(U) FBI Tampa Division
National Security Threat Awareness Monthly Bulletin
OCTOBER 2011

(U) Administrative Note: This product reflects the views of the FBI-Tampa Division and has not been vetted by FBI Headquarters.

(U) Handling notice: Although UNCLASSIFIED, this information is property of the FBI and may be distributed only to members of organizations receiving this bulletin, or to cleared defense contractors. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

10 NOV 2011

(U) The FBI Tampa Division National Security Threat Awareness Monthly Bulletin provides a summary of previously reported US government press releases, publications, and news articles from wire services and news organizations relating to counterintelligence, cyber and terrorism threats. The information in this bulletin represents the views and opinions of the cited sources for each article, and the analyst comment is intended only to highlight items of interest to organizations in Florida. This bulletin is provided solely to inform our Domain partners of news items of interest, and does not represent FBI information.

In the OCTOBER 2011 Issue:

(U) NATIONAL SECURITY THREAT NEWS FROM GOVERNMENT AGENCIES:

(U) DSS Counterintelligence Directorate Releases Unclassified Publication, "Targeting US Technologies: A Trend Analysis Reporting from Defense Industry" (*19 OCT 2011, Defense Security Service*)

(U) The Defense Security Service (DSS) in October released its 2011 report that analyzes suspicious contact reports received from defense industry in fiscal year 2010. DSS supports national security and the warfighter through security oversight and education missions. It oversees the protection of US and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP) and serves as the DoD functional manager for education, training, and professional development of security professionals for the DoD, federal government, and industry.

(U) According to the 2011 report, "Targeting US Technologies: A Trend Analysis Reporting from Defense Industry" , the number of suspicious contact reports (SCRs) resulting from foreign attempts to obtain illegal or unauthorized access to sensitive or classified information and technology in the US cleared industrial base more than doubled from fiscal year 2009 (FY09) to FY10. The large scope and diversity of collection efforts targeting US technologies meant that foreign entities simultaneously directed considerable efforts at many technologies using variations of methods and collectors.

(U) Overall, the majority of collection attempts in FY10 originated from the East Asia and the Pacific region; commercial entities were the most active collector affiliation category for the second year in a row; targeting of information systems (IS) technology more than doubled from FY09; and collectors continued to most commonly use requests for information (RFIs) to elicit information from cleared contractors

(U) Collection MOs continue to span the range between the direct, immediate, and seemingly legitimate, such as RFIs; to the more indirect, more long-term, and more opaque, such as academic solicitation, seeking employment, and solicitation or marketing; to the often obscure suspicious network activity (SNA) that seeks to penetrate US industry networks

(U) The full report is available online at http://www.dss.mil/counterintel/2011-unclassified-trends.pdf

(U) Analyst Comment: All cleared defense contractor facility security officers, IT security specialists and executives should download and read this report. Anyone corporate security officer or manager in

Florida should also read this report to understand the types of technology being targeted by foreign collectors and the methods they are using to collect.

(U) COUNTERINTELLIGENCE/ECONOMIC ESPIONAGE THREAT ITEMS FROM THE PRESS

(U) White House Orders Agencies to Guard Data to Stop Next WikiLeaks Breach (*08 OCT 2011, Eweek)*

(U) The White House issued an executive order to put systems in place to protect classified government documents from a future WikiLeaks-style data breach. President Obama wants tighter information security measures to prevent another WikiLeaks-style breach. Obama signed an executive order outlining data security measures and rules for government agencies to follow to prevent further data leaks by insiders, the White House said Oct. 7. The executive order defines basic security measures to protect data as well as mandates the creation of committees to oversee the effort.

(U) Last November, anti-secrecy Website WikiLeaks started posting hundreds of thousands of United States diplomatic cables online, severely embarrassing the United States government. Shortly after the leak, the government ordered agencies to restrict the use of "removable media" such as CDs and USB flash drives on classified systems. "We are only as strong as our weakest link and this is a shared risk with shared responsibility," the White House said. The orders reinforce the rule that employees can't download private data to removable hard drives, require agencies to track what government employees are doing when accessing sensitive information, and define how information should be encrypted and secured.

(U) The national security team at the White House formed a committee and spent the past seven months reviewing and defining guidelines that would reduce the risk of a future breach. The newly signed executive order would coordinate implementing broad security measures across all agencies of the federal government, including the Federal Bureau of Investigation, Central Intelligence Agency and the Department of Defense. "The strategic imperative of our efforts has been to ensure that we provide adequate protections to our classified information while at the same time sharing the information with all who reasonably need it to do their jobs," according to a White House fact sheet on the executive order.

(U) The order included the creation of a senior steering committee that will oversee the safeguarding and sharing of information. While chaired by senior representatives of the Office of Management and Budget and the National Security Staff, the technical safeguards will be created by the secretary of defense and the director of the National Security Agency. The intra-agency Insider Threat Task Force will establish policies and evaluate efforts to detect and deal with government employees and military personnel who may be at risk of leaking classified information. The attorney general and the director of national intelligence will lead the task force. The executive order also required the steering committee to submit a report to the president within 90 days on how the new measures are working or failing at protecting classified data. The committee will also issue follow-up reports at least once a year to keep track of successes and failures.

(U) US Army Sgt. Bradley Manning is suspected of copying secret documents from classified databases onto a CD masquerading as a Lady Gaga music CD. Security experts noted that a low-ranking intelligence analyst such as Manning should not have had access to these sensitive documents on the military's classified network in the first place. WikiLeaks initially posted the documents with potentially vulnerable names redacted, but dumped the full archive of 251,000 diplomatic cables online last month when reports emerged that the documents were available on file-sharing sites.

(U) US Army Soldier Arrested in Alaska in Espionage Probe (*Reuters, 01 NOV 2011; The Army Times, 29 OCT 2011*)

(U) A soldier stationed in Alaska was arrested in late October on suspicion of espionage, according to an Army official. Specialist William Colton Millay, a 22-year-old military policeman from Owensboro, Ky., was taken into custody in October at Joint Base Elmendorf-Richardson by special agents from Army Counterintelligence and Army Criminal Investigation Command. The FBI and Army Counterintelligence are continuing to investigate Millay, assigned to the rear detachment of the 164th Military Police Company, 793rd Military Police Battalion, 2nd Engineer Brigade. The unit, known as the Arctic Enforcers, deployed to Afghanistan in the spring without Millay.

(U) An Army spokesman did not say who Millay, of Owensboro, Kentucky, was suspected of spying for or what sensitive information he may have had access to. He said the investigation was ongoing. An FBI spokesman said the case would be tried in military courts. He also said the arrest was not related to the WikiLeaks case, in which US Army Private Bradley Manning is charged with downloading more than 150,000 diplomatic cables and passing some of them to Wikileaks while working as an intelligence analyst in Iraq. "It's unrelated, forget WikiLeaks," the FBI spokesman told Reuters.

(U) "Today's arrest was the result of a close working relationship between the FBI and its military partners in Alaska," the special agent in charge of the FBI in Alaska, said in a brief written statement. "Through this ongoing partnership, we are better able to protect our nation." Joint Base Elmendorf-Richardson is a combined Army and US Air Force facility near Anchorage.

(U) Suspected Russian Spies Arrested in Germany, Reportedly Identified Through FBI Investigation and Arrest of Russian Spies in New York and New Jersey (*22 OCT 2011, Deutsche Welle; Der Spiegel, 25 OCT 2011*)

(U) Special police units in Germany have arrested a married couple suspected of working for the Russian Foreign Intelligence Service (SVR) for more than 20 years. Two weekly German news magazines, Spiegel and Focus, reported in October that the woman of the couple was arrested in Marburg, in the state of Hesse, while listening to coded news via a radio receiver. Her husband was arrested in the town of Balingen in the state of Baden-Württemberg.

(U) According to the reports, the two entered Germany via Mexico with false papers in 1990 and spent years sending coded messages to Russian Intelligence using a shortwave receiver. If the date is correct, it would mean they began their activity in the last years of the Soviet-era KGB internal security agency. The KGB was remodeled after the fall of the communist regime into the Federal Security Service (FSB) and the SVR. Unlike the FSB, the SVR deals in international, and often industrial, espionage. The man in this case is a mechanical engineer who is said to have worked for a supplier of spare parts for cars and spied on the company.

(U) The two were reportedly exposed last year when the American Federal Bureau of Investigation (FB) broke a network of SVR agents and arrested at least one other Russian spy, with whom the German pair had apparently had contact. A 2010 federal intelligence report suggested Russia and China had the biggest active spy networks in Germany, though they focus on industrial, rather than state, espionage. Russia's SVR runs an estimated 13,000 agents and is active in economic areas, science and technology, the report says. The SVR is thought to focus on gathering information about propulsion systems, satellites, sensors and communication technology.

(U) The Marburg arrest is the culmination of a secret, weeks-long effort by German security authorities to hunt down suspected Russian agents. It was an operation straight out of the annals of the Cold War. Heidrun A., 45, and her husband Andreas, 51, (their surname is reportedly Anschlag) are suspected of having spent over 20 years as undercover agents spying on Germany for Moscow. The spy thriller could hurt relations between Germany and Russia. This is the first arrest of "illegal" Russian agents in Germany since reunification in 1990. "Illegals" practice a high art of spycraft. These weren't standard agents masquerading as diplomats operating from an embassy and immune from prosecution. The worst such diplomatic spies have to fear is expulsion from Germany. But the married couple recently arrested can expect a long jail sentence. A spectacular trial resulting in a conviction could lead to a marked cooling in diplomatic relations between the two countries.

(U) Spying During Berlin Wall Era

(U) Officially, Chancellor Angela Merkel likes to stress that German-Russian relations are excellent. "They have broadened in recent years, and some haven't kept up," she said last year. Russian President Dmitry Medvedev has gushed that "Germany is our key country." That obviously also applies to secret service activity. The German Federal Prosecutor's Office and the Federal Office for the Protection of the Constitution, which is Germany's domestic intelligence service, say the undercover operation by the married couple from Marburg began before the fall of the Berlin Wall in 1989, in the days of the Soviet KGB.

(U) In 1988, Andreas A. moved to Germany, a young man who said he was born in Argentina and raised in Austria and who wanted to study in Germany. In 1990 he married his partner, Heidrun, who presented a similar CV, born in Peru, Austrian citizen. Andreas studied engineering and plastics technology in Aachen. The couple soon had a daughter. In 1998, after he had completed his studies, Andreas joined an auto components manufacturer. He changed jobs several times and the family moved to North Rhine-Westphalia and then to Rhineland-Palatinate. Early this year Andreas joined a company in the southwestern town of Balingen as a project manager. Sometimes he commuted the 360-kilometer distance to Marburg, sometimes he spent weeknights in an apartment close to his work. Police arrested him in that apartment. He seemed to be living the ordinary, inconspicuous life of an employee who has to commute long distances to and from work.

(U) Similarities With Anna Chapman Case

(U) His life was as unspectacular, in fact, as that of Anna Chapman, who has more in common with Andreas and Heidrun A. than would seem apparent at first sight. The photogenic Russian with red-dyed hair was part of a spying ring of 11 illegal agents uncovered in the United States in June 2010. Some of the Russians had spent over a decade working for the SVR. Their headquarters had been especially interested in reports about US foreign policy. The agents communicated with messages written in invisible ink and coded statements such as, "Tell him Uncle Paul loves him," and "He will know it is wonderful to be Santa Claus in May."According to an encrypted message from Russia retrieved by US officials, one agent was told: "You were sent to the USA for long-term service trip. Your education, bank accounts, car, house, etc. -- all these serve one goal: Fulfill your main mission, i.e. to search and develop ties in policymaking circles in US and send intels (intelligence reports) to C(enter)."

(U) A few days before the FBI pounced in the summer of 2010, a Russian intelligence officer defected to the United States. He was believed to have been working for the CIA since 1999: Alexander Poteyev, one of the officers handling the team of agents on the US east coast. Poteyev is believed to have betrayed Chapman and Co: a Moscow court has sentenced him in absentia to 25 years in jail. He didn't just offer the Americans information on the 11 agents but also gave them deep insight into the workings of Moscow's "Illegals" program -- including the rumor that a similar group of agents was also operating in

Europe. The longer German counter-intelligence agents spent looking at the Chapman case and at further information, the clearer the picture became. They concluded, based on radio messages to Germany, that at least one, and perhaps several Russian spy couples were living in Germany. In late summer the trail of clues led them to the Marburg home of Andreas and Heidrun A.

(U) Incriminating Evidence

(U) Time seemed to be running out for the investigators. Andreas had already resigned from his job, sold his car and was packing up to leave Germany, saying he could earn more money abroad. The German authorities suspected that the couple wanted to make a getaway, and that the SVR headquarters might have known that the agents were close to being caught. It is not clear if Heidrun and Andreas A., as with Chapman and her colleagues, focused on foreign policy. Alongside the agent radio which they both regularly received, another incriminating fact is the false information on their Austrian passports. Inquiries in Argentina and Peru showed that the places of birth listed were not correct. In addition, Andreas A., who said his hobbies were travel, walking and deep sea fishing, speaks with a detectable Russian accent, although, according to his own information, he only speaks German, Spanish and English.

(U) Experts believe it is possible that the couple used Germany as a base but operated elsewhere in Europe. Another theory is that they were in contact with other agents and acted as a relay station for information to Moscow. During the investigation, specialists from the Federal Criminal Police Office (BKA) used a mobile X-ray laboratory to locate cavities possibly used to hoard secret documents: Even a tennis racket was X-rayed.

(U) 'An Interesting and Bright Life'

(U) The case could go down in legal history. Under German law, it is only punishable to work for a foreign intelligence agency against Germany. The question is, whether, in the context of the European Union, Germany's interests would be damaged by an agent using Germany as a base to operate in a nearby country. For the federal prosecutor, this will determine whether the case will end in failure or be a big success, like the Anna Chapman case. In the high-profile Chapman case, the FBI could not prove that the Russian and her agent friends were involved in spying. Instead they were charged with money laundering and conspiracy. But after the arrest, the Kremlin admitted they were Russian citizens. In true Cold-War style, the agents were exchanged for four alleged CIA spies who had spent years in Russian prisons.

(U) After their return Vladimir Putin lauded the risk that they had undertaken. "Just imagine ... You have to master a foreign language as your own, think and speak it and fulfill tasks in the interest of the motherland for many years without counting on diplomatic immunity," he said. Speaking about the spies arrested in America, Putin made a promise which will also be of interest to Andreas and Heidrun A.: "I am sure that they will have an interesting and bright life."

(U) Analyst Comment: This report highlights the continuing threats to the US government and industry from Russian intelligence collection. Russia continues to use “Cold War” collection methods like illegal agents who create false identities in a target country, in addition to asymmetric methods such as tasking legitimate visitors like students and business delegations to collect information.

(U) Suspected Russian Spy Tries to Stop Her Deportation from Britain; Admits Affair with Member of Parliament but Denies Espionage (*Associated Press, 18 OCT 2011; SkyNews, 19 OCT 2011*)

(U) An accused Russian spy who worked as an assistant for a British lawmaker went to court in October in a bid to block her deportation, telling judges that she had a four-year affair with her boss but was not a secret agent. Ekaterina Zatuliveter, also known as Katia, was arrested in December, 2010 on suspicion of using her job in the office of legislator Mike Hancock to pass information to Russian intelligence. She was not charged, but British authorities want to deport her as a danger to national security. Zatuliveter denies spying and is asking the Special Immigration Appeals Commission to block her extradition. The case, expected to last nine days, is being heard by three judges and a former head of the MI5 intelligence agency. Hancock, a Liberal Democrat member of Parliament who sits on the House of Commons Defense Committee, has said 26-year-old Zatuliveter worked as a researcher in his office for 2½ years, but was not involved in sensitive matters. In a statement he said that "at no time, did I pass on to Ms. Zatuliveter any information that was not in the public domain or any classified information."

(U) Zatuliveter said she met Hancock in Moscow in 2006 and they began an affair that continued when she moved to Britain to study. But she denied an allegation by Jonathan Glasson, a lawyer for the British government, that she had targeted Hancock because he was influential in British politics. "I don't think that he is very influential," she said. "He is a backbench MP." Asked why she thought Hancock would be of interest to Russian spies, she replied: "I have no idea what would be of interest to the Russian Intelligence Service." Glasson, acting on behalf of the Home Secretary, said she targeted the Portsmouth South MP because she thought his well-publicized extra-marital affairs made him "potentially vulnerable". It is claimed she was interested in Mr. Hancock because he sat on the Commons defense committee, chaired the all-party Russian group and represented an area with a Royal Navy base. Miss Zatuliveter's access meant "Russian intelligence had eyes and ears in the House of Commons", the Special Immigration Appeals Commission was told. Zatuliveter acknowledged she had a four-year relationship with Mr. Hancock as well as liaisons with a NATO official, a Dutch diplomat and someone who worked for the United Nations. She told the officers about a man from the Russian embassy, referred to as Boris, and said she scribbled "KGB" on the business card he gave her because there were rumors he was a spy. But the former MP's assistant denied the accusation she met him in Parliament in 2008. 'Boris' has since been expelled from the country. The UK agents also asked her about her relationship with 'Y', the NATO official, which began when she ended her affair with Mr. Hancock last April. They confronted her about an email to him regarding a NATO meeting and the former US Secretary of State Madeleine Albright.

(U) Zatuliveter denies the claims Mr. Hancock met her when she was a student at a conference in Russia in 2006. Diary entries from the time, which noted her "strong personal feelings" for him, were handed to the judges. When she arrived in Britain to study, she worked as an unpaid intern in Mr. Hancock's office before becoming a full-time researcher in 2008. She then moved into his London flat. She denied knowing Mr. Hancock had affairs and said she believed he was divorced, only discovering he was still married in 2010. Her lawyer said it was common for young Russian women to fall for older men because "in Russia many young men are undesirable alcoholics".

(U) Zatuliveter said she was first questioned by British intelligence officials in August 2010 when she was asked how she could afford her London apartment on a researcher's salary. She said she replied that Hancock helped her out financially. Hancock, 65, who is married with two children, said in his statement that it was "not appropriate for me to make any further comments at this time on any aspect of the hearing." Russia's Foreign Ministry has dismissed the spying accusations as "paranoid" and an attempt to undermine U.K.-Russian relations. Those relations have been chilled since the death in 2006 of Alexander Litvinenko, a former KGB officer who died after ingesting a radioactive substance. Litvinenko blamed Russian President Vladimir Putin for the poisoning.

(U) New York Resident and His Company Plead Guilty to Conspiracy to Export Computer-Related Equipment to Iran (*Department of Justice Press Release, 07 OCT 2011*)

(U) Jeng "Jay" Shih, 54, a US citizen, and his Queens, N.Y., company, Sunrise Technologies and Trading Corporation, pled guilty in October in the District of Columbia to conspiracy to illegally export US-origin computers from the United States to Iran through the United Arab Emirates (UAE). At a hearing before a US District Judge, Shih and his company each pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States. The maximum sentence is five years in prison and $1 million in criminal fines. Sentencing has been scheduled for Jan. 13, 2012. Under the terms of the plea and related civil settlements with the US Department of Commerce's Bureau of Industry and Security and the Office of Foreign Assets Control (OFAC) Shih and his company have agreed to forfeiture of a money judgment in the amount of $1.25 million. In addition, Shih and Sunrise are denied export privileges for 10 years, although this penalty will be suspended provided that neither Shih nor Sunrise commits any export violations.

(U) Shih was arrested on a criminal complaint on April 6, 2011. He and his company were later indicted on April 21, 2011. According to court documents filed in the case, beginning as early as about 2007, Shih conspired with a company operating in Dubai, UAE, and Tehran, Iran, to procure US-origin computers through Sunrise and export those computers from the United States to Iran, through Dubai, without first obtaining a license or authorization from OFAC. Specifically, in April 2010, the defendants caused the illegal export of 368 units of computer-related goods to Dubai, which were later sent to Iran. Later that month, the defendants caused the illegal export of 158 additional units of computer-related goods to Dubai, which were later sent to Iran. The defendants subsequently caused an additional 185 units of computer-related goods to be illegally exported to Iran via Dubai.

(U) This investigation was conducted by the ICE-Homeland Security Investigations (HSI) field offices New York and San Diego and the Department of Commerce Office of Export Enforcement field offices in New York and Los Angeles, with assistance from ICE-HSI offices in Chicago, Newark, N.J., Los Angeles and Orange County, Calif. The Department of Homeland Security's US Customs and Border Protection and OFAC's Office of Enforcement also assisted in the investigation.

(U) Analyst Comment: This report highlights the continuing efforts of Iran to collect information technology and electronics components in the United States. Companies in New Jersey that manufacture or distribute electronics technology should be aware of the threat that front companies based in the United States or locations like Hong Kong, the UAE, Singapore or other foreign countries may try to acquire this technology in the United States on behalf of Iran.

(U) Software Engineer Indicted for Theft of Globex Computer Trade Secrets While Allegedly Planning Business in China (*US Department of Justice Press Release, 28 SEP 2011*)

(U) A former senior software engineer for Chicago-based CME Group, Inc., was indicted in September for allegedly downloading and removing computer source code and other proprietary information while at the same time pursuing business plans to improve an electronic trading exchange in China. The defendant, Chunlai Yang, who was arrested in July, was charged with two counts of theft of trade secrets in an indictment returned by a federal grand jury. The indictment seeks forfeiture of computers and related equipment that were seized from Yang.

(U) "This case is an excellent example of how law enforcement and corporations can work together to protect trade secrets. CME Group brought this matter to the attention of federal authorities and fully cooperated with the investigation. Economic espionage is a crime that effects both the interests of corporations and our national interest in protecting intellectual property. We will continue to working collaboratively with the private sector to investigate and prosecute trade secret theft," US Attorney Patrick J. Fitzgerald said.

(U) According to the indictment, Yang began working for CME Group in 2000 and was a senior software engineer at the time of his arrest. His responsibilities included writing computer code and, because of his position, he had access to the software programs that supported CME Group's Globex electronic trading platform. Globex allowed market participants to buy and sell exchange products from any place at any time. The source code and algorithms that made up the supporting programs were proprietary and confidential business property of CME Group, which instituted internal measures to safeguard and protect its trade secrets.

(U) Between Dec. 8, 2010, and June 30, 2011, Yang allegedly downloaded more than 1,000 computer files containing CME computer source code from CME's secure internal computer system to his CME-issued work computer; he then transferred many of these files from his work computer to his personal USB flash drives; and then transferred many of these computer files from his USB flash drives to his personal computer located at his home. During the same time, Yang also downloaded and printed numerous CME internal manuals and guidelines describing how many of the computer files that comprise Globex operate and how these computer files interact with each other, the indictment alleges.

(U) Yang and two unnamed business partners, identified as Individuals A and B, allegedly developed business plans to form a business referred to as the Tongmei (Gateway to America) Futures Exchange Software Technology Company (Gateway), with the purpose of increasing the trading volume at the Zhangjiagang, China, chemical electronic trading exchange (the Zhangjiagang Exchange). The indictment alleges that Yang was to become Gateway's president, and he allegedly engaged in contract negotiations on behalf of Gateway with the Zhangjiagang Free Trade Board for Gateway to provide computer source code to the Zhangjiagang Exchange.

(U) Yang allegedly expected that Gateway would provide the Zhangjiagang Exchange with technology to allow for high trading volume, high trading speeds, and multiple trading functions. To help the Chinese exchange attract more customers and generate higher profits, Gateway proposed to expand the capabilities of Zhangjiagang's software by providing customers with more ways of placing orders; connecting the exchange's database storage system and matching systems; rewriting the trading system software in the JAVA computer programming language; raising the system's capacity and speed by modifying communication lines and structures; and developing trading software based on the FIX computer coding language, the indictment alleges.

(U) Chinese Nationals Sentenced 24 Months for Illegally Attempting to Export Radiation-Hardened Microchips to the PRC (*US Department of Justice Press Release, 30 SEP 2011*)

(U) Two Chinese nationals were sentenced to 24 months in prison in September for participating in a conspiracy to violate the Arms Export Control Act and smuggle radiation-hardened microchips from the United States for an agency controlled by the People's Republic of China (PRC) and responsible for the development of missiles and launch vehicles. "The line between traditional espionage, export violations and economic espionage has become increasingly blurred as the sensitive information sought by the PRC commonly has ramifications both economically and in terms of national security," said a US Attorney.

"Today's sentences should serve as a deterrent to anyone who might seek to illegally obtain sensitive information for the PRC. The person they are dealing with may turn out to be a federal undercover agent."

(U) On June 1, 2011, Hong Wei Xian, a/k/a "Harry Zan," 32, and Li Li, a/k/a "Lea Li," 33, both from the PRC, pled guilty to conspiring to violate the Arms Export Control Act and to smuggle goods unlawfully from the United States. Xian and Li were officers of Beijing Starcreates Space Science and Technology Development Company Limited (Beijing Starcreates), which, among other things, engages in the business of importing and selling programmable read-only memory microchips to China Aerospace Science and Technology Corporation (China Aerospace). China Aerospace is controlled by the PRC government and plays a substantial role in the research, design, development and production of strategic and tactical missile systems and launch vehicles for the PRC.

(U) Since 1990, the US government has maintained an arms embargo against the PRC that prohibits the export, re-export, or re-transfer of any defense article to the PRC. Prohibited defense articles are placed on the United States Munitions List, which includes spacecraft systems and associated equipment. A programmable read-only memory microchip (PROM) serves to store the initial start-up program for a computer system and is built to withstand the conditions present in outer space.

(U) According to their guilty pleas, Xian and Li admitted that they neither applied for nor received a license from the United States to export defense articles of any description; however, from April 2009 to Sept. 1, 2010, the two contacted a company in the Eastern District of Virginia, seeking to export thousands of radiation-hardened PROMs from that company. Xian and Li knew a license was required, but did not seek to obtain one because it would have required them to identify the end user, their PRC-controlled customer, China Aerospace, and describe the end use that would occur on behalf of the PRC. To avoid drawing attention to the true purpose of their orders, the defendants conspired to break up orders into multiple shipments and designate countries outside the PRC for delivery.

(U) On Sept. 1, 2010, the defendants were arrested in Hungary pursuant to a United States provisional arrest warrant and transferred into the custody of US Marshals on April 1, 2011, after they waived extradition. In sentencing the defendants, Judge Lee expressly stated that he had already taken into account the time the defendants had spent in jail in Hungary, and that those seven months would not reduce the sentence imposed today. Effectively, then, the defendants' sentence was 31 months in prison.

(U) Analyst Comment: This case highlights the continuing threat of PRC acquisition of electronics components and technology in the United States. As China seeks to develop and expand its space program, aerospace and aeronautics capabilities, and military information technology industries, it will continue to attempt to acquire reliable, state of the art US electronics.

(U) Ex-Dow Scientist Admits to Economic Espionage (*Bloomberg, 18 OCT 2011; Associated Press, 18 OCT 2011)*

(U) **An ex-Dow AgroSciences LLC researcher pled guilty to economic espionage in connection with the theft of trade secrets from his former employer to benefit a Chinese university**, the US Justice Department said. Kexue Huang, 48, also admitted to stealing trade secrets from the Minneapolis-based grain distributor Cargill Inc. "Mr. Huang used his insider status at two of America's largest agricultural companies to steal valuable trade secrets for use in his native China," Assistant US Attorney General Lanny Breuer said in the statement. Huang entered guilty pleas today in two separate criminal cases before a US District Judge in Indianapolis. The total loss from the charges Huang pled guilty to came to $17 million, but a Justice Department spokesman said Huang was responsible for a total of $300 million in losses.

(U) Huang, who was born in China, worked for the Indianapolis-based unit of Midland, Michigan-based Dow Chemical Co., where he researched the development of organically derived pesticides, from 2003 to 2008. He then went to work for Cargill as a biotechnologist. Huang was indicted in June 2010 and charged under the Economic Espionage Act, which was passed in 1996 after the United States determined other countries were spying on private businesses. His was the eighth case nationwide under the 15-year-old law.

(U) From 2007 to 2010, Huang shared confidential information with at least two people, one of whom conducted research first at the Hunan Normal University in China and later in Dresden, Germany, according to a plea agreement that didn't name the people. In stealing, transferring and using Dow trade secrets, Huang "intended to benefit" Hunan Normal University and the National Science Foundation of China, according to the plea agreement. Each of those institutions is controlled by the Chinese government. After joining Minnetonka, Minn.-based Cargill Inc. in March 2008, Huang stole a key component to make a new food product and gave it to a student at Hunan Normal University in China.

(U) A Dow spokesman, said it can take more than 10 years for the technology Huang tried to obtain to reach the market. "Dow AgroSciences has analytical technology and processes in place to identify third-party product produced with proprietary technology stolen by Mr. Huang," the spokesman said in an e-mailed statement. Dow is strengthening security measures to protect its technology and seeking to ensure that counterfeit products derived from it never find a market, said Hamlin. The crime of economic espionage is punishable by as long as 15 years in prison, and trade-secret theft carries a maximum term of 10 years, the Justice Department said.

(U) Analyst Comment: This individual found guilty in this incident came to the United States to conduct legitimate research, but used his access to sensitive information to benefit a university in his native China. The compromise of this information cost a US-based company millions of dollars. US companies should be aware of this risk and ensure they have adequate safeguards in place to monitor who is accessing and working with sensitive, proprietary corporate information.

(U) Engineer Guilty in Software Theft; Passed American Superconductor Codes to Wind Turbine Company in China (*The Boston Globe, 24 SEP 2011; The Financial Times, 12 OCT 2011*)

(U) A court in Klagenfurt, Austria, found an engineer guilty of stealing wind turbine technology from American Superconductor Corp. and giving it to a Chinese turbine maker that is a former customer of the Devens, Massachusetts company. After a three-hour trial in September, Dejan Karabasevic, 38, was sentenced to one year in jail and two years probation for passing proprietary turbine control software to Sinovel Wind Group Co., based in Beijing. Karabasevic, who worked in American Superconductor's subsidiary in Austria, was also ordered by Klagenfurt district court officials to pay his former employer roughly $270,000 in damages. "I made the biggest mistake of my life,'' Karabasevic said before the jury began deliberations, "and I am deeply sorry for it.''

(U) American Superconductor is pursuing separate claims against Sinovel, which it believes is using the company's electronic software code illegally. "This sentence was an important first legal step for AMSC,'' said a company spokesman. "This individual's admittance of guilt and collusion with Sinovel demonstrates the strength of our commercial, civil, and criminal cases against Sinovel in China.''

(U) American Superconductor, which makes control systems and other advanced technologies for wind turbines and power utilities, began to suspect Sinovel of theft in June, when an American Superconductor crew inspecting turbines in China found an imperfect replica of its software in a Sinovel turbine. An investigation led American Superconductor officials to Karabasevic, who was arrested in Austria in July. Earlier this month, the company also filed suit against Sinovel, which denies any wrongdoing.

(U) According to an indictment filed in the public prosecutor's office in Klagenfurt, Karabasevic had developed "increasingly strong ties'' with Sinovel as the "result of numerous business trips to China.'' Karabasevic, the indictment states, was paid at least $20,700 to copy codes downloaded from American Superconductor's network, and use them to help Sinovel upgrade versions of the US company's software that he said the Chinese company had already "cracked.''

(U) In court, Karabasevic's lawyer said his client's actions stemmed from "frustration'' about a failed marriage, which had been strained by his trips abroad for work as a department manager involved in software development, followed by a demotion to the customer service department last year. Karabasevic believed he was undervalued at AMSC Windtec, the American Superconductor subsidiary in Klagenfurt, according to the lawyer.

(U) Karabasevic in April downloaded American Superconductor software to his notebook computer and transferred it to Sinovel using his Gmail account, said Thomas Liensberger, the state prosecutor in Klagenfurt. An attorney for American Superconductor, said there is evidence that Sinovel wooed Karabasevic by offering him an apartment, a five-year contract at twice his current pay, and "all the human contact'' he wanted, "in particular, female co-workers.'' The attorney said that American Superconductor now believes the theft of its software by Karabasevic was the catalyst that caused Sinovel, once its largest customer, to stop accepting shipments from the Devens company earlier this year.

(U) In addition to this intellectual property case, Sinovel, China's biggest wind turbine maker by number of turbines manufactured, has launched a $125m counterclaim against former supplier American Superconductor. Its move comes after American Superconductor launched five lawsuits and arbitration proceedings against the Chinese company in September, saying that it had breached contracts and stolen intellectual property. Sinovel asked an arbitration commission in Beijing to dismiss the claims that the US company had brought to the commission. Sinovel also said it was seeking Rmb799m ($125m) in compensation for economic losses, according to a statement to the Shanghai Stock Exchange.

(U) Sinovel was once American Superconductor's biggest client, accounting for over 70 per cent of the company's revenues last year. But earlier this year Sinovel stopped accepting contracted shipments of wind turbine components. The companies had several long-term supply contracts in place, and each side accuses the other of contractual violations. In September, American Superconductor started arbitration proceedings over the alleged contractual violations, asking for undisclosed damages, in addition to the lawsuits the US company has brought in Chinese courts. Sinovel says that it stopped accepting components shipments because of quality problems. American Superconductor has said in the past that between shipments that were not paid for and scheduled deliveries that were not accepted, it is owed about $250m.

(U) American Superconductor scored an initial victory in the dispute in a separate case in Austria, where a former employee recently confessed in court to selling commercial secrets to Sinovel for cash. The employee was sentenced to one year in jail and has been co-operating with prosecutors. Among the lawsuits brought by American Superconductor in Beijing, one is a criminal lawsuit against Sinovel staff who were allegedly involved in the events in Austria, according to the US company. The police bureau in Haidian, where Sinovel's offices are located, did not comment on whether it had opened an investigation

over the criminal allegations brought by American Superconductor. In China, after a criminal complaint is made, it may take the police one to two months to decide whether to accept the case, a spokesman for the Haidian police said.

(U) Open Source Center Report: Beijing Funded Huawei (*The Washington Times, 12 OCT 2011*)

(U) An unclassified, open source US intelligence report for the first time links China's largest telecommunications company to Beijing's KGB-like intelligence service and says the company recently received nearly a quarter-billion dollars from the Chinese government. The disclosures are a setback for Huawei Technologies Co. Ltd.'s efforts to break into the US telecommunications market. The company has been blocked from doing so three times by the US government because of concerns about its links to the Chinese government.

(U) The report by the CIA-based “Open Source Center” (OSC) states that Huawei's chairwoman, Sun Yafang, worked for the Ministry of State Security (MSS) Communications Department before joining the company. The report on Huawei's board members states that Ms. Sun used her connections at MSS to help Huawei through "financial difficulties" when the company was founded in 1987. Based in part on Chinese media reports and Huawei's website, the report reveals that the Beijing government paid Huawei $228.2 million for research and development during the past three years. Huawei's links to the Chinese military have been disclosed previously. The Open Source Center (OSC) report provides the first details of its links to Chinese intelligence, which US officials have said has been engaged in a massive effort to acquire secrets and economic intelligence from government and private-sector computer networks around the world.

(U) According to US officials, senior Chinese government officials in recent months have pressed the Obama administration to allow Huawei to buy into the US telecommunications market. A spokesman for Huawei's US subsidiary, declined to comment on the report because the company has not seen it. But he said Ms. Sun's biography published in the company's most recent annual report "accurately describes her work experience." "Huawei only sells commercial-grade solutions, and our sales to the Chinese government account for less than 1 percent of our total sales," the Huawei spokesman said.

(U) The co-presidents of Huawei USA stated in a letter to The Washington Times last year that, despite US government allegations, Huawei is an "employee-owned" company, and China's government and military do not hold any shares or control the company. However, the Pentagon's latest annual report on the Chinese military said China's industry, including Huawei, is closely integrated with the military. "Information technology companies in particular, including Huawei, Datang and Zhongxing, maintain close ties to the PLA [People's Liberation Army]," the report says.

(U) The new OSC report, dated Oct. 5, says Chinese media reported that Huawei's senior leaders have "connections" to the PLA. Ms. Sun "used her 'connections' at the Ministry of State Security to help Huawei through financial difficulties 'at critical moments' when the company was founded in 1987," the report says, quoting an item by the pro-Beijing Hong Kong broadcaster Phoenix Satellite Television. The OSC report states that Huawei's 2010 annual report failed to mention that Ms. Sun, considered the most trusted aide to Huawei founder Ren Zhengfei, has ties to MSS, fueling suspicions of "potential close links between Huawei and the Chinese government."Mr. Ren was identified in the report as having worked for China's military from 1974 to 1983 in the engineering corps. The report says that Mr. Ren is purportedly China's most influential business leader "who seldom mentions his military background in public."

(U) In April, a publication sponsored by China's State Council newspaper reported that Huawei received $36.8 million and $63.2 million in 2009 and 2010, respectively, from the government for "domestic

development, innovation, and research." The company also received $48.2 million and $80 million in 2009 and 2010 for "completing certain research projects." The report contradicts past statements by Huawei officials that the company receives little or no government subsidies and instead relies on profits from its annual $28 billion in revenue for investments.

(U) Michelle K. Van Cleave, the former national counterintelligence executive and a senior counterspy policymaker, said China continues to view the United States as its main strategic enemy and is expanding aggressive intelligence operations here. "Big companies like Huawei are business giants, but they're also stalking horses for Chinese intelligence," Ms. Van Cleave said. "They can provide both cover and entree for intelligence operations." China's agents are targeting sensitive US technologies through lawful purchase, theft and guile, including acquisitions and investments, she said. "Two years ago, [Britain's domestic intelligence service] MI-5 warned that equipment installed by Huawei in British Telecom's networks could be used to disrupt critical services like power and transportation," Ms. Van Cleave said. "The same could be true here if we don't watch our backs."

(U) Kenneth deGraffenreid, former deputy national counterintelligence director, said China's strategic-technology acquisition efforts are similar to those used by the Soviet Union during the Cold War. "But unlike the Soviets, the Chinese use companies that appear on the surface not related to the government, but they are," Mr. deGraffenreid said. "All these Chinese companies are part of state ministries, MSS or [military intelligence], and have interlocking structures and personnel." Mr. deGraffenreid said the US government needs greater efforts to prevent strategic losses to China, including tighter technology controls and better counterspy activities.

(U) Huawei USA's first headquarters office was in Plano, Texas. Other Huawei locations in the United States include Chicago, Dallas, Denver, Philadelphia, San Diego and Seattle, as well as Santa Clara, Calif.; Walnut Creek, Calif.; San Antonio; and New Jersey.

(U) Taiwanese Deported from United States in Iran Missile Case (*Associated Press, 20 OCT 2011*)

(U) A Taiwanese man has been deported from the United States after serving prison time for illegally arranging shipments of parts to Iran that can have nuclear and military uses. US Immigration and Customs Enforcement officials say Yi-Lan "Kevin" Chen arrived in Taipei, Taiwan, on Wednesday. Chen spent almost two years in federal prison following his February 2010 arrest. Investigators say since 2007 Chen had put together at least 30 banned shipments to Iran. The parts included electrical connectors, detonators, small engines and seals that can be used for missiles and unmanned drones. Iran could also use some parts in its nuclear program. Court records show Chen falsely labeled the shipments as bound for Taiwan or Hong Kong. Chen pleaded guilty in May 2010 to conspiring to export banned items to Iran.

(U) Virginia Man Accused of Acting as Unregistered Agent of Syrian Government and Spying on Syrian Protestors in America (*US Department of Justice Press Release, 12 OCT 2011*)

(U) Mohamad Anas Haitham Soueid, 47, a resident of Leesburg, Va., has been charged for his alleged role in a conspiracy to collect video and audio recordings and other information about individuals in the United States and Syria who were protesting the government of Syria and to provide these materials to Syrian intelligence agencies in order to silence, intimidate and potentially harm the protestors. Soueid, aka “Alex Soueid” or “Anas Alswaid,” a Syrian-born naturalized US citizen, was charged by a federal grand jury on Oct. 5, 2011, in a six-count indictment in the Eastern District of Virginia. Soueid is charged with conspiring to act and acting as an agent of the Syrian government in the United States

without notifying the Attorney General as required by law; two counts of providing false statements on a firearms purchase form; and two counts of providing false statements to federal law enforcement.

(U) Soueid was arrested on Oct. 11, 2011, and will make an initial appearance before US Magistrate Judge Theresa C. Buchanan today at 2:00 p.m. If convicted, he faces a maximum penalty of 15 years in prison on the conspiracy and foreign agent charges, 15 years in prison on the firearms purchase charges and 10 years in prison on the false statement charges. "Our national security is threatened when foreign governments use unregistered agents in an attempt to influence and intimidate those who live here lawfully," said FBI Assistant Director in Charge McJunkin. "Their alleged acts desecrate the values cherished in our fair and open society. The FBI will be counted on to detect and deter unregistered agents who attempt clandestine activities on behalf of a foreign political power and work to bring them swiftly to justice."

(U) According to the indictment, since March 2011, Soueid has acted in the United States as an agent of the Syrian Mukhabarat, which refers to the intelligence agencies for the Government of Syria, including the Syrian Military Intelligence and General Intelligence Directorate. At no time while acting as an agent of the government of Syria in this country did Soueid provide prior notification to the Attorney General as required by law, the indictment alleges.

(U) Under the direction and control of Syrian officials, Soueid is accused of recruiting individuals living in the United States to collect information on and make audio and video recordings of protests against the Syrian regime – including recordings of conversations with individual protestors – in the United States and Syria. He is also charged with providing the recordings and other information to individuals working for the Mukhabarat. According to the indictment, Soueid and others conspired to use this information to undermine, silence, intimidate and potentially harm those in the United States and Syria who engaged in the protests.

(U) The indictment states that in late June 2011, the Syrian government paid for Soueid to travel to Syria, where he met with intelligence officials and spoke with President Bashar al-Assad in private. He returned to the United States in early July 2011, and he was searched and questioned at Dulles International Airport upon his arrival. The indictment states that Soueid communicated with his "boss," an unindicted co-conspirator (or UCC-1) who was working for the Mukhabarat, soon after to alert him of the search and questioning and to assure the individual that the airport encounter would not "stop the project."

(U) In addition to the recordings, Soueid is accused of providing the Mukhabarat contact information, including phone numbers and email addresses, for protestors in the United States. In a handwritten letter sent to UCC-1, Soueid allegedly expressed his belief that violence against protestors – including raiding their homes – was justified and that any method should be used to deal with the protestors. The indictment also alleges that Soueid provided information regarding US protestors against the Syrian regime to an individual who worked at the Syrian Embassy in Washington, D.C.

(U) On Aug. 3, 2011, FBI agents interviewed Soueid, and the indictment accuses him of lying to the agents when he denied that he had collected information on US persons and transmitted that information to the government of Syria. In addition, Soueid allegedly made further false statements when he denied to FBI agents that he had directed someone to audio or videotape a conversation, meeting, rally or protest, or that he was aware of any individual taking photographs or videotaping people. He also allegedly made false statements when he denied that he had ever been an agent of the Syrian government or a foreign intelligence officer.

(U) The indictment states that the day following the interview, Soueid asked UCC-1 to inform the Mukhabarat about his FBI interview. In addition, the indictment alleges that, when purchasing a Beretta pistol on July 11, 2011, Soueid listed a false current residence address on a firearms purchase application and in records that were kept by a licensed firearms dealer.

(U) CYBERSECURITY SPECIAL FOCUS FOR INDUSTRY:

(U) Six Deadly Security Blunders Businesses Make; Small, Subtle Mistakes Can Lead to Big Security Breaches (*26 OCT 2011, Darkreading*)

(U) Sometimes it's the unknown or overlooked little mistakes that leave an organization wide open to attack: a missing hash mark in a server configuration, a long-forgotten PBX user account, or an embedded Web server in an office printer. With compliance pressures, increasingly cagey malware, and the fear of being the next front-page data breach victim, it's no wonder that enterprises might not notice potential problems with their lower-profile devices, or make subtle configuration mistakes. Even so, ignorance is no excuse when the bad guys hone in on an inconspicuous weakness, like a few older, rarely used desktops that haven't been updated with the latest patches. It takes only one weak link for an attacker to gain a foothold into an organization and steal valuable data, or set up shop for long-term cyberespionage.

(U) Spooked yet? Take a look at some subtle but potentially dangerous mistakes enterprises make that could come back to haunt you.

(U) 1. Improperly configuring an SSL server.

(U) SSL has gotten a bad rap lately for some inherent security weaknesses. But many SSL servers aren't configured properly such that they aren't even exploiting the benefits of an encrypted session. Only about one-fifth of SSL websites actually redirect to SSL for authentication, and about 70 percent of SSL servers handle credential logins in plain text. More than half submit passwords in plain text. That's according to a global SSL survey by SSL Labs, Qualys' community project. But that's not all: Now the bad guys can perform a denial-of-service attack on an SSL server without the help of a botnet. A new hacking tool unleashed this week abuses the SSL renegotiation feature to DoS an SSL server from a single laptop or other machine.

(U) Organizations that mistakenly leave SSL renegotiation enabled are vulnerable to this attack with the so-called THC-SSL-DOS tool now circulating. Security experts say SSL renegotiation on a Web server isn't really necessary, anyway, and recommend disabling it altogether. But there's still no actual solution to defend against the attack, says the manager of security research and development at nCircle. "It's the way the protocol works," he says. He notes the DoS attack is one more piece of evidence that SSL is broken. "We need something better."

(U) 2. Overlooking a rarely used account with high-powered privileges.

(U) Many organizations fail to lock down an administrative account, using default logins and passwords that can ultimately give attackers the keys to the kingdom. But there are other lesser-known or used accounts that can easily be forgotten and left open for abuse. A Fortune 500 financial services firm that was considered highly secured and had protected its admin account recently was caught unaware by a long-forgotten field-manager user account on an old Siemens Rolm PBX: That relatively powerful user account was all penetration testers from Trustwave SpiderLabs needed to set a trap to infiltrate the firm's heavily fortified network. They used the account to establish a cloned help-desk voicemail box, and waited for a caller they could social-engineer for his user credentials. Havelt, posing as an IT help-desk

engineer, easily obtained a VPN user's username and two-factor authentication token password when he fixed his VPN connection. That led the pen testers to the firm's HR finance and wealth management transfer systems, as well as other sensitive information.

(U) "It was a tiny, little thing that snowballed," says the director of penetration testing for Trustwave SpiderLabs, who worked on the pen-testing engagement for the company's financial services firm client. "It's always the little thing: That's a recurring theme. Leave a default account, default password. It might not seem like a big deal, but it can rapidly [escalate]. ... If you give anyone any level of access, they will find a hole." He says organizations should audit all equipment, even legacy systems like PBXes. "Make sure you are enforcing password policy," he says. In the case of the financial services firm, the PBX systems "belonged" to the telecommunications group rather than IT, and there was a disconnect security-wise. "Ideally, you need somebody to take responsibility for anything that can be plugged in [the network]," he says.

(U) 3. Assuming your VPN traffic is always secure.

(U) Just because a user connects to the corporate VPN from a hotel network doesn't necessarily mean remote security. "It's a pretty serious mistake" assuming a remote employee coming in over the VPN is safe and secure traffic, says the vice president of marketing and business development for AlgoSec. "Working from a hotel network, there's a lot of malware they can pick up, and a lot that might not be detected by the endpoint's AV. Then if they are allowed to tunnel in, that malware on the PC is pretty bad stuff coming into the corporate network," he says. "When a typical user working remotely or from home connects to the VPN, they may not have [proper] security controls in place."

(U) So although a VPN session is theoretically authenticated and encrypted, an already-infected user machine can be introducing badness to the corporate network. If the user's machine is bot-infected, the botnet then also has access to the internal network, he says. The key is to stop even VPN traffic at the DMZ first for inspection. "Most companies don't do that," he says. "They inspect traffic from untrusted external sources, but if traffic is over a VPN, it isn't perceived as a risk." That could be accomplished with a firewall policy, for instance. "A lot of people believe traffic over the VPN is secure. We argue that this is not the case," he says.

(U) 4. Ignorance of embedded systems.

(U) Copiers, scanners, and VoIP phones contain embedded Web servers that typically aren't secured or are misconfigured such that they are exposed to the Web when they are installed. " Virtually none of these should be exposed to the Internet. There's not a good reason that an HP scanner should be exposed to the Net," says the vice president of security research for Zscaler Labs, who shared his findings about the breadth of the problem at Black Hat USA this summer. He found Ricoh and Sharp copiers, HP scanners, and Snom VoIP phones most commonly accessible via the Internet. And it's likely they belong to companies that have no idea the devices are showing up online. Digital archives of photocopies could be lifted by attackers, who also can eavesdrop on the embedded VoIP systems via a packet capture feature, for instance. "If [the VoIP system is] accessible, you can log in, turn it on, capture traffic, download PCAPs ... and with Wireshark, you can eavesdrop on organizations," he says. The key is to scan for these types of vulnerable devices before the bad guys find them.

(U) Other network equipment also comes with misconfigurations that leave unknowing customers at risk. The chief security officer at Rapid7 and chief architect of Metasploit last year revealed how he found hundreds of DSL concentrators, SCADA systems, VoIP equipment, and switches that contained a diagnostics service for feature from VxWorks. It's a feature that should not be enabled in production mode, he warned, because it would allow access to read and write memory and power-cycle the device.

A related problem comes with today's consumer devices that come equipped with GSM or cellular access. A security consultant with iSec Partners, says GPS tracking devices, car alarms, and even SCADA sensors are vulnerable to attack via the network. Once an attacker finds one of these devices on the network, he can abuse them. The consultant successfully hacked into a popular car alarm system and started the car remotely by sending it a text message. Even more chilling is the potential for abuse for a SCADA sensor.

(U) 5. Typos in source code or configuration files.
(U) A missing forward-slash symbol in Apache Web servers, and possibly other Web platforms, could lead attackers to databases, firewalls, routers, and other internal network devices. The recently revealed reverse-proxy bypass attack on Apache servers demonstrated how a single character in a configuration file can make or break security. A research and development manager at Context Information Security, which discovered the problem, says it's more of a misconfiguration issue that users didn't know about: that a forward slash was required in a so-called "rewrite rule" for an Apache Web proxy "It's a classic case of functionality lying around that people didn't know was there, and didn't know the misconfigurations are," he says. Apache released a patch for the issue earlier this month, but Jordon says it's a problem that likely affects other Web platforms as well. "The patch reduces the likelihood of misconfiguring it," he says. "Any other URL-rewriting reverse proxy would potentially have the same issue. We have contacted other Web server providers to inform them of this," he says.

(U) 6. The obvious, but still common, problem of leaving obscure systems unpatched.

(U) Patching is an obligatory best practice, but that doesn't mean organizations do it right, on time, or even at all for some systems deemed low-risk. Take the US Department of Energy, which in October was called out for poor patching practices. According to the DoE Inspector General's office, 15 different DoE locations were found running desktop systems, network systems, and network devices running apps that hadn't been patched for known vulnerabilities. About 46 percent of the desktop systems were running operating systems or apps without the most current patches, for example, according to the IG's report. "These applications were missing security patches for known vulnerabilities that had been released more than 3 months prior to our testing," the report says.

(U) But the federal agency is far from alone in leaving systems unpatched: Many organizations struggle to get a handle on the vulnerabilities in their environments. Recent research from Secunia suggests that enterprises could realize big-time security improvements if they prioritize their patches by the severity of the vulnerability instead of the prevalence of the application. The CTO and co-founder of eEye Digital Security, says it comes down to not knowing what you don't know. "Companies ... don't have the visibility, so they don't have a handle on where the weaknesses are in their environment. Or they don't know where to start, and they give up," he says.

(U) Analyst Comment: IT security specialists and network administrators in New Jersey should review these six security problems with senior management to ensure they are discussed and addressed across corporate networks. It is especially important to ensure that network accounts are reviewed for privilege-levels and validity. Rigorous patch management must also be instituted to ensure networks are protected from all known vulnerabilities.

(U) CYBER THREAT ITEMS FROM THE PRESS:

(U) Malicious Cybersecurity Assaults Increased 650 Percent in Past Five Years, Feds Say (*Layer 8, 04 OCT 2011*)

(U) Cybercriminals and other villains intent on stealing all manner of personal and government data are bombarding federal government agencies. Over the past 5 years, the number of incidents reported by federal agencies to US-CERT (United States Computer Emergency Readiness Team) has increased from 5,503 incidents in fiscal year 2006 to 41,776 incidents in fiscal year 2010, including a more than tripling of the volume of malicious software since 2009, an increase of over 650%, according to a Government Accountability Office security report released in early October.

(U) US-CERT aggregates and disseminates cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection, the GAO added. "Reported attacks and unintentional incidents involving federal systems and critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices," the GAO stated.

(U) The good news is perhaps that according to US-CERT, the growth in the gross number of incidents is attributable, at least in part, to agencies improving detection of security incidents on their respective networks, and then possibly implementing appropriate responsive and preventative countermeasures, the GAO stated.

(U) Agencies reported the following types of incidents are occurring frequently:

- (U) Unauthorized access: Gaining logical or physical access to a federal agency's network, system, application, data, or other resource without permission.

- (U) Denial of service: Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.

- (U) Malicious code: Installing malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.

- (U) Improper usage: Violating acceptable computing use policies.

- (U) Scans/probes/attempted access: Accessing or identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.

(U) Download the GAO report at: http://www.gao.gov/new.items/d12137.pdf

(U) Anonymous Can't Attack SCADA Systems Now, but May Do So in Future: DHS (*Eweek, 18 OCT 2011; Computerworld, 18 OCT 2011*)

(U) The Department of Homeland Security has evaluated Anonymous and found that while the collective currently may not be able to take over critical IT infrastructure today, they may be able to someday. The "hacktivist" collective Anonymous is capable of crippling critical infrastructure, but the odds of developing a Stuxnet-style attack on industrial Supervisory Control and Data Acquisition systems were slim, according to a Department of Homeland Security bulletin. The four-page report from the department's National Cyber-Security and Communications Integration Center was posted on the Public Intelligence Website on Oct. 17. The Department of Homeland Security evaluated the collective's potential to disrupt critical infrastructure in the "Assessment of Anonymous Threat to Control Systems" report, dated Sept. 17.

(U) Even though hacktivist groups are increasingly more active in their attacks, DHS said actual threats to control systems don't seem to have increased. Anonymous currently has a "limited ability" to conduct attacks that target industrial control systems, the DHS found. The group has the capability to disrupt operations with distributed denial-of-service attacks, but it doesn't currently have the necessary skills to take over critical infrastructure, according to the DHS. "However, experienced and skilled members of Anonymous…could be able to develop capabilities to gain access and trespass on control system networks very quickly," according to the DHS bulletin. DHS evaluated the group after a known Anonymous member posted on Twitter on July 19 a directory tree for Siemens SIMATIC control system software, according to the report. "This is an indication in a shift toward interest in control systems by the hacktivist group," the report said.

(U) Critical infrastructure refers to the systems and networks that power communications, energy, financial systems, food, government operations, health care systems, transportation and water. The vast majority of the infrastructure is currently controlled by the private sector. **The idea that Anonymous might target critical infrastructure is not far-fetched. Members have called for attacking energy companies and on July 11, some members of the collective attacked biotechnology seed company Monsanto. As part of the attack, Monsanto's Web infrastructure had been disabled for two days, email servers disabled for three days and data on 2,500 employees and partners stolen.**

(U) Groups such as Anonymous and LulzSec choose to "harass and embarrass their targets using rudimentary attack methods," DHS said. All the information released by Anonymous and LulzSec indicated that the groups showed "no indication of exploitation capability," according to the report. While the risks currently are low, there was a "moderate likelihood" that future protests could be accompanied by attacks on core infrastructure in the future. The group can become more interested, especially as they realize how poorly these systems are secured in the first place, the report warned. Members can study industrial control systems using publicly available information and develop malware to exploit well-known vulnerabilities, according to the federal agency.

(U) In the report, the DHS cites several recent actions that point toward a growing interest by Anonymous in industrial control systems. In July, it notes, Anonymous members released a report spelling out the collective's concerns about global warming and called for protests against the Alberta Tar Sands project in Montana. The Anonymous report aimed to draw attention to what the group claimed was "boundless greed" of several energy and financial services companies. In July, a known member of Anonymous also publicly claimed to have accessed multiple control systems. The Anonymous post included administrative code used to create password dump files for a human-machine interface system from Siemens, and so-called "foundation code" that is used in server communication with programmable logic controllers, industrial controllers and remote terminal units, the DHS bulletin said.

(U) The report notes that Anonymous has the ability to disrupt some systems within the critical infrastructure, such as Windows systems and Web applications, by using "rudimentary attack methods" such as denial of service attacks. The DHS assessment comes amid increasing concern about vulnerabilities in US critical infrastructure. Last year's Stuxnet worm in particular drew massive attention to the possibility that cyberattacks could disrupt or take down critical infrastructure targets. The DHS in recent months issued several similar alerts about the activities of Anonymous, which indicates that the loosely affiliated collection of so-called hactivists is seen as a serious threat.

(U) The DHS report still warned that even though Anonymous may not attack the control systems, all businesses should still make sure their IT systems are protected. Attackers can easily locate and access industrial control systems with "minimal skills" using Internet search engine tools and applications to carry out "nefarious activities" or conduct reconnaissance activities to launch other attacks, the department warned. Oil and gas companies are potentially attractive targets as the collective supports the "green energy" agenda and has opposed pipeline projects in the past. The report says that Anonymous recently called on members to target energy companies. DHS said the call is likely to attract both members of the collective and the broader activist hacking community. "Asset owners and operators of critical infrastructure control systems are encouraged to engage in addressing the security needs of their control system assets," the DHS said.

(U) Analyst Comment: As this report points out: biotechnology, food/agriculture, chemical and energy companies in New Jersey should dedicate the time and resources to ensure all necessary network intrusion detection and monitoring programs are in place, as they may be targeted by cyber hackers seeking to make political statements.

(U) DHS: Cyber Attacks on Utilities, Industries Rise (*Associated Press, 01 OCT 2011*)

(U) US utilities and industries face a rising number of cyber break-ins by attackers using more sophisticated methods, a senior Department of Homeland Security official said during the government's first media tour of secretive defense labs intended to protect the US power grid, water systems and other vulnerable infrastructure. Acting DHS Deputy Undersecretary Greg Schaffer told reporters Thursday that the world's utilities and industries increasingly are becoming vulnerable as they wire their industrial machinery to the Internet. "We are connecting equipment that has never been connected before to these global networks," Schaffer said. Disgruntled employees, hackers and perhaps foreign governments "are knocking on the doors of these systems, and there have been intrusions."

(U) According to the DHS, Control System Security Program cyber experts based at the Idaho National Laboratory responded to 116 requests for assistance in 2010, and 342 so far this year. Department officials declined to give details about emergency response team deployments, citing confidentiality agreements with the companies involved. Under current law, the reporting of cyber attacks by private organizations is strictly voluntary. The Obama administration has proposed making reporting mandatory, but the White House could find the idea difficult to sell at a time when Republicans complain about increased regulation of business. Officials said they knew of only one recent criminal conviction for corrupting industrial control systems, that of a former security guard at a Dallas hospital whose hacking of hospital computers wound up shutting down the air conditioning system. The former guard was sentenced to 110 months in prison in March.

(U) The Homeland Security Department's control system program includes the emergency response team, a Cyber Analysis Center where systems are tested for vulnerabilities, a malware laboratory for analyzing cyber threats and a classified "watch and warning center" where data about threats are assessed and shared with other cyber security and intelligence offices. The offices are located at nondescript office

buildings scattered around Idaho Falls. No signs announce their presence. The chief of the control system security effort, said the malware lab analyzed the Stuxnet virus that attacked the Iranian uranium enrichment facility in Natanz last year. He did not describe the group's findings in detail, except to say that they confirmed that it was "very sophisticated." He said that several years ago he had asked the German company Siemens to study the same kind of industrial controllers used at Natanz for vulnerabilities to attack, because they were so widely used in industry. But he said the study was not part of any effort to target the controllers with malware, and said his program's work on the controllers could not have helped Stuxnet's designers.

(U) A senior Homeland Security cyber official, who spoke on condition of anonymity because of the sensitivity of the topic, said the Stuxnet worm exploited well-known design flaws common to many system controllers, vulnerabilities that in general can't be patched. Many independent experts and former government officials suspect that Stuxnet was created by the United States, perhaps with the help of Israel, Britain and Germany. The United States and other nations believe Iran is building a nuclear weapons program, but Tehran insists it is interested only in the peaceful uses of nuclear technology.

(U) While US officials talk frequently about the threat of cyber attacks to America, they seldom discuss the country's offensive cyber weapons capability. The United States is thought to be the world's leader in cyber warfare, both defensive and offensive. US officials and others long have feared that future wars will include cyber assaults on the industries and economies of adversaries, and the potential targets include power plants, pipelines and air traffic control systems. Foreign nations could also target military control systems, including those used for communications, radar and advanced weaponry. Because of its advanced industrial base and large number of computer controlled machines connected to the Internet, the United States is thought to be highly vulnerable to a cyber attack on its infrastructure.

(U) In a 2007 test at the Idaho National Laboratory, government hackers were able to break into the control system running a large diesel generator, causing it to self-destruct. A video of the test, called Aurora, still posted on YouTube, shows parts flying off the generator as it shakes, shudders and finally halts in a cloud of smoke. A former State Department official now with the Center for Strategic and International Studies in Washington, said in an interview that the Aurora test ushered in a new era of electronic warfare. Before the test, he said, the notion of cyber warfare "was mainly smoke and mirrors. But the Aurora tests showed that, you know what? We have a new kind of weapon." Homeland Security officials said they have not conducted such a test on that scale since. But they demonstrated Thursday how a hacker could tunnel under firewalls in computer systems to take command of industrial processes. "All systems deployed have vulnerabilities," the senior cyber official said.

(U) On the Front Line Against the Next Stuxnet; Meet the People Who Will Get the Call When the Next Stuxnet Worm Strikes *(IDG News Service, 01 OCT 2011*)

(U) Something has gone terribly wrong on the plant floor at ACME Specialty Chemical International Inc. Liquid is overflowing from vats, the power keeps shutting off, and CEO Jeff Hahn has no idea what's going on. Behind him is a computer used to control the factory. Ominously, the cursor moves around on the screen as if it has developed a life of its own. "I have no control of my mouse," says the woman at the terminal. It turns out that Jeff Hahn is the one to blame. Like many CEOs, he clicks on any interesting link he sees in his email inbox. This time, he clicked on a link sent by hackers working for a rival company, Barney Advanced Domestic Chemical Co.

(U) Fortunately, ACME Chemical isn't real. It's part of a training exercise run by the US Department of Homeland Security (DHS) and Idaho National Laboratory (INL). And Jeff Hahn isn't actually a CEO. He's a training lead at INL, playing his part in a cyberexercise that took place Friday at the lab's training facility in Idaho Falls, Idaho. People who run industrial systems, like those at ACME Chemical, have traditionally cared about one thing above all others: They want their machines to run without interruption, and nothing -- not even an important security patch or operating system update -- can get in the way. These obscure systems are built by big companies such as Siemens, Honeywell, and Rockwell Automation, but they've kept a low profile. Last year's Stuxnet worm changed everything, showing that these types of machines can be attacked, and even brought down with a cyberattack.

(U) That's put the DHS-funded INL security programs in the spotlight, because they form the backbone of the government's plan to secure industrial systems. "In many ways, we are connecting equipment that has never been connected before to this global network, and as we do so, we have the potential for problems," said the acting deputy undersecretary with the DHS's National Protection and Programs Directorate, speaking at a briefing for reporters at INL. "They are kicking on the doors of these systems, and in some cases there have been intrusions." There are about 75 people working on the INL programs, known collectively as the Control Systems Security Program. With an annual budget of just over US$25 million, they form the first line of defense against attacks on industrial systems.

(U) The recent exercise was put on for the benefit of the press. But every month about 40 engineers and computer security professionals are invited to test their skills at these day-long exercises, where members of a hacking group, known as the Red Team, try to break into a test network defended by the Blue Team. According to Hahn, the good guys usually win, but not easily. The test networks are riddled with holes, none of which are known in advance to Blue Team members, and it's often a scramble to secure the systems before the Red Team maps out the network and disrupts the factory floor.

(U) The control systems program one of the US government's main weapons as it tries to beef up computer security in power plants, at chemical refineries and on factory floors. Companies that make the hardware and software for big industrial machines can come to INL for a hard-nosed security evaluation of their products. It's a good deal for vendors, as part of their testing costs are covered by taxpayers, and it's good for the lab, because its engineers get to learn about security problems that could flare up in the future.

(U) Although INL has been doing this work quietly for close to a decade, last year it assessed products from 75 vendors, the publicity around Stuxnet has put it in the spotlight like never before. The world dodged a bullet with Stuxnet. Although it spread across the globe, it left almost every system it infected operational. It was a cyber sniper-shot aimed at uranium-enriching centrifuges at Iran's Natanz nuclear reactor. The possibility of a second industrial systems worm has many security experts worried, though. Stuxnet infected tens of thousands of systems, including many that contained Siemens programmable logic controllers. If it had been designed to mess up every Siemens system it infected, instead of damaging only the Natanz centrifuges, it could have caused widespread damage.

(U) Now that Stuxnet has proved that these machines can be hit, another cyber attack on industrial systems is inevitable, according to the CEO of the National Board of Information Security Examiners, and a noted expert on industrial security issues. "It's a matter of time," he said. But is the US Department of Homeland Security's ICS-CERT (Industrial Control Systems) team, set up at INL to respond to this type of incident, ready for a serious problem? Critics say the DHS was slow to respond to the Stuxnet threat and parsimonious with the information it did share.

(U) DHS officials at the training exercise defended their handling of Stuxnet, but the man in charge of ICS-CERT said there's room for improvement. "I think there's always going to be an evaluation of how much information do we release, when do we release it and how do we release it," said the ICS-CERT's director. "So as we continuously evaluate those, and Stuxnet was a very good case study of how we performed, we'll continue to fine-tune the processes to give industry the tools they need to defend these systems." DHS intentionally released fewer details about the problem than vendors like Symantec, he explained. "We still haven't released broadly the [Stuxnet] technical details, because I still believe that they're sensitive," he said. "You're not going to see us post those kind of details to a completely open, public website because we don't want to encourage the script kiddy or the copycat types."

(U) Just a few blocks from the training facility that was home to the exercise, INL operates a "watch floor" for industrial systems. This is the classified building where phones will start ringing should the next Stuxnet show up, and home to staffers who specialize in IT and industrial systems. It's small -- there were just four analysts there on a Thursday -- but it looks like the security operations centers you see big companies such as Cisco and Symantec: people sitting in front of computers, with a big screen showing a real time feed of any situations that need to be handled. When Stuxnet first appeared in July 2010, this is where the US response was mustered. The worm was quickly handed over to a special malware analysis lab, also run by INL in Idaho Falls, where it was dissected by security experts and industrial engineers. An executive says the group "had an appropriate response to what was a complex and new set of circumstances that we had to deal with." And while he believes that the siphoning off of intellectual property is the largest cyber issue facing the United States right now, the doomsday possibilities of a well crafted attack on power plants or nuclear facilities makes the kind of work that goes on at Idaho National Labs important. "This is an issue that is evolving and that could have significant impacts to us," he said. "This program is designed to get us in front of those problems."

(U) FAQ on Son of Stuxnet; Duqu Has a Lot of the Same Code, Different Intent (*20 OCT 2011, Network World*)

(U) What is Duqu?

(U) Duqu (pronounced dyu kyu) is primarily a remote-access Trojan targeted at a limited number of organizations in Europe, Africa and the Middle East to gather intelligence that can help plan a future attack.

(U) Why is it called Duqu?

(U) It creates files with the prefix DQ.

(U) Why is it called Son of Stuxnet?

(U) Much of its code is identical to Stuxnet code, the malware that took over control of machinery in Iran's nuclear refinement program and wore it out.

(U) How long has it been in use?

(U) It was discovered Sept. 1 but might have been in use since December 2010.

(U) What has it done?

(U) It has performed reconnaissance on the networks it infects.

(U) How does it do that?

(U) First, it infects a system. The mechanism for getting in -- thumb drive, social engineering, etc. -- is not known.

(U) Once it is running on a system, it connects with a command and control server in India (since blocked by its ISP) from which it downloads other malware. This includes information-stealing programs that can copy keystrokes, gather system information and scan networks for vulnerabilities. It could download other types of malware as well.

(U) What is its purpose?

(U) That's uncertain. Experts think it is laying the groundwork for an attack of unspecified intent. Duqu had no offensive capabilities but could reach out to a command and control server for them. Stuxnet's capabilities included exploiting vulnerabilities in Siemens gear that controlled industrial systems.

(U) Who is targeted?

(U) Experts differ. Some say it was after certificate authorities, some say it was after a maker of control systems based in Europe.

(U) Who's behind it?

(U) Likely the same group that was behind Stuxnet because it uses so much identical code. No one knows for sure who was behind Stuxnet but the sophistication indicates a nation, possibly the United States and Israel.

(U) How do you know if you've got it?

(U)Anti-malware vendors should develop signatures for it that will find it and remove it. It's also likely that if it is used again, its creators will alter the signature to avoid detection.

(U) Is it a major worry?

(U) At the moment, it seems to have been put out of business by knocking out its command and control server. It's possible, though, that if it can't reach its primary C&C server, it may try a backup. The code hasn't all been deciphered and reviewed, so not all of its capabilities are known.

(U)Who discovered it?

(U) That's secret, but it's described as an independent research group.

(U) SEC Orders Disclosure of 'Potential' Security Breaches (*CNET, 13 OCT 2011*)

(U) Even potential data security breaches must be disclosed by US companies in some circumstances, the Securities and Exchange Commission announced in October. The move by the SEC is likely to shed more light on how publicly-traded companies are grappling with cybersecurity problems, especially because the agency's ruling says that disclosure is needed when "the risk of potential incidents" becomes significant enough to impact the bottom line.

(U) In a statement, the SEC indicated it would like to see:

(U) • Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences...

(U) • Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences...

(U) • Risks related to cyber incidents that may remain undetected for an extended period...

(U) The announcement isn't exactly a surprise. A handful of Democratic US senators had been pressing the agency since May to take steps in this direction. Companies have disclosed actual attacks before, just not, generally, potential ones. The new order thus marks a significant shift in required disclosure. "For years, cyber risks and incidents material to investors have gone unreported in spite of existing legal obligations to disclose them," Sen. John Rockefeller IV, chairman of the Senate Commerce committee said. "Intellectual property worth billions of dollars has been stolen by cyber criminals, and investors have been kept completely in the dark. "

(U) This kind of regulation may be what a billionaire investor, a member of Facebook's board of directors, had in mind when he told CNET last month that there are good reasons for companies not to go public. The investor said: "There's simply a degree to which public companies are given a scrutiny that is much greater and much more heavily regulated than private companies... The correct decision that people have made in the last decade in Silicon Valley has been to try to defer the IPO process as long as possible."

(U) 111 Arrested in Massive ID Theft Bust; Restaurant Workers and Bank Insiders are Charged in What's Billed as the Largest-Ever ID Theft Round-Up (*IDG News Service, 07 OCT 2011*)

(U) Prosecutors call it the biggest identity theft bust in US history. In October, 111 bank tellers, retail workers, waiters and alleged criminals were charged with running a credit-card-stealing organization that stole more than $13 million in less than a year-and-a-half. "This is by far the largest -- and certainly among the most sophisticated -- identity theft/credit card fraud cases that law enforcement has come across," the Queens County District Attorney's office said in a statement announcing the arrests.

(U) The credit card numbers came from far and wide: from skimming operations in the United States, where restaurant employees or retail cashiers were paid to steal credit card data from customers; from carder forums on the Internet; and also from shady overseas suppliers in countries such as Russia, China and Libya. On all, five groups of criminals were targeted in the two-year law enforcement operation, dubbed "Operation Swiper." Together, they ran the full gamut of criminal activities required to steal credit card numbers and convert that data into cash, prosecutors said. Eighty-six of the defendants are in custody; police are looking for the remaining 25, prosecutors said.

(U) The accused are charged with running a thoroughly modern identity theft ring that included ID thieves, skimmers, card makers, fences and shopping crews: groups that would buy thousands of dollars worth of merchandise in stores throughout the United States. "Many of the defendants charged today are accused of going on nationwide shopping sprees, staying at five-star hotels, renting luxury automobiles and private jets, and purchasing tens of thousands of dollars worth of high-end electronics," the Queens DA office said.

(U) During a raid earlier this week, police seized "a box truck full of electronics, computers, shoes and watches, skimmers, card readers, embossers and various amounts of raw material, such as blank credit cards and fake identifications," the DA's office said. Six of the accused are charged with stealing $850,000 worth of computer equipment from a Citigroup building in Long Island City last August. Prosecutors say that a former Citi employee, Steven Oluwo, and a security guard under contract to Citigroup, Angel Quinones, helped with the theft. Apple, Best Buy, Nordstrom, Macy's and many financial institutions, including Citi, Chase Bank and Bank of America, are credited with helping with the investigation.

(U) 'Well Organized, Sophisticated, Fast' Cybercriminals Scare US Banks; Expert in Financial Services IT Says Public/Private Partnerships are the Only Way to Battle Hackers (*Network World, 04 OCT 2011*)

(U) BITS, the US financial industry's IT policy arm, has a new leader: Paul Smocer, an expert in email security and authentication. Smocer is taking the lead of BITS at a time when financial services firms are responding to the emergence of new technologies, including social networking, mobile computing and cloud computing, while remaining under attack from ever-savvier cybercriminals. BITS is coordinating efforts by the US banking industry to create new top-level domains, such as .bank, .insure and .invest, that would be restricted to financial services firms and could offer consumers extra protection from phishing, malware and other attacks.

(U) Network World interviewed Smocer about the online threats and opportunities that he is most concerned about. Here are excerpts from the conversation:

(U) What are the most pressing issues facing BITS over the next year?

(U) We're focused on a handful of things. One is the public/private information sharing concept. As we have recognized the sophistication of what's going on in the cybercrime world, we also recognize that we need to coalesce around better sharing of information among financial institutions, among the various industry sectors, and with the government as well. We're in the middle of piloting an effort with the Treasury Department, [Department of Homeland Security] and its [Computer Emergency Readiness Team], where government resources come in and help do resiliency reviews of organizations.

(U) We're doing a lot of work with regard to mobile financial services [and] what kind of security and controls are needed. We're also doing work with [the Internet Corporation for Assigned Names and Numbers] around new top-level domains. We're working with the [American Bankers Association] and other associations to look at creating some top-level domains that could serve to enhance the security and resiliency of financial institutions on the Internet.

(U) What is the BITS position on the ICANN plan to adopt hundreds of new top-level domains like .bank?

(U) It presents opportunities and challenges. Other trade associations are still tending to fight the whole idea, but we see it as an opportunity to build a more secure and resilient space on the Internet for financial services. I don't know how quickly there will be a lot of conversion of consumer services to these domains, but they certainly afford us the opportunity for b-to-b transactions. Financial institutions exchange a lot of information amongst themselves, and having a space that's more secure than the general dot-com space works to our advantage.

(U) What does BITS think of the new DNS security standard -- DNSSEC -- which helps organizations to prevent DNS spoofing attacks?

(U) DNSSEC is an important step forward and some new top-level domains do require it, including those domains that deal with financial institutions and financial transactions. I like to think that's a direct result of our efforts. We're also spearheading work in Web security for whatever top-level domain that we would apply for.

(U) What new technologies are you most excited about having an impact on the financial services industry?

(U) Mobile is certainly a channel that we see having a great future in terms of customer service, but we think it has to be done in an appropriately secure way. We just published a paper around social media, giving some guidance to the financial industry. We're also working on a better definition of the risks and controls that are necessary in the cloud computing space. There are strong economic enticements for companies to look at cloud computing, whether for software or storage. But, obviously, that has to be approached with some caution. When we look at new technologies with our members, the one thing we always want to retain is the trust in the financial system. We always look at risk management.

(U) How do you foresee cloud computing evolving in the financial services industry?

(U) I think honestly for a while we will see much more activity in the private cloud space ... because that is the safest place to be.

(U) What risks do social media sites pose to financial services firms and how is BITS helping mitigate them?

(U) We encourage companies to have all the right players participate in the development of the social media presence and social media policy, from the legal department to the ethics office to the HR department. It's not just about technology. Content is a big issue. You need to make sure that you have the ability to control who is posting content and they understand what content is good to post. From the perspective of the individual, you have to understand that it's another channel to introduce malicious software into the environment. But in many ways, social media is just an evolution. A lot of the policies and practices that apply to how you allow employees to use email and what you allow them to say and what they are allowed to export apply to social media.

(U) What role is BITS taking in the depletion of IPv4 addresses and the adoption of the replacement standard, IPv6, by the financial industry?

(U) Most of our members are very aware of the technical issues out there, IPv6 being one of them. We have been discussing the necessary risk and control considerations of a rollout of IPv6. We likewise have talked about that IPv6 is already in their environments whether or not they know it, so they need to take precautions. Right now, we're largely in an education and continuing to watch developments stage around IPv6.

(U) What are the cybersecurity worries that keep you up at night?

(U) One, how organized the cybercrime community is. Two, how quickly and how sophisticated that community moves. How many versions of the Conficker worm do we have? As people have responded to version 1 and blunted its impact, you see a move to version 2 and then version 3. There's the speed and sophistication. It all goes back to strong information-sharing between public

and private organizations so that the good guys are as organized as the bad guys. My third worry is that the evolution of technology is happening so quickly. It just seems like the pace of change has become so rapid, that it's difficult to keep up with it and understand the implications of it.

(U) What can CIOs in other industries learn from your experience at BITS with cybersecurity?

(U) The first thing is to collaborate. In any industry, there are competitive issues, but there are also issues that are easy to collaborate around that benefit the industry as a whole and make the industry better. Maybe because the financial services industry has a history of trust, our members collaborate very effectively with each other around topics that they know are going to benefit everyone in the industry.

(U) Secondly, we are in an ecosystem now that is not just about one industry vertical anymore. We exist in a system that has us all relying on each other. Mobile financial services involve telecom providers, Internet providers and technology providers. The idea of partnerships needs to extend beyond your own industry vertical. We all need to effectively share information with each other and work together.

(U) The third thing is to be aware about not only your organization but about your customers. If you're focused on the ultimate protection of both your organization and your customers, that gives you the focus to continually try to strengthen the environment.

(U) Healthcare Security Needs a Booster Shot (*CSO, 30 SEP 2011*)

(U) A new survey from PricewaterhouseCoopers has found that a majority of health enterprises do not have the security in place, nor the policies, to properly protect patient data and privacy. In its report, "Old data learns new tricks: Managing patient privacy and security on a new data-sharing playground", the advisory firm PwC says health organizations are slipping behind the rapid pace of new technological adoption as there's more data sharing, increased collaboration with partners, as well as the industry's fast embrace of electronic health records, mobile computing and social networks.

(U) None of this is news to readers of CSOonline, as we covered the issues previously in "Digitized medical records are easy prey", and " Is health care security in intensive care?" The findings are from a US-based PwC Health Research Institute survey of 600 executives from hospitals, physician organizations, health insurers and pharmaceutical and life sciences companies. In the survey, data theft scored high: In fact, theft of records accounted for 66 percent of reported health data breaches during the previous two years. Also, just over one-third of hospitals and physician groups reported cases of medical identity theft. And 54 percent of health organizations reported at least one issue with information privacy and security over the past two years. "The increase in thefts doesn't surprise me, because attackers have the tools and smarts necessary to successfully attack these systems and get away with the goods," says the research director at Spire Security. "The industry is exposing the data to the world and making more complex apps, and they're getting hacked as a result."

(U) As one would suspect, commonly it's insider improper use of protected health information, with 40 percent of providers saying that has happened in their organization during the 24 months prior to the survey. With a peek at the lack of policies healthcare organizations have in place, it doesn't seem too surprising why there are problems with security and privacy. For instance, the survey found that more than half of firms allow access to social networking at work, while only 37 percent incorporate approved uses of mobile devices and social media as part of privacy training.

(U) The survey also found that organizations that try to integrate their privacy and security efforts at least believe that the security of their organization's data has increased in the past year. However, the actual

reduction in breaches for their effort has been anemic, from 1.22 average reported breaches in the past two tears to 1.14. "It's tough to tell if companies are getting the value out of their security investments, with the difference in breached vs. non-breached being so tight," research director says.

(U) Massive DDoS Attacks a Growing Threat to VoIP services; TelePacific Communications Tells of VoIP Floods (*04 OCT 2011, Network World*)

(U) When the massive distributed denial-of-service (DDoS) attack in March brought down the voice-over-IP (VoIP) call processing supplied by TelePacific Communications to thousands of its customers, it marked a turning point for the local-exchange services provider in its thinking about security. The massive DDoS attack came blasting in from the Internet in the form of a flood of invalid VoIP registration requests. The attack resulted in widespread service disruptions for a number of days in late March and cost the company hundreds of thousands of dollars in customer credits. After the attack was over, the facilities-based services provider, based in California and Nevada, took steps to boost security measures to seek to prevent any similar occurrence again, said the vice president of network engineering at TelePacific Communications, which provides the VoIP "Smart Voice" service to thousands of customers.

(U) But the vice president, who spoke out about the massive DDoS attack during a presentation he made at the fall 2011 Comptel Plus Conference, said he was sharing details about the attack because the pace of many types of DDoS attacks appears to be growing and the telecommunications industry isn't sharing information about them as well as they might for the common good. TelePacific, he said, sees a multitude of daily scans against its network, and low-level attacks can occur about twice a day. But the services provider had never before seen what happened in the March period when the normal level of 34 million SIP traffic registration requests for VoIP connections suddenly shot up to 69 million and "flooded our systems," he said. "There was no calling ability."

(U) Comptel, the industry trade group for competitive communications services providers and their suppliers, says it does believe its membership is seeing an uptick in DDoS attacks and that's why it scheduled the session panel on the topic that included the TelePacific Vice President; a supervisory special agent and cybercrime supervisor at the FBI; and a principal security strategist at Cisco. In recounting the DDoS event against his company's VoIP service, the TelePacific vice president said he did contact the FBI to report the attack, but he found out that TelePacific simply did not have the necessary event-analysis information that the FBI needed to be able to successfully pursue a case. "We were not prepared," he said. "We didn't capture enough information." That situation has been rectified with new data-capture systems, he adds.

(U) Much of the DDoS attack streams did appear to be originating from China. But even if a botnet based on compromised Chinese computers was the source of the attack, that does not necessarily mean that someone in China is the culprit originating it, though that is a possibility. The vice president said there was no extortion threat accompanying the DDoS flood, and he has no idea who or what would decide to launch such a massive crippling attack against TelePacific and its customers. In the aftermath, TelePacific turned to a number of firms, including Acme Packet and Arbor Networks, for help in security and network analysis. But even installing Arbor's PeakFlow anti-DDoS equipment isn't the complete answer to the problem because when DDoS attacks are strong enough, PeakFlow can't necessarily stop the worst of them, Poe added. And TelePacific still fights against denial-of-service attacks, which often originate as traffic coming from China and Africa.

(U) The FBI supervisory special agent said many cases of network attacks which the FBI works on do appear to involve a financial motive. There have been a few cases that involved instances where a "competitor DDoSed a competitor" to make the competitor look bad. But that's unusual. More commonly, the goal for the attacker appears to be stealing information of value through the incident. **She urged service providers to join the local chapter of InfraGard, the FBI's information-sharing organization with the private sector. She said to get to know FBI people and to get their cell number to call them the minute something happens.**

(U) The TelePacific vice president said there doesn't seem to be sufficient information-sharing among services providers themselves about these types of serious attacks. Others agree. The IT community doesn't talk among itself enough about the serious problems occurring in terms of DDoS and other security events, said the Cisco security strategist. In contrast, he added, "The hacking community talks to each other all day long." He said the service providers need to understand they are a target and they need to have a plan in place for this kind of devastating event.

(U) "DDoS attacks and SYN floods are extraordinarily common today," said a senior director at Cbeyond Cloud Services, a division of Cbeyond Communications, which was attending the Comptel conference. He said telecom providers in general seem to be reluctant to talk about the problem. In a cynical sense, he even thinks some telecom providers can be seen as sometimes deriving revenue from DDoS floods that hit customers. He said that his company, which is a hosting provider, sees constant attacks against customer servers in which an attacker gains access to them or will brute force a password. The monitoring at his company does both inbound and outbound seeks to detect this, while also fending off some types of attacks with intrusion-prevention systems. But he pointed out that his own general practice also involves communicating about serious events with about half a dozen colleagues at other firms, including Hosting.com. "If I have a problem coming out of Hosting.com, I'll call them," he said. "We know each other. We call each other."

(U) DDoS and server hacking aren't the only problems service providers face. Hackers are also trying to break into the computer-based funds-transfer systems that service providers have to their banks. One conference attendee told the story of how just a few weeks ago, the chief financial officer at an undisclosed services provider was authorizing a payment transfer of more than $180,000 from his computer, when suddenly a spam explosion of pop-ups erupted on it, and a second unauthorized transfer for the same dollar amount was zapped off to a bank in Hong Kong. Fortunately, the CFO was quickly able to recover the full amount that was stolen -- minus the small charge for a wire transfer -- due to this direct attack on the CFO's computer. Speaking on security, the FBI supervisory special agent said, "The targeted email attack is the easiest way for the bad guys to get into the network." Since we live in a world where much information is readily available, attackers are using methods such as combing though public information, including social-networking sites, to find out what they can about corporate employees and their jobs.

(U) Are CIOs Too Cocky About Security? (*CIO, 28 SEP 2011*)

(U) There's been no shortage of high-profile and damaging data breaches in the past year. And the targets are widely varied-they include security firms RSA Security and HBGary Federal, defense contractors Lockheed Martin and Northrop Grumman, entertainment giant Sony, major retailers, healthcare companies and marketing firms. Despite these attacks, the ninth annual Global Information Security Survey conducted by CIO's sister publication CSO magazine and PricewaterhouseCoopers(PwC) indicates that of the 9,600-plus business and technology execs surveyed, 43 percent identify themselves as security frontrunners and believe they have a sound security strategy and are executing it effectively.

(U) "Clearly, something unusual is happening, with so many organizations viewing themselves as security leaders," says a principal in the advisory services division of PwC. In reality, "nowhere near 43 percent [are] leaders." The research director at Spire Security, has another take. "Either 43 percent are fooling themselves, or they are reaching a good level of success in setting their strategy and hitting it."

(U) To better understand the actual security-management capabilities of the respondents who said they were leaders, PwC filtered the results according to factors it thinks are markers of real leadership. To meet the criteria, a company had to have a security strategy in place, IT security had to report to senior business leadership, the company had to have reviewed its IT security policy in the past year, and if the business had suffered a breach, it had to understand the cause. "When we finished that analysis, the amount of frontrunners fell from 43 percent to 13 percent," the PwC principal says. Where does this unwarranted confidence come from? "Perhaps they didn't have bad things happen, or they're not aware that bad things have happened," he says. "That can definitely create a false sense of security."

(U) That complacency could partially explain why so many organizations have decided to defer security spending. This year, 51 percent of respondents said they were postponing security-related capital expenditures, up from 46 percent last year. Operating expenditures didn't get by unscathed either, with 48 percent of respondents saying they've deferred projects. That's up from 43 percent. That's not to say respondents aren't spending on security. They are, and they're focusing on protecting Web attack vectors and deploying technologies that aim to prevent attacks. Investment in application firewalls grew from 72 percent to 80 percent in the past year, and investment in malicious-code-detection tools rose from 72 to 83 percent.

(U) "It's good to see the investment in technologies," the PwC principal says. "However, the data shows they're not making investments in the processes necessary to make sure security policies are in place so [technology] works in sync to defend the enterprise." A business technology officer at BAE Systems Intelligence and Security, calls the security budget cuts shortsighted. Security breaches can leak product designs, ruin reputations and make a company less competitive, he points out. "If your systems are penetrated, everything that you thought you saved in budget cutbacks will be lost."

(U) Air Force Says Malware Discovered 'A Nuisance,' Not A Keylogger; Officials say Online Credential-Stealing Malware was Isolated to Mission Support Systems Separate from Flight Systems (*Darkreading, 14 OCT 2011; Eweek, 08 OCT 2011*)

(U) The US Air Force revealed in an October press statement that malware discovered on systems at its Creech Air Force Base was not a keylogger and did not impact its Remotely Piloted Aircraft, or drone, operations. The statements came in response to a Wired report that said malware had infected computers at Creech Air Force Base in Nevada -- home to the Predator and Reaper unmanned drone aircraft systems, and that it was logging the keystrokes of the pilots. Sources who spoke to Wired said the virus had been detected two weeks before, but it had neither disrupted any flight missions nor had any classified information been exposed. They said it was likely "benign," but difficult to kill.

(U) The Air Force said that its 24th division detected the malware on Sept. 15, and alerted Creech Air Force Base "regarding the malware on their portable hard drives approved for transferring information between systems." It identified the infection as a credential-stealing malware program that was discovered on a stand-alone Windows system used in its mission-support network. The malware was "more of a nuisance than an operational threat. It is not designed to transmit data or video, nor is it designed to corrupt data, files or programs on the infected computer. Our tools and processes detect this type of malware as soon as it appears on the system, preventing further reach," the Air Force said in its

statement.

(U) The infected machines were part of a separate ground control system that supports the drone operations, according to the Air Force, not the same systems that Air Force pilots use to remotely operate the drone aircraft. The malware had no impact on the drone flights, according to the statement.
An Air Force official told the Associated Press yesterday that the malware was the type used to steal usernames and passwords for users of online gambling and gaming sites.

(U) Meanwhile, an Air Force Space Command spokesperson said in a statement that the Air Force's policy is not to discuss "the operational status of our forces." "However, we felt it important to declassify portions of the information associated with this event to ensure the public understands that the detected and quarantined virus posed no threat to our operational mission and that control of our remotely piloted aircraft was never in question," said Colonel Kathleen Cook, spokesperson for Air Force Space Command. "We continue to strengthen our cyber defenses, using the latest anti-virus software and other methods to protect Air Force resources and assure our ability to execute Air Force missions. Continued education and training of all users will also help reduce the threat of malware to Department of Defense systems."

(U) An Air Force Air Combat Command spokesman, which oversees the drone program, said that it doesn't discuss specific vulnerabilities, threats and responses to its computer networks because it could help intruders refine their attacks on military systems. US armed forces rely on drones to attack and spy on enemies without risking American lives. Since President Obama assumed office, approximately 30 drones controlled by the Central Intelligence Agency have hit targets in Pakistan more than 230 times. Missiles fired from the pilotless drones have killed more than 2,000 people, including the Sept. 30 killing in Yemen of Anwar Al-Awlaki, an American-born Muslim cleric who was wanted for inciting terrorism attacks on the United States. The attack on Al-Awlaki was part of an antiterrorism surveillance campaign conducted over the southern Arabian Peninsula and the Horn of Africa.

(U) The malware affected Predator and Reaper drones, which are under the Air Force's control and fly over Afghanistan and Iraq. The bulk of the missions are controlled from the Creech air base. Ever since the WikiLeaks data breach, when hundreds of thousands of US diplomatic cables were leaked, the use of removable drives has been restricted, except at Creech and a few other Air Force bases. Crews working with Predator and Reaper used removable drives to load map updates and transport mission videos from one computer to another. It appears the malware is spreading and re-infecting systems through these removable devices. Drone units at other Air Force bases worldwide have now been ordered to stop using removable drives.

(U) At a October cyber-security summit in New York, the CEO of Kaspersky Lab, pointed out that cyber-combatants were getting increasingly more sophisticated in their targets and attacks. With computers controlling practically every aspect of daily life, there is a growing risk of a "hi-tech catastrophe" such as attacks on the electric grid happening. "People are people, they make mistakes," he said. This isn't the first time the drone fleet has been compromised. US forces discovered that Iraqi insurgents had used a software which they'd bought for a mere $26 to capture "days and days and hours and hours" of unencrypted video footage that had been sent from the Reapers and Predators in the air to the troops on the ground.

(U) British Signal Intelligence Chief Warns of 'Disturbing' Cyber Attacks (*AFP, 31 OCT 2011*)

(U) The head of British intelligence agency Government Communications Headquarters (GCHQ) recently warned of a "disturbing" rise in cyber attacks on the country's government and industry systems which he said risked damaging the economy. Iain Lobban, Director of the GCHQ, which provides Signals Intelligence (known as SIGINT) and Information Assurance (IA) for the United Kingdom, said the attacks included a "significant" but unsuccessful attempt to acquire sensitive information from the Foreign Office, in an article ahead of a global conference on cyberspace in London in October. "The volume of e-crime and attacks on government and industry systems continue to be disturbing," he wrote in The Times newspaper. This included attempts to steal British ideas and designs, he said, adding: "Such intellectual property theft doesn't just cost the companies concerned: it represents an attack on the UK's continued economic wellbeing. "We are also aware of similar techniques being employed to try to acquire sensitive information from British government computer systems, including one significant (but unsuccessful) attempt on the Foreign Office and other government departments this summer."

(U) Criminals were also using cyberspace to extort money and steal identities, Lobban said, warning: "We are witnessing the development of a global criminal market place -- a parallel black economy where cyber dollars are traded in exchange for UK citizens? credit card details." In an interview with the same newspaper, Foreign Secretary William Hague revealed that the details of credit card users were being traded on illegal websites for as little as 70 pence (80 euro cents, $1.10). Hague said a dividing line was opening up between countries who could defend themselves and their citizens against cyber crime, and those that could not. "Countries that cannot maintain cyber security of their banking system, of the intellectual property of their companies, will be at a serious disadvantage in the world," he said.

(U) COUNTERTERRORISM THREAT ITEMS FROM THE PRESS:

(U) Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States (*US Department of Justice Press Release, 11 OCT 2011*)

(U) Two individuals have been charged in New York for their alleged participation in a plot directed by elements of the Iranian government to murder the Saudi Ambassador to the United States with explosives while the Ambassador was in the United States. A criminal complaint filed in the Southern District of New York charges Manssor Arbabsiar, a 56-year-old naturalized US citizen holding both Iranian and US passports, and Gholam Shakuri, an Iran-based member of Iran's Qods Force, which is a special operations unit of the Iranian Islamic Revolutionary Guard Corps (IRGC) that is said to sponsor and promote terrorist activities abroad.

(U) Both defendants are charged with conspiracy to murder a foreign official; conspiracy to engage in foreign travel and use of interstate and foreign commerce facilities in the commission of murder-for-hire; conspiracy to use a weapon of mass destruction (explosives); and conspiracy to commit an act of international terrorism transcending national boundaries. Arbabsiar is further charged with an additional count of foreign travel and use of interstate and foreign commerce facilities in the commission of murder-for-hire. Shakuri remains at large. Arbabsiar was arrested on Sept. 29, 2011, at New York's John F. Kennedy International Airport and will make his initial appearance today before in federal court in Manhattan. He faces a maximum potential sentence of life in prison if convicted of all the charges.

(U) "The criminal complaint unsealed today exposes a deadly plot directed by factions of the Iranian government to assassinate a foreign Ambassador on US soil with explosives," said Attorney General Eric Holder. "Through the diligent and coordinated efforts of our law enforcement and intelligence agencies, we were able to disrupt this plot before anyone was harmed. We will continue to investigate this matter

vigorously and bring those who have violated any laws to justice." "The investigation leading to today's charges illustrates both the challenges and complexities of the international threat environment, and our increased ability today to bring together the intelligence and law enforcement resources necessary to better identify and disrupt those threats, regardless of their origin," said FBI Director Mueller.

(U) The Alleged Plot

(U) The criminal complaint alleges that, from the spring of 2011 to October 2011, Arbabsiar and his Iran-based co-conspirators, including Shakuri of the Qods Force, have been plotting the murder of the Saudi Ambassador to the United States. In furtherance of this conspiracy, Arbabsiar allegedly met on a number of occasions in Mexico with a DEA confidential source (CS-1) who has posed as an associate of a violent international drug trafficking cartel. According to the complaint, Arbabsiar arranged to hire CS-1 and CS-1's purported accomplices to murder the Ambassador, and Shakuri and other Iran-based co-conspirators were aware of and approved the plan. With Shakuri's approval, Arbabsiar has allegedly caused approximately $100,000 to be wired into a bank account in the United States as a down payment to CS-1 for the anticipated killing of the Ambassador, which was to take place in the United States.

(U) According to the criminal complaint, the IRCG is an arm of the Iranian military that is composed of a number of branches, one of which is the Qods Force. The Qods Force conducts sensitive covert operations abroad, including terrorist attacks, assassinations and kidnappings, and is believed to sponsor attacks against Coalition Forces in Iraq. In October 2007, the US Treasury Department designated the Qods Force for providing material support to the Taliban and other terrorist organizations.

(U) The complaint alleges that Arbabsiar met with CS-1 in Mexico on May 24, 2011, where Arbabsiar inquired as to CS-1's knowledge with respect to explosives and explained that he was interested in, among other things, attacking an embassy of Saudi Arabia. In response, CS-1 allegedly indicated that he was knowledgeable with respect to C-4 explosives. In June and July 2011, the complaint alleges, Arbabsiar returned to Mexico and held additional meetings with CS-1, where Arbabsiar explained that his associates in Iran had discussed a number of violent missions for CS-1 and his associates to perform, including the murder of the Ambassador.

(U) $1.5 Million Fee for Alleged Assassination

(U) In a July 14, 2011, meeting in Mexico, CS-1 allegedly told Arbabsiar that he would need to use four men to carry out the Ambassador's murder and that his price for carrying out the murder was $1.5 million. Arbabsiar allegedly agreed and stated that the murder of the Ambassador should be handled first, before the execution of other attacks. Arbabsiar also allegedly indicated he and his associates had $100,000 in Iran to pay CS-1 as a first payment toward the assassination and discussed the manner in which that payment would be made.

(U) During the same meeting, Arbabsiar allegedly described to CS-1 his cousin in Iran, who he said had requested that Arbabsiar find someone to carry out the Ambassador's assassination. According to the complaint, Arbabsiar indicated that his cousin was a "big general" in the Iranian military; that he focuses on matters outside Iran and that he had taken certain unspecified actions related to a bombing in Iraq.

(U) In a July 17, 2011, meeting in Mexico, CS-1 noted to Arbabsiar that one of his workers had already traveled to Washington, D.C., to surveill the Ambassador. CS-1 also raised the possibility of innocent bystander casualties. The complaint alleges that Arbabsiar made it clear that the assassination needed to go forward, despite mass casualties, telling CS-1, "They want that guy [the Ambassador] done [killed], if the hundred go with him f**k 'em." CS-1 and Arbabsiar allegedly discussed bombing a restaurant in the United States that the Ambassador frequented. When CS-1 noted that others could be killed in the attack,

including US senators who dine at the restaurant, Arbabsiar allegedly dismissed these concerns as "no big deal."

(U) On Aug. 1, and Aug. 9, 2011, with Shakuri's approval, Arbabsiar allegedly caused two overseas wire transfers totaling approximately $100,000 to be sent to an FBI undercover account as a down payment for CS-1 to carry out the assassination. Later, Arbabsiar allegedly explained to CS-1 that he would provide the remainder of the $1.5 million after the assassination. On Sept. 20, 2011, CS-1 allegedly told Arbabsiar that the operation was ready and requested that Arbabsiar either pay one half of the agreed upon price ($1.5 million) for the murder or that Arbabsiar personally travel to Mexico as collateral for the final payment of the fee. According to the complaint, Arbabsiar agreed to travel to Mexico to guarantee final payment for the murder.

(U) Arrest and Alleged Confession

(U) On or about Sept. 28, 2011, Arbabsiar flew to Mexico. Arbabsiar was refused entry into Mexico by Mexican authorities and, according to Mexican law and international agreements; he was placed on a return flight destined for his last point of departure. On Sept. 29, 2011, Arbabsiar was arrested by federal agents during a flight layover at JFK International Airport in New York. Several hours after his arrest, Arbabsiar was advised of his Miranda rights and he agreed to waive those rights and speak with law enforcement agents. During a series of Mirandized interviews, Arbabsiar allegedly confessed to his participation in the murder plot.

(U) According to the complaint, Arbabsiar also admitted to agents that, in connection with this plot, he was recruited, funded and directed by men he understood to be senior officials in Iran's Qods Force. He allegedly said these Iranian officials were aware of and approved of the use of CS-1 in connection with the plot; as well as payments to CS-1; the means by which the Ambassador would be killed in the United States and the casualties that would likely result.

(U) Arbabsiar allegedly told agents that his cousin, who he had long understood to be a senior member of the Qods Force, had approached him in the early spring of 2011 about recruiting narco-traffickers to kidnap the Ambassador. Arbabsiar told agents that he then met with the CS-1 in Mexico and discussed assassinating the Ambassador. According to the complaint, Arbabsiar said that, afterwards, he met several times in Iran with Shakuri and another senior Qods Force official, where he explained that the plan was to blow up a restaurant in the United States frequented by the Ambassador and that numerous bystanders could be killed, according to the complaint. The plan was allegedly approved by these officials.

(U) In October 2011, according to the complaint, Arbabsiar made phone calls at the direction of law enforcement to Shakuri in Iran that were monitored. During these phone calls, Shakuri allegedly confirmed that Arbabsiar should move forward with the plot to murder the Ambassador and that he should accomplish the task as quickly as possible, stating on Oct. 5, 2011, "[j]ust do it quickly, it's late . . ." The complaint alleges that Shakuri also told Arbabsiar that he would consult with his superiors about whether they would be willing to pay CS-1 additional money.

(U) Feds Warn of Possible Revenge Attacks After American Cleric's Death (*01 OCT 2011, FoxNews.com*)

(U) Federal authorities are warning that the killing of American-born cleric Anwar al-Awlaki in a CIA-led strike on his hideout in Yemen early Friday may trigger revenge attacks inside the United States and against US citizens traveling overseas. The death of the cleric, a digital jihadist, who inspired countless plots in the United States, Canada, Europe and Australia "could provide motivation for homeland attacks," according to a joint FBI and Department of Homeland Security bulletin issued in late September.

(U) The State Department put US citizens across the globe on alert for potential retaliation. The death of Awlaki, in the near term, could provide motivation for anti-American attacks worldwide from individuals or groups seeking to retaliate against US citizens or interests because of this action," the State Department said in the travel alert. "In the past Awlaki and other members of AQPA have called for attacks against the United States, US citizens and US interests," the alert reads. "Awlaki's standing as a preeminent English-language advocate of violence could potentially trigger anti-American acts worldwide to avenge his death." The air strike also killed Samir Khan of North Carolina, who edited a Jihadi Internet magazine.

(U) Justice Department background documents -- shared with the Fox News Specials Unit as part of its ongoing investigation of the cleric -- show a documented case of homegrown terrorism with ties to an international terrorist group every two to three weeks, since January 2009. In many of those cases, the suspects were avid followers of the cleric's online lectures and videos. US officials are concerned that the new generation of recruits – al Qaeda 2.0 – will seek to immortalize al-Awlaki who was born in Las Cruces New Mexico in 1971, educated in Colorado in the 90's and was an Imam in San Diego, CA. and Falls Church, Va.

(U) While the death of al-Awlaki is a body blow to the Al Qaeda affiliate, current and former intelligence officials who tracked the American cleric for nearly a decade say the demise of the terror networks most active and lethal affiliate is not imminent. "Its international arm, its propagandist is gone--that's a big setback," former CIA veteran and Department of Homeland Security Intelligence chief Charlie Allen told Fox News exclusively. Allen was the first US official to publicly identify al-Awlaki as a threat to US national security. "We shouldn't get too ebullient right now. We should take this very seriously that we still have a major problem," he said. "This Al Qaeda affiliated network remains strong and remains dangerous."

(U) What sets Al Qaeda in Yemen, behind the last two major plots against the United States using aircraft, apart from other terror groups is its bomb maker. Ibrahim al-Asiri, a Saudi, perfected a non-metallic explosive that evades traditional airport security. He was behind the failed underwear bomb in 2009 and the cargo printer bombs a year later. A Yemeni government source confirmed to Fox News that al-Asiri's fingerprints were found either in al-Awlaki's vehicle; the target of the CIA led strike, or in al-Awlaki's hide out. And while the forensics are being shared with the FBI and other US government entities, neither Yemeni nor US officials familiar with the strike would confirm reports the bomb maker was also dead.

(U) The leader of Al Qaeda in Yemen was not the American cleric, as has been often misreported, but rather a former personal aide to Bin Laden. It was the escape of Nasir al-Wuhayshi along with other al Qaeda operatives from a Yemeni prison in 2006 that laid the foundation for al Qaeda in Yemen, also known as al Qaeda in the Arabian Peninsula (AQAP). Correspondence found in Bin Laden's compound revealed that al-Wuhayshi wanted al-Awlaki to replace him as leader of the group, but bin Laden told his long time aide that he wanted to deal with someone he already knew.

(U) "There are some hardened groups," Allen said referring to al-Wuhayshi and others. The 47-year veteran of the CIA added that the number of extremists in Yemen "probably numbered between 500 and 1000 fighters" and now eclipsed those in Pakistan's tribal region. It is the base for the remaining Al Qaeda senior leadership. As Allen notes, Al Qaeda has metastasized since 9/11. It is no longer a Fortune 500 Company with a Bin Laden or an al-Zawahiri as CEO. It is a franchise operation in Yemen, Somalia and North Africa. It now includes a homegrown component, the Americans of al Qaeda 2.0; a development that was unthinkable a decade ago. "The answer is not finally a kinetic answer," Allen said. "Until we really combat the ideology, we will not be successful in diluting and overcoming this virulence that has spread and metastasized globally."

(U) Jury Convicts Three North Carolina Men in Terror Trial (*Associated Press, 13 OCT 2011*)

(U) A federal jury convicted three North Carolina men in a trial that focused on a plot to carry out terrorist attacks on the US Marine Corps base at Quantico, Va., and foreign targets. The jury in the month-long trial delivered its verdict against Mohammad Omar Aly Hassan, Ziyad Yaghi and Hysen Sherifi after deliberating for several days. Yaghi and Sherifi were convicted on all counts. Hassan was found not guilty of conspiracy to carry out attacks overseas but convicted of providing material support to terrorists.

(U) Hassan, Yaghi and Sherifi were part of a group of eight men who federal investigators say raised money, stockpiled weapons and trained in preparation for jihadist attacks against American military targets and others they deemed enemies of Islam. Three other men pleaded guilty in the case earlier this year, including Daniel Boyd, a convert to Islam whom prosecutors described as the ringleader. Boyd's two sons also pleaded guilty. Another man, Anes Subasic, is scheduled to go on trial separately in the case. The eighth suspect is still at large and believed to be living in Pakistan.

(U) Prosecutors claimed during the trial that Hassan and Yaghi attempted to travel to Israel in 2007 to meet up with Boyd and his sons to carry out an attack. During the closing argument, jurors were shown a large cache of rifles, pistols and ammunition amassed by Boyd at his rural home near Raleigh. Defense lawyers said none of the hundreds of audio recordings and video surveillance collected by the FBI ever captured Boyd or his alleged co-conspirators discussing specific plans for an attack with the defendants now on trial. The men's lawyers said the government's case amounted to prosecuting young Muslims who did little more than watch jihadist videos on computers and trade "stupid" Facebook posts in support of those fighting Americans overseas.

(U)The 2009 arrests of the men provoked anger and fear among some Raleigh-area Muslims, who worried their community was subject to aggressive scrutiny by federal law enforcement. Some members of a Raleigh mosque regularly made the five-hour round trip to New Bern to offer moral support to the three defendants on trial.

(U) Polish Police Arrest Two in IKEA Bombings in Europe (*Associated Press, 08 OCT 2011*)

(U) Two Polish men have been arrested and charged with a string of bomb attacks at IKEA stores across Europe and trying to extort millions from the Swedish furniture giant, authorities said in October. The arrests shed light on a mysterious spate of bombings that had prompted the evacuation of spooked shoppers and forced the retailer known for its affordable self-assembly furniture and bright blue-and-yellow stores to beef up security around the continent. A handful of homemade bomb attacks, which involved booby-trapped alarm clocks, occurred from May to September in France, Belgium, the

Netherlands, Germany and the Czech Republic. Two people were slightly injured in the German attack but there were no fatalities. Some of the bombs were potentially lethal, though not all detonated.

(U) Polish officials said they have significant evidence incriminating the two men for planting the explosives and trying to extort euro6 million ($8 million) from IKEA. The arrests were made after a manhunt involving investigators from across Europe. "The perpetrators prepared for this very carefully. They set up a bank account, demanded a transfer over the Internet, but fortunately the ransom was never paid," said Andrzej Matejuk, police commander with the Central Bureau of Investigation. "Significant evidence was gathered on the men which clearly points to their guilt," Matejuk said.

(U) After the last attack, in Prague, the men demanded that IKEA pay them euro6 million ($8 million) and threatened more attacks if the money wasn't paid quickly, Matejuk said at a news conference in Wroclaw. An IKEA spokeswoman said that the "detonations recently have developed into an extortion scheme, which we of course have taken very seriously." She said IKEA was informed of the arrests by Polish police but did not want to comment further at this point. "We continue to closely cooperate with the Polish police," she told The Associated Press.

(U) Both men were charged with endangering the lives of many people, extortion and racketeering and could face up to 10 years in prison. They were identified as Mikolaj G. and Adam K., both 39-year-olds from the northern Polish city of Gdynia. Their full names were not given, in accordance with Polish laws that protect the identities of suspects. Matejuk said that one of them has committed crimes in the past, including dealing drugs. The other has a very different profile: a former manager of several companies who speaks four languages and had no criminal record. Police spokesman Mariusz Sokolowski said the men were arrested Wednesday after hundreds of Polish officers worked on the case along with counterparts in the countries where the attacks occurred. "Because the bomb loads were getting stronger, there was a serious threat to the life and health of many people. Time counted," Sokolowski told the news agency PAP.

(U) Stores in Belgium, the Netherlands and France were hit by simultaneous bombings in May. Witnesses at a store in Ghent compared the explosions to large firecrackers and an employee and a security guard complained of minor ear injuries as a result of the noise. The explosion in the Netherlands destroyed a trash can. Two people suffered blast trauma and some furniture was slightly damaged in a blast in Germany in June. IKEA said at the time the explosives were different from those used in the simultaneous incidents. The most recent bombing was in the Czech Republic on Sept. 2.

(U) The attacks across Europe frightened shoppers and prompted IKEA to beef up security and vigilance at its stores. It's not clear, however, if the attacks scared off enough shoppers to hurt IKEA's income. The family-owned company last reported earnings early this year. IKEA said net income was euro2.69 billion ($3.55 billion) in the 12 months to Aug. 31, 2010. That was up from a profit of euro2.53 billion in the previous year, which was the first time the company released a full-year financial statement.

PRESENTATIONS AND OUTREACH

To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC (see below for information).

The CI Strategic Partnership Newsletter is a product of the FBI's Counterintelligence Program Coordination Section which plays a key role in protecting our sensitive technologies from our adversaries.

The Challenge: to protect United States sensitive information, technologies and thereby competitiveness in an age of globalization.

Our Solution: to foster communication and build awareness through partnerships with key public and private entities, by educating, and enabling our partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange with partners, the goal of which is to change behaviors and reduce opportunities that benefit the opposition's efforts.

The United States is a world's leader in innovation. Consider the breakthrough research and development that's taking place on the nation's campuses and in research facilities—often on behalf of the government. Sensitive research, much of which occurs in the unclassified realm, is the key to our nation's global advantage, both economically and militarily.

The Counterintelligence (CI) Program Coordination Section is responsible for determining and safeguarding those technologies which, if compromised, would result in catastrophic losses to national security. Through our partnerships with businesses, academia, and US Government agencies, the FBI and its counterintelligence community partners are able to identify and effectively protect projects of great importance to the U.S. Government. This provides the first line of defense inside facilities where research and development occurs and where intelligence services are focused.

The FBI's outreach efforts continue to evolve. This newsletter is one way we hope to expand our outreach to the elements of our "CI Domain." We continue in contacting businesses and organizations with which we have not yet made personal contact. In support of its Counterintelligence Domain/Strategic Partnership Program, the Federal Bureau of Investigation hosts an annual Research and Technology Protection (RTP) Conference for Facility Security Officers and RTP Professionals. Unclassified presentations address specific country threats to your technology, industrial and economic espionage, counterintelligence threat issues, and computer intrusion/cyber threat matters. The annual RTP Conference is offered in two locations during the year: Orlando and Clearwater.

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them

to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC. You may also be interested in scheduling a presentation of the FBI video "BETRAYED" followed by Q&A.

"Betrayed" represents a scenario where an FBI Intelligence Analyst is slowly but steadly compromised by a series of steps that ultimately fully compromise him into working on behalf of a foreign intelligence service. The video clearly demonstrates the traits and activities demonstrated by individuals who are involved in stealing classified information (or even proprietary information and trade secrets). The video also shows the passivity of co-workers who have clearly seen demonstrations of suspicious activity by the Intelligence Analyst, and how their failure to report the suspicious activity exasperates the situation.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

James "Pat" Laflin (James.Laflin@ic.fbi.gov) 813.253.1029

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000