Office of Intelligence and Analysis
Homeland Security

Federal Bureau of Investigation

Joint Homeland Security Assessment

(U) Recent Terrorist Plots Highlight Insider Threat

7 August 2007

(U//FOUO) Prepared by the DHS/Critical Infrastructure Threat Analysis Division and the FBI/Threat Analysis Unit.

(U) Key Findings

(U//FOUO) Information from several recent planned or thwarted terrorist plots shows the importance of the use of insiders to gain access to targets and collect preoperational information.

— ***(U//FOUO) Al-Qa'ida planner Dhiren Barot, whom UK authorities arrested in 2006, had tasked a member of his group to secure employment at a hotel in the United Kingdom to learn how to deactivate fire and security systems.***

— ***(U//FOUO) Russell Defreitas[USPER], the alleged mastermind behind the plot discovered this year to explode jet fuel pipelines at John F. Kennedy (JFK) International Airport, had been a cargo handler at the airport. Defreitas used his job-related knowledge to conduct surveillance and plan the attack.***

— ***(U//FOUO) The group that planned to attack military personnel on Fort Dix, New Jersey earlier this year used a family member's pizza restaurant to gain access to the post in 2006 and conduct preoperational surveillance.***

(U) Recent Plots Underscore the Insider Threat

(U//FOUO) The best example of the potential insider threat is the self-proclaimed "sleeper cell" of al-Qa'ida operative Dhiren Barot. He and his group of six men were sentenced in June 2007 to a combined 136 years in UK prisons for assisting in planning attacks in the United Kingdom and on U.S. targets in New York City, New Jersey, and Washington, D.C.

(U//FOUO) Barot's Use of Insiders

(U//FOUO) Barot's associates had a range of roles and responsibilities in their plotting against U.S. and UK targets, several of which involved taking advantage of employment opportunities to gain insider knowledge that would be useful for carrying out the plots.

— (U//FOUO) Omar Rehman was tasked with learning how to disable fire and security systems. He found a job at a hotel in Watford, England and police believe he used his time there to research how to disable the hotel's systems. At Rehman's home investigators discovered plans of a security system and diagrams showing the position of security guards, although DHS does not know if these plans were a direct result of his employment at the hotel.

— (U//FOUO) Junade Feroze owned a commercial garage in Blackburn, England that he could use to dispose of cars and obtain tires and gas canisters which figured prominently in the attack plans, according to a British Broadcasting Company report. Feroze's ownership of the garage—while not a specific example of an insider threat—illustrates the potential for an employee to use access to such a facility to acquire materials to support an attack plan.

— (U//FOUO) Mohammed Naveed Bhatti, who has a degree in engineering, was found with an advertisement for a tanker driver—possibly indicating that the plotters hoped he could obtain a job as a tanker driver. The use of a tanker as a vehicle-borne improvised explosive device figured in the terror conspiracies.

(U//FOUO) JFK Plot Leader a Retired Airport Employee

(U//FOUO) The arrests in the disrupted JFK International Airport and Fort Dix plots show similar insider patterns and tactics. On 1 June 2007 FBI and Trinidadian authorities disrupted a plot by Islamic extremists to attack the JFK airport jet fuel storage and pipeline systems. Defreitas—the alleged mastermind behind the plot—was arrested in New York by FBI authorities; while two other suspects, Kareem Ibrahim and Abdul Kadir, were taken into custody by Trinidadian authorities. The fourth suspect, Abdel Nur, turned himself into Trinidadian authorities on 5 June 2007.

(U//FOUO) Defreitas worked as a cargo handler at the airport until he retired in 1995. In a recorded conversation Defreitas confided to an FBI informant that his "unique knowledge of the airport" as a former cargo worker would help him launch a terrorist attack surpassing the magnitude of the 11 September 2001 attacks.

— (U//FOUO) Since Defreitas retired, however, airport operations have changed and security has tightened significantly, leaving his assumed knowledge of airport operations highly dated.

— (U//FOUO) Defreitas explained he previously had been able to access restricted areas while visiting friends who worked at the airport, but that now identification was needed.

(U//FOUO) Fort Dix Planning Centered on Insider Knowledge

(U//FOUO) On 7 May 2007 Mohamad Shnewer[USPER], Serdar Tatar[USPER], and illegal alien brothers Dritan, Shain, and Eljvir Duka were arrested on charges related to their plans for a terrorist attack against Fort Dix. The suspects intended to acquire firearms and mount an attack against a concentration of soldiers on the post. The attack plan apparently called for a hit-and-run strike, with the suspects intending to escape afterward.

— (U//FOUO) The terrorist operatives used a nearby restaurant as cover for their surveillance. Recorded conversations revealed that Tatar delivered pizzas to Fort Dix from a pizzeria his family owned near the post.

— (U//FOUO) The six men showed interest in other East Coast military installations, but settled on Fort Dix largely because Tatar was familiar with the post.

(U) Suggested Actions to Reduce the Insider Threat

(U//FOUO) To mitigate the potential insider threat, DHS and the FBI recommend that facilities incorporate potential indicators of insider threat into workplace awareness and training activities. Certain behaviors may signify that an individual may be collecting information for criminal purposes. Not all behaviors are actionable, but when combined they could indicate a threat. Some examples of indicators are:

— (U//FOUO) Questions from employees that appear outside their realm of responsibility.

— (U//FOUO) Attempts to enter restricted areas without proper credentials.

— (U//FOUO) Unexplained or excessive copying of files—particularly blueprints of buildings or systems such as security and fire suppression.

- (U//FOUO) Improper use of information technology systems or repeated attempts to access restricted files.

- (U//FOUO) Requests for irregular work schedules or attempts to be left alone in a facility.

- (U//FOUO) Patterns of inaccurate statements or making excuses for irregular behaviors.

(U//FOUO) In addition, all personnel who require access to sensitive or restricted areas or information should be vetted with Federal, State, and local law enforcement authorities. This strategy will not necessarily uncover potential terrorists; however, it will ensure that employees do not have a prior criminal record.

(U//FOUO) By ensuring the use of proper credentials and using access controls—such as badges, biometrics, keypads, and swipe cards—employers can further control access to sensitive information and areas. Controls also are essential when managing the access of subcontractors and other non-employees. If access to restricted areas is necessary, these personnel should be escorted or monitored by a facility employee who is familiar with the area of the facility or system on which the non-employees are working.

(U) Reporting Notice:

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operation Center (NOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the NOC can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@hq.dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) **Tracked by:** HSEC-021500-01-05, HSEC-030000-01-05, TERR-050100-01-05, TERR-050200-01-05, TERR-050300-01-05, ESEC-010000-01-05