re-export to Pakistan. The Dubai associate informed Akhtar that he would need to handle the sale directly with the Pennsylvania company, including pricing and shipping, for receipt by Bosfor General Trading in Dubai. In May, Akhtar allegedly placed an order with a contractor (name redacted) of the Pennsylvania company for the resins at a cost of $1,112.50. The indictment does not indicate whether this contractor was located in the United States or abroad. Akhtar allegedly sent five drums containing 25 cubic feet of NRW100 resin to Bosfor General Trading in Dubai via the Virginia freight forwarder, with a false invoice stating the contents were “resin for water purification.” The drums were ultimately sent to CNPP with a Pakistani associate urging the Dubai partner to ship them by the “fastest means” possible and remove all the original invoices.

In May 2006, Akhtar allegedly placed another order with the Pennsylvania company’s contractor for 50 cubic feet of NRW100 resin and 50 cubic feet of NRW400 resin for a total of $9,475. In June, Akhtar allegedly made the payment to the Pennsylvania company. A Pakistani associate directed Akhtar to have the shipment sent to Shairook Scrap USP LLC in Dubai. Akhtar allegedly shipped the drums to Dubai listed as “resin for water purification w-100” on the shipping invoice and valued only $600. A Pakistani associate instructed the Dubai partner to transship the goods to CNPP in Pakistan. Apparently the order was not entirely filled to Chashma’s specifications, requiring the Pakistani to apologize that the order was short, which he described as being due to the difficulty of obtaining goods “for nuclear application.”

**Case 3: U.S. Company Makes a Bad Sale**

In March 2007, a Chashma representative asked a Pakistani associate to obtain a price quote for a MPC 9300 manual alpha-beta counting system, which is a dual-use good used to detect radiation. A Pakistani associate instructed Akhtar to obtain a quote and noted that Akhtar had been asked to “accept all penalties in case of default.” He suggested that Akhtar place the order with a five percent advance and to use “probing tactics” to weigh the manufacturer’s “reaction.” Meanwhile, the Pakistani associate warned the CNPP representative that alpha-beta systems were considered “nuclear accessories” and that using a public advertisement process would “adversely affect” their “procurement plans.”
A Pakistani associate later sent a price quote of $73,565 to the CNPP representative. In July 2007, Akhtar allegedly e-mailed a company in Tennessee with the credit card information of a United Kingdom billing address to cover a $5,000 down payment for 2 alpha-beta counting machines and accessories. In September, Akhtar allegedly told the Tennessee company that the buyer of the systems (a company whose name has been redacted from the indictment) would be leasing the systems to SUPARCO in Pakistan. The Tennessee company responded that an export license and end-user information would be required.

In January 2008, Akhtar allegedly transferred $28,750 to the Tennessee company for the two machines at a total price of $33,750 and the company issued an invoice noting the sale to CC-USA of Maryland. The invoice itself allegedly stated that the end-user was PIEAS. The end-user certificate was signed by the Chashma representative, who was representing himself as the head of procurement for PIEAS. Akhtar allegedly created a false invoice for the sale of the goods to Shairook Scrap USP LLC in Dubai, worth $1,000, and described as the actual contents. In May, the CNNP representative advised Akhtar of receipt of the goods.

**Case 4: U.S. Commerce Department Official Questions Akhtar about Export**

In September 2007, a Pakistani associate asked Akhtar to obtain price quotes from a company in Texas for 3M abrasive sheets, controlled for their dual-use applications in refinishing valve surfaces and other equipment which requires high tolerances. A Pakistani associate soon notified CNPP that the 3M abrasive sheets would cost $15,978. In January and February 2008, respectively, Akhtar allegedly sent two transfers from CC-USA to the Texas company of $3,050 and $4,051.48. Akhtar allegedly placed an order specifying shipment by sea to Shairook Scrap USP LLC in Dubai via the Virginia freight forwarder. The false invoice allegedly claimed the shipment contained 3 boxes of 3M abrasive at a cost of $150.

In April 2008, Akhtar was contacted by a Department of Commerce Special Agent via e-mail regarding the end-user of the 3M abrasive sheets. A Pakistani associate provided a false answer for Akhtar to give to the agent. Akhtar allegedly responded to the agent’s e-mail by saying that the end-user of the sheets, which were still awaiting shipment at the Virginia freight forwarder, was “Karachi Shipyard and Engineering Works Machine Shop.” In May, the goods left Virginia and were received by CNPP.

**Findings and Lessons**

This case study shows the importance of improving government/industry cooperation and information sharing to detect procurement attempts and schemes in the United States. Both industry and government experience difficulty in detecting experienced procurement operations backed by national smuggling operations, such as those employed by Pakistan. The U.S. government needs to be more open with U.S. suppliers of dual-use goods, warning them about procurement schemes and providing the names of suspicious trading companies. Companies need to be more proactive in forwarding suspicious enquiries to the U.S. government. Thwarting the elaborate means used to obtain these goods rests heavily on supplier vigilance and due diligence in investigating suspicious buyers. Increased cooperation could also allow the U.S. government to draw out cooperation from companies that are “on the fence” about whether they want to provide information about suspicious enquiries.
This case study shows that it can take years for a network to make a mistake that authorities find suspicious enough to investigate, leading to the busting of the network. This alleged Pakistani network’s use of false shipping labels and monetary declarations and its classic transshipment scheme using Dubai prior to Dubai’s implementation of export control laws made its activities opaque to enforcement officials for some time.

In the cases described above, closer government/industry cooperation could have thwarted these successful procurement attempts.

The first case involving Akhtar’s alleged use of the Illinois company to procure goods for Pakistan, thus avoiding the need to obtain an export license for a domestic sale, could have been avoided if the North Dakota supplier recognized that an earlier attempt to procure dosimeters was suspicious. It should have investigated much more fully the Illinois company’s alleged attempt just a few months later. If it were communicating regularly with the U.S. government, the government would have likely investigated this sale and advised against it.

In the second case, a thorough internal compliance investigation on the part of the Pennsylvania company into the contractor’s intended sale could have led to suspicions about the sale and the passing of this information to the U.S. government. At the same time, the U.S. government should develop a procedure to tip companies about suspicious trading companies, as is done in Britain and Germany.

In the third instance, the Tennessee company obviously made an unwise sale, since it sold goods to what it believed was a procurement division of PIEAS. This entity is on government warning lists. Enhanced U.S. government/industry cooperation would have likely ensured that the company knew it was about to commit a violation of dual-use export control laws. Although the actual end-user was CNPP, the company should have known that sales of a nuclear dual-use good are also illegal to PIEAS.

It is also intriguing that the Chashma representative chose to list PIEAS instead of CNPP as his identifying information on the end-user certificate. PIEAS has historically been involved in Pakistan’s nuclear program. This information is publicly available, but not common knowledge. This highlights the fact that governments often possess the type of knowledge that would be helpful to a company in identifying suspicious requests.

This case shows that some companies are still willing to risk doing business with illicit procurement networks despite the costs of getting caught. It also highlights a fundamental problem in the U.S. system—companies are expected to perform investigations of end users without the resources of the U.S. government to assist them. The U.S. government does not provide updated lists of trading companies to avoid, for example. Instead, penalties against U.S. companies have grown larger in the United States as they make mistakes about end users, while companies’ mistrust of the government’s motivations for communicating with them chills their willingness to come forward with important procurement information that could help the government stop future inadvertent sales to illicit nuclear procurement networks.

Finally, this case study shows that Pakistan remains an active procurer of nuclear dual-use goods and utilizes highly sophisticated networks to obtain what it needs. This case reveals that Pakistan also appears to hold or threaten to hold its procurement agents accountable for delays and failures to
obtain needed goods, a sign of how confident Pakistan appears to be in obtaining goods despite knowing that its agents are violating U.S. laws.

Pakistan publicly claims to be a responsible nuclear nation and says it wants a civilian nuclear trade deal as a result. Yet, its illicit nuclear procurement efforts remain steadfast and belie its claims of acting like a responsible nation. As an ally, the United States should insist that Pakistan stop its illicit nuclear trafficking activities and prove it is truly committed to global non-proliferation norms and laws.