FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

October 1, 2011
Volume 3 Issue 10

Federal Bureau of Investigation
5525 West Gray Street
Tampa, FL 33609, 813.253.1000

INSIDE THIS ISSUE:

Counterintelligence Includes Situational Awareness

As we prepare this issue of our monthly Strategic Partnership Newsletter, events of the day remind us of the need to be vigilant and aware of our surroundings. Vigilance is called for, not only within our workplaces, but in the surroundings of our offices, plants, facilities, parking lots and perimeters around all of our work sites.

The drone strike that took out Anwar al-Aulaqi and some of his accomplices today once again demonstrates the capabilities and accomplishments of the defense base in providing the war fighter with the best technology the United States has to offer.

Even as successes such as these emerge from battlefields around the world we are reminded of the frustrations expressed by terrorists of being unable to fight against these strikes from the air. On more than one occasion there have been expressions and sentiments from terrorists about striking at the manufacturing base of the drones.

Even though, at this time, there are no specific threats of this nature, the possibility certainly exists. How this type of a threat could manifest itself is certainly open for discussion, but one thing is almost certain. If an attack were being contemplated, surveillance would almost certainly precede such an incident.

That is why it is critical to be aware of our surroundings, especially around and near our work sites. Always be observant, on the lookout for anomalies, for people and things that are out of place. If you see a person taking pictures of your building, outside your perimeter fences, holding or operating electronic equipment that looks out of place, pacing a specific distance or pattern, or exhibiting any strange or unusual actions or mannerisms, report it. Report it to your security staff. Report it to the police if the action especially alarms you. If you have a doubt, don't think it merits a report because you think it's probably nothing, but it still bothers you, at least talk to a colleague or friend. Their ideas or thoughts might help solidify in your mind that what you have seen should be reported.

Never think that reporting something that might turn out to be nothing serves no purpose. Every report that is submitted, whether it be to a company's security staff, to the police, to another law enforcement agency or to the military, every report helps to build an intelligence base. A well constructed intelligence base can serve to warn, to prevent, to interdict, to stop something bad from

happening. Innocuous reports still may help to clarify other incidents and observations that might be precursors to bad events.

If in doubt, please report.

One last point to consider is what we and others have posted on the internet about ourselves and our jobs, and the work that we do. Especially of concern should be the searchable content of Facebook pages, Linkedin posts, company web pages, or just general information posted anywhere on the web that discusses our work.

Is it wise to post to the internet the fact that an individual works on drones, or with individuals that fly or operate these types of devices. If photographs are posted to the web where drones are made, repaired, operated, etc. has consideration been made to ensuring the photos don't have geo-tags associated with them, thus compromising the location where the photo was taken?

These are just general Operational Security 101 basics. We on the home front, contributing to this war effort, need to protect the security of ourselves and others that support the military through our work in the defense industry.

Be safe, be smart, don't paint a potential target on your backs, or of those around you.

ARRESTS, TRIALS AND CONVICTIONS

Former CME Group Software Engineer Indicted for Theft of Globex Computer Trade Secrets While Allegedly Planning Business to Improve Electronic Trading Exchange in China

http://www.fbi.gov/chicago/press-releases/2011/former-cme-group-software-engineer-indicted-for-theft-of-globex-computer-trade-secrets-while-allegedly-planning-business-to-improve-electronic-trading-exchange-in-china

U.S. Attorney's Office

September 28, 2011 Northern District of Illinois

(312) 353-5300

CHICAGO—A former senior software engineer for Chicago-based CME Group, Inc., was indicted today 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, announced Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, and Robert D. Grant, Special Agent in Charge of the Chicago Office of the Federal Bureau of Investigation.

Yang, 48, of Libertyville, was released on a $500,000 secured bond following his arrest on July 1 after being charged in a criminal complaint. He will be arraigned on a date to be determined in U.S. District Court. The indictment seeks forfeiture of computers and related equipment that were seized from Yang.

"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 affects 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," Mr. Fitzgerald said.

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.

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.

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.

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.

CME Group has fully cooperated with the investigation.

Each count of theft of trade secrets carries maximum penalty of 10 years in prison and a $250,000 fine. If convicted, the court must impose a reasonable sentence under the advisory United States Sentencing Guidelines.

The government is being represented by Assistant United States Attorneys Barry Jonas and Paul Tzur.

The public is reminded that an indictment contains only charges and is not evidence of guilt. The defendant is presumed innocent and is entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

Former Guard Charged with Attempting to Communicate National Defense Information to People's Republic of China

http://www.fbi.gov/washingtondc/press-releases/2011/former-guard-charged-with-attempting-to-communicate-national-defense-information-to-peoples-republic-of-china

U.S. Department of Justice

September 28, 2011

Office of Public Affairs

(202) 514-2007/ (202) 514-1888

WASHINGTON—Bryan Underwood, a former contract guard working at a U.S. Consulate in China, has been charged in a superseding indictment with one count of attempting to communicate national defense information to a foreign government, two counts of making false statements, and one count of failing to appear in court pursuant to his conditions of release.

The superseding indictment, which was returned today by a federal grand jury in the District of Columbia, was announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; and James W. McJunkin, Assistant Director in Charge of the FBI's Washington Field Office.

Underwood, 31, was first charged in an indictment on Aug. 31, 2011, with two counts of making false statements and was arrested on Sept. 1, 2011. On Sept. 21, 2011, Underwood was scheduled to appear at a status hearing in federal court in the District of Columbia, but failed to do so. The FBI located Underwood in Los Angeles and arrested him there in the early morning hours of Sept. 24, 2011. Underwood will be brought back to the District of Columbia for arraignment on the superseding indictment. If convicted of the charges against him in the superseding indictment, Underwood faces a maximum potential sentence of life in prison.

According to the superseding indictment, from about March 1, 2011, to about Aug. 5, 2011, Underwood knowingly and unlawfully attempted to communicate photographs and other information relating to the national defense to representatives of the People's Republic of China (PRC), with the intent and reason to believe that these materials would be used to the injury of the United States and to the advantage of a foreign nation.

The indictment further alleges that on Aug. 5, 2011, Underwood made a false statement when he stated to an FBI representative that he was intending to assist the FBI when he wrote a letter stating his "interest in initiating a business arrangement" with the PRC. Underwood also made a false statement, according to the indictment, when he stated to an FBI representative that he was intending to assist the FBI when he took certain photographs of his place of work. Finally, the indictment alleges that Underwood failed to appear in court on Sept. 21, 2011 in accordance with the conditions of his release, after his initial arrest on Aug. 31, 2011.

"As this case demonstrates, we remain vigilant in protecting America's secrets and in bringing to justice those who attempt to compromise them," said Assistant Attorney General Monaco.

"Our national security depends upon our ability to keep our most sensitive information confidential. Bryan Underwood is charged with trying to pass American secrets to China and then lying to cover up his betrayal," said U.S. Attorney Machen. "I want to congratulate the FBI for so quickly tracking down this defendant in California so that he could be brought back to the District of Columbia to face these charges."

"The FBI is committed to working with our partners in the U.S. Government to prevent the compromise of U.S. national security information by those who would attempt to sell it for personal gain," said FBI Assistant Director in Charge McJunkin. "Those who seek to flee from justice should know that the FBI will locate and apprehend them."

This investigation was conducted by the FBI's Washington Field Office, with assistance from the State Department's Bureau of Diplomatic Security. The prosecution is being handled by the U.S. Attorney's Office for the District of Columbia and Trial Attorney Ryan Fayhee from the Counterespionage Section of the Justice Department's National Security Division.

Pakistani National Pleads Guilty in Scheme to Illegally Export Restricted Nuclear Materials to Pakistan

http://www.fbi.gov/baltimore/press-releases/2011/pakistani-national-pleads-guilty-in-scheme-to-illegally-export-restricted-nuclear-materials-to-pakistan

U.S. Attorney's Office

September 09, 2011

District of Maryland

(410) 209-4800

BALTIMORE—Nadeem Akhtar, age 46, of Silver Spring, Maryland, pleaded guilty today to conspiring to commit export violations and to defraud the United States in connection with a scheme to illegally export nuclear-related materials.

The plea agreement was announced by United States Attorney for the District of Maryland Rod J. Rosenstein; Special Agent in Charge Richard A. McFeely of the Federal Bureau of Investigation; and Special Agent in Charge Rick Shimon of the U.S. Department of Commerce, Office of Export Enforcement's Washington Field Office.

"The United States regulates the export of items that can be used in nuclear facilities, requiring a purchaser to truthfully disclose the end user," said U.S. Attorney Rod J. Rosenstein. "Nadeem Akhtar conspired to violate export regulations by selling controlled items while misrepresenting what they were and to whom they would be sold."

"U.S. businesses that produce regulated technology must remain vigilant about purchasers who misrepresent the intended use, especially as it relates to foreign transactions," said FBI Special Agent in Charge Richard A. McFeely. "We cannot let our guard down in keeping regulated technology from reaching those who are prohibited from acquiring it."

"This conviction is the product of a vigorous, cooperative joint-agency investigation focused on denying and disrupting the illegal export of controlled nuclear technology destined for Pakistan," said Eric L. Hirschhorn, Under Secretary of Commerce for Industry and Security. "We will continue to work aggressively to identify and apprehend willful proliferators, no matter where they operate, in order to guard against these types of national security threats."

According to his plea agreement, Akhtar, a Pakistani national and lawful permanent resident of the U.S., owns Computer Communication USA (CC-USA).

From October 2005 through March 11, 2010, Akhtar and his conspirators used CC-USA to obtain or attempt to obtain radiation detection devices, resins for coolant water purification, calibration and switching equipment, attenuators and surface refinishing abrasives for export to restricted entities in Pakistan. Due to their use in both commercial and military applications, a license would be required to export these items to an end-user of concern or if exported in support of a prohibited end-use, such as activities related to related to nuclear explosives, nuclear reactors, or the processing and production of nuclear-related materials. Other items that Akhtar unlawfully procured or exported, or attempted to procure or export, to restricted entities in Pakistan include mechanical and electrical valves, cranes and scissor lifts. The total worth of all of these items exceeds $400,000.

The restricted entities in Pakistan included organizations of concern to the U.S. government as acting contrary to the national security or foreign policy interests of the United States. These restricted entities included: Pakistan's Space and Upper Atmosphere Research Commission; and the Pakistan Atomic Energy Commission (PAEC) and its subordinate entities, such as the Chasma Nuclear Power Plant I in Kundian, Pakistan and the research reactor maintained by the Pakistan Institute of Engineering and Applied Sciences, a constituent institution of the PAEC in Nilare, Pakistan, specializing in nuclear-related research and

development. Exports of commodities to these organizations were prohibited absent the issuance of an export license.

Akhtar attempted to evade export regulations and licensing requirements by: undervaluing and falsely describing the items being exported; failing to reveal the true end-user by using third parties and/or real and fake business entities/locations in Pakistan, Dubai, and the United States; using individuals in Illinois and California to procure items for him under false pretenses; shipping items to his residences in Maryland so it would appear as though his company was the actual purchaser/end-user of the items; and transhipping the items from the U.S. through the UAE.

Akhtar took direction from the owner of a trading company located in Karachi, Pakistan, who had business relationships with governmental entities in Pakistan. This individual would obtain orders for nuclear-related and other commodities from Pakistani government entities identified above, and then direct Akhtar as to what commodities to purchase in the United States for export to Pakistan, and the methods to be used to conceal the true nature, value and end-user of the items. Akhtar would then negotiate prices with manufacturers and suppliers of commodities sought in the U.S. and arrange for shipment of the commodities. Akhtar's co-conspirators included individuals in Pakistan, Dubai, UAE, and New York associated with the owner of the Pakistani trading company. The owner usually paid Akhtar a commission of five to seven and a half percent of the cost of each item Akhtar obtained for export from the U.S.

Akhtar faces a maximum sentence of five years in prison and a $250,000 fine, and remains detained in federal custody. U.S. District Judge J. Frederick Motz has scheduled sentencing for January 6, 2012, at 9:30 a.m.

United States Attorney Rod J. Rosenstein praised the FBI and the Department of Commerce, Office of Export Enforcement for their work in the investigation. Mr. Rosenstein thanked Assistant United States Attorney Christine Manuelian, who is prosecuting the case.

California man sentenced to nearly 4 years in prison for attempting to export military items to Iran

http://www.ice.gov/news/releases/1109/110912wilmington.htm

September 12, 2011

Wilmington, DE

WILMINGTON, Del. — A California man was sentenced to 46 months in federal prison for attempting to export military items to the Islamic Republic of Iran. The sentence is the result of an extensive investigation led by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI).

Marc Knapp, 35, of Simi Valley, Calif., pleaded guilty on Jan. 13, 2011, to engaging in a seven-month course of criminal conduct involving illegal exports to Hungary and attempted exports to the Islamic Republic of Iran and Russia.

The announcement was made by U.S. Attorney Charles M. Oberly, III, District of Delaware; and John P. Kelleghan, special agent in charge of HSI in Philadelphia. "Today's sentencing underscores HSI's commitment to ensuring that those who are willing to put America's national security at risk, are held accountable," said Kelleghan. "HSI is committed to pursuing technology and weapons smuggling crimes and continuing to lead the fight in counter proliferation investigations."

Knapp was charged with one count of violating the International Emergency Economic Powers Act, Title 50, United States Code, Sections 1702 and 1705(c), and Executive Order 13222, and Title 31, Code of Federal Regulations, Sections 560.204-560.205, and one count of violating the Arms Export Control Act, Title 22, United States Code, Sections 2778(b)(2) and 2778(c), and Title 22, Code of Federal Regulations, Sections 121.1, 123.1, and 127.1.

Knapp's conduct involved the illegal export and attempted export of the following U.S. defense articles:

An F-5B Tiger II fighter jet;

Five (5) CSU-13 Anti-Gravity (Anti-G) Flight Suits, which are worn by pilots to counteract the forces of gravity and acceleration;

One F-14 NATOPS emergency procedures manual, which is designed for use by pilots during in-flight emergencies in F-14A & B (Tomcat), F-5 (Tiger II) and F-4B (Phantom) fighter jets;

Three (3) electronic versions of the NATOPS emergency procedures manual;

Four (4) AN/PRC-149 Survival radios, which are hand-held search and rescue radios used primarily by U.S. Navy pilots as an emergency locator beacon; and

Two (2) F-14 (GRU-7A) Ejection Seats.

According to court documents, a cooperating defendant introduced Knapp to an undercover HSI special agent ("UC"). Between December 2009 and July 2010,

the UC met with Knapp on several occasions, at locations in California, Pennsylvania, Delaware, and Budapest, Hungary. During the meetings, Knapp informed the UC that he had various defense items for sale. He also admitted to procuring an F-14 (GRU-7A Ejection Seat), which was sold to the UC by the cooperating defendant. Over the course of their interaction, Knapp provided the UC with various lists containing items for sale, and he sent photographs and descriptions to the UC via email.

On two occasions, Knapp exported items outside the United States. On Feb. 22, 2010, Knapp exported two CSU-13 anti-gravity flight suits and a NATOPS emergency procedures manual to an address in Hungary; and on May 13, 2010, Knapp exported an additional three CSU- 13 anti-gravity flight suits to an address in Hungary. On a third occasion, Knapp sold the UC an F-14 (GRU-7A) ejection seat. On March 17, 2010, Knapp delivered the seat to a shipping company located in California. Knapp identified the item to the shipping company as a "museum display chair," and he provided the shipping company with a consignee's address in Denmark from which it was to be transshipped to Iran. After Knapp left the shipping company, HSI agents seized the ejection seat prior to its export outside the United States.

Knapp first broached the idea of obtaining an F-5 fighter jet from a source in California to sell to the UC in January 2010. Knapp told the UC that the "Iranians" might be interested in various items, including the F-5 fighter jet, and stated that he was not concerned whether the jet or the other items ended up in Iran. Knapp stated on Jan. 4, 2010: "We're essentially … for lack of a better term … leveling the playing field…."

Knapp also asked the UC whether he had customers in China or Russia who would be interested in pilot emergency radios for use in locating downed pilots. Knapp explained that the customers would be able to "just listen in" to locate the downed pilot, and would therefore be interested in reverse-engineering the radios.

During a Jan. 13, 2010 meeting in California, Knapp took the UC to an airport to inspect the aircraft. Over the course of the next several months, the UC and Knapp had multiple conversations regarding transporting the aircraft from California to a freight forwarder in Delaware; determining appropriate transshipment points to Iran; and devising a payment scheme. They also arranged to meet in Budapest, Hungary, to discuss the purchase.

On April 29 and 30, 2010, the UC and another undercover law enforcement officer posing as an Iranian intermediary, met with Knapp in Budapest. During the meetings, Knapp explained that he would have a contact fly the F-5 from California to the East Coast, where it would subsequently be crated and shipped

to Hungary for transshipment to Iran. Knapp said that the F-5 would be flown cross country using "uncontrolled" airports. Knapp also displayed additional photographs of the F-5 on his laptop computer. Knapp also discussed making payment for the F-5 into a "trust" and setting up documents to make the payment look like a "gift" or a "loan". Knapp also stated:

"... [A]s more and more time goes on, I'm starting to hate the U.S. more and more…."

On July 9, 2010, Knapp sent a contract for the F-5 fighter jet to the UC via the United States mail. The body of the contract (entitled "Contract for acquisition and transport of F-5B from CA to DE") set forth in detail the purchase price and terms for the sale of the aircraft. The contract further set forth the timing (approximately four weeks) for flying the F-5 to Delaware after the UC transferred $3.25 million into a bank account specified by Knapp. In addition, the contract provided terms for insurance, registration, and operational costs of flying the aircraft from California to Delaware. Knapp further noted that his requested commission would be $500,000, "with 50% paid on the date of arrival and landing of the aircraft at the DE (New Castle) or other agreed on airport, and 50% paid at the time of arrival at destination."

On July 20, 2010, Knapp met with the UC at a location in Wilmington, Del. Knapp brought to the meeting various defense items, including the four AN/PRC-149 handheld search and rescue radios, which the UC agreed to purchase for $11,000. The UC told Knapp the customer was Russian, to which Knapp replied:

"Awesome." Knapp amplified: "Whoever your customer is, I'm happy with."

Knapp stated that he was going to open an offshore bank account for the proceeds of the F-5 sale. Knapp and the UC discussed the logistics of flying the F-5 fighter jet from California to Delaware, and preparing the jet for transshipment to Iran. UC told Knapp that the Iranians expected Knapp to make a personal guarantee that the aircraft would arrive in Iran and that it would be operational. Knapp explained that the Iranians would know that it was in working order based upon his transport of the plane from California to Delaware. He further stated that what the Iranians had already seen in photographs was what they would get. According to Knapp, the only thing he would not be able to test was the weapons systems. The UC asked whether he could tell the Iranians that Marc Knapp personally guaranteed the aircraft, to which Knapp replied that he could. The parties then signed the contract.

Knapp was provided with a power of attorney form for use in exporting the F-5. He stated that he would use a false name and said that he would describe the item to be shipped as a "Museum Display Shell."

Following the meeting, HSI special agents placed him under arrest.
This case was prosecuted by Assistant U.S. Attorneys David L. Hall and Robert F. Kravetz.

Noted Scientist Pleads Guilty to Attempted Espionage

http://www.justice.gov/opa/pr/2011/September/11-nsd-1142.html

Office of Public Affairs FOR IMMEDIATE RELEASE

Wednesday, September 7, 2011

Scientist Arrested in 2009 Following Undercover Operation

WASHINGTON - Stewart David Nozette, a scientist who once worked for the Department of Energy, the Department of Defense, the National Aeronautics and Space Administration and the White House's National Space Council, pleaded guilty today to attempted espionage for providing classified information to a person he believed to be an Israeli intelligence officer.

The guilty plea, which took place this morning in the U.S. District Court for the District of Columbia, was announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; and James W. McJunkin, Assistant Director in Charge of the FBI's Washington Field Office.

Nozette, 54, of Chevy Chase, Md., pleaded guilty to one count of attempted espionage. Senior Judge Paul L. Friedman, who presided at the plea hearing, scheduled a status hearing for Nov. 15, 2011. No sentencing date was set. The plea agreement, which is subject to the judge's approval, calls for an agreed-upon prison term of 13 years.

Nozette has been in custody since his arrest on Oct. 19, 2009. FBI agents arrested him following an undercover operation in which he provided classified materials on three occasions, including one occasion that forms the basis for today's guilty plea. He was subsequently indicted by a federal grand jury. The indictment does not allege that the government of Israel or anyone acting on its behalf committed any offense under U.S. laws in this case.

"Stewart Nozette betrayed America's trust by attempting to sell some of the nation's most closely-guarded secrets for profit. Today, he is being held accountable for his actions. As this case demonstrates, we remain vigilant in

protecting America's secrets and in bringing to justice those who compromise them," said Assistant Attorney General Monaco.
"Stewart Nozette was once a trusted scientist who maintained high-level government security clearances and was frequently granted access to classified information relating to our national defense. Today he is a disgraced criminal who was caught red-handed attempting to trade American secrets for personal profit. He will now have the next 13 years behind bars to contemplate his betrayal," said U.S. Attorney Machen. "The FBI and its partners deserve tremendous credit for their outstanding work on this case. This investigation and prosecution demonstrate our commitment to identifying and punishing those who would put our national security at risk."

"Preventing the loss or compromise of high-technology and vital national security information is a top priority of the FBI," said Assistant Director in Charge McJunkin. "This case is a prime example of what happens when a person decides to sell our nation's most valuable secrets for individual gain."

Background

Nozette received a Ph.D. in Planetary Sciences from the Massachusetts Institute of Technology in 1983. He has worked in various capacities on behalf of the U.S. government in the development of state-of-the-art programs in defense and space. For example, Nozette worked at the White House on the National Space Council, Executive Office of the President, from approximately 1989 through 1990. He also worked as a physicist for the U.S. Department of Energy's Lawrence Livermore National Laboratory from approximately 1990 to 1999, where he designed highly advanced technology.

Among other things, Nozette assisted in the development of the Clementine bi-static radar experiment which purportedly discovered water ice on the south pole of the moon. A version of the Clementine satellite currently hangs on display at the National Air and Space Museum of the Smithsonian Institution in Washington, D.C., and was later hailed as the vanguard of the new "faster, cheaper, better" revolution in space exploration.

Nozette was also the president, treasurer and director of the Alliance for Competitive Technology (ACT), a non-profit organization that he organized in March 1990. Between January 2000 and February 2006, Nozette, through his company, ACT, entered into agreements with several government agencies to develop highly advanced technology. Nozette performed some of this research and development at the U.S. Naval Research Laboratory in Washington, D.C., the Defense Advanced Research Projects Agency in Arlington, Va., and the National Aeronautics and Space Administration Goddard Space Flight Center in Greenbelt, Md.

According to a factual proffer in support of the guilty plea, from 1989 through 2006, Nozette held security clearances as high as TOP SECRET and had regular, frequent access to classified information and documents related to the national defense of the United States. The factual proffer also provides details about the undercover operation that led to Nozette's arrest.

The Investigation

According to the factual proffer, on Feb. 16, 2007, law enforcement agents executed a search warrant at Nozette's home in Maryland as part of a fraud investigation and found classified documents. Further investigation into the classified documents revealed that in 2002, Nozette sent an e-mail threatening to take a classified program he was working on, "to [foreign country] or Israel and do it there selling internationally..." As a result of this and other information giving rise to suspicion of espionage, the FBI decided to conduct an undercover operation.

On Sept. 3, 2009, Nozette was contacted via telephone by an individual purporting to be an Israeli intelligence officer from the Mossad, but who was, in fact, an undercover employee of the FBI. During that call, the defendant agreed to meet with the undercover employee that day on Connecticut Avenue N.W., in front of the Mayflower Hotel in downtown Washington, D.C.

Later that day, Nozette met with the undercover employee and had lunch in the restaurant of the Mayflower Hotel. After the undercover employee made it clear that he was a "Mossad" agent, Nozette stated, "Good. Happy to be of assistance."

After lunch in the hotel restaurant, Nozette and the undercover employee retired to a hotel suite to continue their discussion. During the conversation, the defendant informed the undercover employee that he had clearances "all the way to Top Secret SCI, I had nuclear…," that "anything that the U.S. has done in space I've seen," and that he would provide classified information for money and a foreign passport to a country without extradition to the United States.

The defendant and the undercover employee met again on Sept. 4, 2009, at the Mayflower Hotel. During this encounter, Nozette assured the undercover employee that, although he no longer had legal access to any classified information at a U.S. government facility, he could, nonetheless, recall the classified information to which he had been granted access. The defendant said, "It's in my" head, and pointed to his head.

Undercover Operation Continues

On Sept. 10, 2009, FBI agents left a letter in the prearranged "dead drop" facility for the defendant. In the letter, the FBI asked Nozette to answer a list of questions concerning classified U.S. satellite information. FBI agents also provided signature cards, in the defendant's true name and an alias, for Nozette to sign and asked the defendant to provide four passport sized photographs for the Israeli passport the defendant requested. The FBI agents also left $2,000 cash for the defendant in the "dead drop" facility, which Nozette retrieved the same day, along with the questions and signature cards.

On Sept. 16, 2009, Nozette left a manila envelope in the "dead drop" facility in the District of Columbia. One of the "answers" provided by the defendant contained information classified as SECRET/SCI which related to the national defense, in that it directly concerned classified aspects and mission capabilities of a prototype overhead collection system and which disclosure would negate the ability to support military and intelligence operations. In addition to disclosing SECRET/SCI information, Nozette offered to reveal additional classified information that directly concerned nuclear weaponry, military spacecraft or satellites, and other major weapons systems.

On Sept. 17, 2009, FBI agents left a second communication in the "dead drop" facility for the defendant. In the letter, the FBI asked Nozette to answer another list of questions concerning classified U.S. satellite information. Nozette retrieved the questions from the "dead drop" facility later that same day.
On Oct. 1, 2009, Nozette left a manila envelope in the "dead drop" facility in the District of Columbia. The FBI also left a cash payment of $9,000 in the "dead drop" facility. Later that day, the FBI agents retrieved the sealed manila envelope left by the defendant. Inside the envelope, FBI agents discovered the encrypted thumb drive that was provided to Nozette on Sept. 17, 2009, which included another set of "answers" from the defendant. The "answers" contained information classified as TOP SECRET/SCI and other information classified as SECRET/SCI. This classified information related to the national defense, in that it directly concerned satellites, early warning systems, means of defense or retaliation against large-scale attack, communications intelligence information, and major elements of defense strategy. (This information is what formed the basis for the charge in today's guilty plea.)

On Oct. 5, 2009, Nozette left a manila envelope in the "dead drop" facility in the District of Columbia. Later that day, the FBI agents retrieved the sealed manila envelope left by the defendant. Inside the envelope, FBI agents discovered the encrypted thumb drive that was provided to Nozette on Oct. 1, 2009, which included another set of "answers" from the defendant. The "answers" contained information classified as TOP SECRET/SAR. This classified information related to the national defense, in that it directly concerned capabilities of a U.S. military weapon system research and development effort.

Nozette and the undercover employee met again on Oct. 19, 2009, at the Mayflower Hotel. During that meeting, the following exchanges took place:

NOZETTE: "So, uh, I gave you even in this first run, some of the most classified information that there is. . . . I've sort of crossed the Rubicon. . . . Now the, uh, so I think when I said like fifty K, I think that was probably too low. . . .The cost to the U.S. Government was two hundred million. . . . to develop it all. Uh, and then that's not including the launching of it. . .Uh, integrating the satellites. . . . So if you say okay that probably brings it to almost a billion dollars. . . So I tell ya at least two hundred million so I would say, you know, theoretically I should charge you certainly, you know, at most a one percent." Nozette was arrested soon after he made these statements. He was subsequently indicted on four charges of attempted espionage. Under the plea agreement, Nozette pleaded guilty to the third count of the indictment, arising out of his passing of TOP SECRET/SCI information on Oct. 1, 2009.

At the time of his arrest, Nozette was awaiting sentencing in another federal case. On Jan. 30, 2009, he pleaded guilty in the U.S. District Court for the District of Columbia to charges of conspiracy to defraud the U.S. government with respect to false claims and tax evasion in an amount up to $399,999. In that case, Nozette agreed to pay restitution of $265,205 to the U.S. government. Nozette is awaiting sentencing in the case. Under terms of today's plea, the sentence in the fraud case is to run concurrently with the sentence for attempted espionage.

This investigation was conducted by the FBI's Washington Field Office, with assistance from the Naval Criminal Investigative Service, Naval Audit Service, National Reconnaissance Office, Air Force Office of Special Investigations, Defense Computer Forensics Laboratory, Defense Advanced Research Projects Agency, Defense Criminal Investigative Service, Defense Contract Audit Agency, U.S. Army 902nd Military Intelligence Group, National Aeronautics and Space Administration (NASA) Office of Counterintelligence, NASA Office of Inspector General, Department of Energy , Internal Revenue Service (IRS) Criminal Investigation Division, IRS Tax Exempt & Government Entities group, U.S. Customs and Border Protection and U.S. Postal Inspection Service, as well as other partners in the U.S. intelligence community.

The prosecution is being handled by Trial Attorneys Deborah A. Curtis and Heather M. Schmidt, from the Counterespionage Section of the Justice Department's National Security Division, and Assistant U.S. Attorney Anthony Asuncion, from the U.S. Attorney's Office for the District of Columbia.

TECHNIQUES, METHODS, TARGETS

Affirmation of the conviction and sentencing of Dongfan "Greg" Chung

http://www.ca9.uscourts.gov/datastore/opinions/2011/09/26/10-50074.pdf

The conviction of Greg Chung for violations of the Economic Espionage Act of 1996 was a landmark prosecution and conviction. This case represented the first instance where a defendant charged with committing Economic Espionage actually went to full trial. Economic Espionage is a rare charge, and in all previous instances, individuals charged had pleaded guilty and made plea agreements. By going to full trial (albeit a bench trial, heard only by a judge versus the more common trial by full jury) the prosecution and defense were both able to argue the merits of their respective positions.

The finding of guilt by Judge Carney, the nearly 16 year prison sentence, and the affirmation by the Ninth Circuit of the conviction and sentencing all serve to send a strong message to individuals contemplating similar activities on behalf of a foreign power.

Because this significant trial is so succinctly summarized in the below opinion, a reader can clearly see the methods and techniques used by an individual committing this type of crime. Accordingly, we are devoting significant space in this month's newsletter to the decision of the United States Court of Appeals for the Ninth Circuit in the case of Dongfan Greg Chung.

PORTIONS OF THIS DECISION HAVE BEEN EDITED. PLEASE REVIEW THE DECISION IN ITS ENTIRETY AT THE ABOVE HYPERTEXT LINK

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, No. 10-50074

DONGFAN "GREG" CHUNG, CJC-1

Appeal from the United States District Court for the Central District of California

Cormac J. Carney, District Judge, Presiding

Argued and Submitted February 17, 2011—Pasadena, California

Filed September 26, 2011 Before: Alfred T. Goodwin, Andrew J. Kleinfeld, and

Susan P. Graber, Circuit Judges.

Opinion by Judge Graber

COUNSEL

John D. Cline, Law Office of John D. Cline, San Francisco, California, for the defendant-appellant.

Gregory W. Staples, Assistant United States Attorney, Santa Ana, California, for the plaintiff-appellee.

OPINION

GRABER, Circuit Judge:

Defendant Dongfan "Greg" Chung, a former Boeing engineer who gave technological information to China, appeals 18272 UNITED STATES v. CHUNG his convictions on six counts of violating the Economic Espionage Act of 1996 ("EEA"), 18 U.S.C. § 1831(a)(1), (3); on one count of conspiring to violate the EEA, 18 U.S.C. § 371; on one count of acting as an unregistered foreign agent, 18 U.S.C. § 951; and on one count of making a false statement to federal agents, 18 U.S.C. § 1001.

Defendant argues primarily that his convictions were not supported by sufficient evidence.

Alternatively, Defendant contends that he is entitled to a new trial because the government failed to turn over exculpatory information in violation of its duty under Brady v. Maryland, 373 U.S. 83 (1963), and because the district court made several erroneous evidentiary rulings. Finally, he challenges the district court's calculation of his offense level under the United States Sentencing Guidelines.

For the reasons that follow, we affirm.

BACKGROUND

A. Investigation and Conviction

Defendant was born in China in 1936 and became a naturalized citizen of the United States in 1972. He began working as a civil engineer at Boeing in 1964. With the exception of a few years spent at McDonnell Douglas, Defendant

worked for either Rockwell or Boeing until September 2002, when his division relocated and he retired.

During his employment with Rockwell and Boeing, Defendant worked mainly as a stress analyst on the forward fuselage section of the space shuttle. After retiring, Defendant returned to Boeing as a contractor in 2003 to help evaluate the crash of the space shuttle Columbia. He remained at Boeing until September 11, 2006, when federal agents searched his home and discovered a trove of Boeing technical documents stored beneath the house.

Federal agents first suspected that Defendant was spying for China during their investigation of Chi Mak, another engineer who worked for a naval defense contractor.

In October 2005, agents searched Chi Mak's residence and found Defendant's contact information in several of Chi Mak's address books. During a second search of Chi Mak's home in June 2006, agents found a letter dated May 2, 1987, addressed to Defendant from Gu Weihao, who was a senior official with the China Aviation Industry Corporation, a Chinese government ministry. In that letter, Gu Weihao asked Defendant to provide information about airplanes and the space shuttle and thanked Defendant for previously providing unspecified information to China. The federal agents also found what they considered to be a "tasking list" in Chi Mak's home. Although the list itself was not addressed to anyone in particular, it requested information about aviation technologies.

Because Chi Mak did not have access to aviation technology, the Federal Bureau of Investigation ("FBI") suspected that the list was meant for Defendant.

Following those discoveries, federal agents began to conduct surveillance and trash searches at Defendant's home. In August and September 2006, agents discovered that Defendant was disposing of Boeing technical documents by hiding them between the pages of Chinese-language newspapers, which he then left out for trash collection.

On September 11, 2006, agents interviewed Defendant and, with Defendant's consent, searched his home. They discovered that Defendant possessed more than 300,000 pages of Boeing and Rockwell documents, many of which related to the space shuttle, Delta IV Rocket, F-15 Fighter, B-52 Bomber, and Chinook Helicopter. Approximately 250,000 pages of those documents were kept in binders in an unfinished storage area beneath Defendant's house. Agents also recovered business cards, letters, briefings, documents related to travel,

numbered lists of technical information related to aerospace or the space shuttle program, and Defendant's journals.

A grand jury indicted Defendant on February 6, 2008. After a bench trial, he was convicted on count 1 for conspiracy to commit economic espionage, on counts 2 through 7 for economic espionage, on count 10 for acting as an unregistered foreign agent, and on count 14 for making a false statement to federal agents.

The district court then sentenced Defendant to 188 months' imprisonment and three years of supervised release.

Defendant timely appeals.

B. Evidence Presented at Trial

During the trial, the government presented many of the documents retrieved from Defendant's home. Much of the evidence, however, relates to activities and communications that predate the limitations period for the alleged crimes. The limitations period for all of the charged offenses ran from February 6, 2003, to February 6, 2008. We therefore will divide our discussion of the evidence chronologically.

1. Activities and Correspondence Predating the Limitations Period

The government introduced a letter written in 1979 by Defendant to Professor Gu (aka Ku Chen Lung) of the Harbin Institute of Technology in China. In that letter, Defendant states that he sent Professor Gu some graduate engineering course materials, a book, and some magazine articles. In closing, Defendant expressed his wish to contribute "to China's Four Modernizations." Professor Gu sent a letter to Defendant thanking him for the materials. There is no evidence in the record of any further communication between Defendant and Professor Gu.

Also in the record is a series of letters, exchanged in 1985, between Defendant and Chen Qinan, who was project manager of the China National Aero Technology Import/Export Corporation. Those letters largely concern what information Defendant should supply while visiting China for a "technical exchange." Chen Qinan sought information related to the fatigue life and structural design of aircraft and armed helicopters.

Defendant, however, offered to provide information about the space shuttle as well, even though he acknowledged that "[i]nformation regarding the space shuttle is classified as secret." He further explained to Chen Qinan that he had

only partial information regarding the helicopter's structural design because "that information is controlled by the Department of Defense." In another letter, Defendant expressed an interest in visiting several Chinese aircraft manufacturers and noted his desire to "contribute [his] expertise."

Agent Kevin Moberly, the lead case agent assigned to Defendant's case, testified that agents found, in Defendant's home, documents and briefings on laminate slides that were responsive to Chen Qinan's requests.

The government also presented a tasking list from the Nanchang Aircraft Company, a production factory of the Chinese Ministry of Aviation. Defendant received the list on July 14, 1985, during his visit to the Nanchang plant. The list requests information concerning methods for determining the fatigue life of aircraft and helicopters, including information regarding United States military specifications. Again, Agent Moberly testified that technical documents responsive to the tasking list were found in Defendant's home.

The record also contains an undated letter from Defendant to Chief Engineer Feng of the Nanchang Aircraft Company. In that letter, Defendant stated that he had "attached the answers for the questions that were not answered when I was in Nan[c]hang." He also referred to a list of books that he had collected, and he stated that Zhao Zhen Lan, the San Francisco Education Consul, would arrange for their delivery. In another letter, Defendant referred to 27 manuals that he had sent, and he attached a list cataloguing 24 structure manuals developed by Rockwell's B-1 Division.

The government presented several letters between Defendant and Gu Weihao,5 Defendant's purported "handler." All of those letters, however, predate the limitations period. The first letter from Gu Weihao to Defendant is dated March 25, 1986. After reporting that he had arrived safely in Beijing after his visit with Defendant in Los Angeles, Gu Weihao stated that he now was engaged in research on damage tolerance and expressed his hope that Defendant could "often provide [his] advice in this area."

The second letter from Gu Weihao to Defendant, dated May 2, 1987, was found in Chi Mak's home. In that letter, Gu Weihao wrote that he had asked Chi Mak to visit Defendant and to deliver a small present. Gu Weihao then requested Defendant's assistance on some "difficult technical issues" concerning the design for "trunkline aircraft (150 seats)" and the space shuttle. Specifically, he was interested in obtaining quality control information. He expressed his preference

to consult with Defendant in person and suggested a meeting in Guangzhou "to discuss with [him] in a small setting, which is very safe."

The letter further reads, in pertinent part:

We'll be responsible for all the expenses of your international travel and stay in Guangzhou. You can discuss the time and route of your trip to China with Mr. Mak in person. . . .

You may use "traveling to Hong Kong" or "visiting relatives in China" as reasons for traveling abroad, or we can ask the "Guangzhou Fine Arts Center" or the "Guangzhou Academy of Fine Arts" to extend an invitation to Mrs. Chung and have Mr. Chung, in the name of accompanying his wife, travel abroad together with her. To sum up, if you have any suggestions or if you have anything that I can help you [with] here, you can have Mr. Mak convey it to me. Normally, if you have any information, you can also pass it on to me through Mr. Mak. This channel is much safer than others.

It is your honor and China's fortune that you are able to realize your wish of dedicating yourselves to the service of your country.

In a third letter, dated April 12, 1988, Gu Weihao informed Defendant that China would soon create the Ministry of Aeronautics and Astronautics Industry. He then wrote:

[W]e are yearning for the enthusiasm and the sincere help from the foreign countries. I profoundly understand what you have in your mind. Therefore, I hope that you will introduce advanced technologies and provide information on advanced technologies. Our perspective will be greatly expanded under the scope of the new ministry. There is no need to limit the scope that we proposed while we were in the United States. Please provide at any time. It is faster and safer by forwarding through Mr. Mak.

In his next letter to Defendant, dated December 12, 1988, Gu Weihao made no requests for information but noted that he had yet to receive a reply to the letters he had written at the beginning of the year. He also sent his regards to Mr. and Mrs. Mak because they had not written him for some time.

Defendant eventually wrote back and apologized for taking so long to reply. Defendant did not refer to Gu Weihao's previous requests for information.

In a letter dated July 5, 1992, Gu Weihao reported that he had fully retired that year.

Although Defendant's journal entries show that he subsequently wrote to Gu Weihao on January 4, 1996, on May 12, 1997, and on December 18, 2001, the content of those letters is unknown. Defendant's journals also document that he hosted Gu Weihao in the United States in 1990, 1991, and 1992. The journal entries, however, merely record when Defendant picked up and dropped off Gu Weihao at the airport, where they ate, and what attractions they visited. One entry notes that Chi Mak and his wife spent an evening with Defendant and Gu Weihao.

Defendant's journals further document that, in April 2001, Defendant traveled to China and gave presentations on the space shuttle. Defendant again traveled to China in September 2002 to attend "National Day" celebrations, but his journal entries record only tourist activities while on that trip.

Immediately preceding Defendant's visit to China in 2002, however, he downloaded more than 500 space shuttle specifications from the Shuttle Drawing System ("SDS"), a restricted Boeing database. Chi Mak's name, plus his work and home phone numbers, were written on one of the SDS documents. Defendant used correction fluid to cover the user name, the date and time stamp, or other information on more than a third of the downloaded SDS documents. On one document, he covered a warning that the document contained proprietary information that could not be disclosed without permission. In January 2003, Defendant created on his home computer a file called "Specification.doc" that contained his indexing system for the downloaded SDS documents.

2. Activities and Correspondence Within the Limitations Period

In early 2003, Defendant recorded in his journal that he input and organized "spec material" on 21 separate occasions.

On March 27, 2003, Defendant wrote that he was "done with organizing Spec. material and arranging in numerical orders."

Defendant then created the file "Spec_Mod.doc" on his home computer on March 28, 2003, in which he further organized and modified the specification material. Between September 2003 and November 2003, Defendant downloaded additional SDS specifications at Boeing. Both SDS files on his home computer were last modified on December 15, 2003.

On December 27, 2003, Defendant traveled to China. There is no direct evidence in the record that establishes what Defendant did on that trip or whether he delivered SDS documents to anyone in China.

Most significantly, as discovered by federal agents on September 11, 2006, Defendant possessed approximately 300,000 pages of Boeing documents, including:

(1) more than 700 SDS documents, one of which bears Chi Mak's name and telephone numbers;

(2) documents related to the X-37 space vehicle;

(3) documents related to the thermal protection system on the International Space Station;

(4) documents related to the F-15 Fighter;

(5) documents related to the CH-46 and CH-47 Chinook Helicopter; and

(6) documents related to the B-52 Bomber.

Defendant told federal agents that he had taken the documents home because he planned to write a book. He also claimed that, although Boeing policy generally prohibited taking home work documents, his supervisor, William Novak, had given him permission to keep the documents.

The government identified six documents in Defendant's possession that allegedly contained trade secrets: four documents about a phased array antenna for the space shuttle and two documents about the Delta IV Rocket.

As noted, the government presented evidence that, between August 4, 2006, and September 1, 2006, federal agents discovered more than 1,000 pages of Boeing documents hidden between the pages of Chinese newspapers that Defendant had placed in the trash. Defendant's journals also record that, between November 12, 2004, and August 5, 2006, he "[g]ot rid of old newspaper," on 27 separate occasions.

Defendant told agents that he had disposed of the documents in that fashion because he did not want NASA documents flying around the trash disposal area.

DISCUSSION

A. Sufficiency of the Evidence

Defendant challenges, for lack of sufficient evidence, his convictions for acting as a foreign agent, violating the EEA, conspiring to violate the EEA, and making a false statement to federal agents. We review the sufficiency of the evidence de novo to determine whether, "viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt."

1. Acting as an Unregistered Foreign Agent

[1] Defendant was convicted of acting as an unregistered foreign agent pursuant to 18 U.S.C. § 951(a), which provides criminal liability for anyone "other than a diplomatic or consular officer or attaché, [who] acts in the United States as an agent of a foreign government without prior notification to the Attorney General." The statute defines "agent of a foreign government" as "an individual who agrees to operate within the United States subject to the direction or control of a foreign government or official." Id. § 951(d). The government therefore must prove that, after February 6, 2003, Defendant acted pursuant to an agreement to operate subject to the direction or control of China. Thus, in addition to proving Defendant's intent, the government must also establish that a Chinese official directed or controlled Defendant's actions during the limitations period.

[2] We conclude that, viewing the evidence in the light most favorable to the prosecution, a rational trier of fact could conclude beyond a reasonable doubt that Defendant still was acting at the direction or control of Chinese officials during the limitations period. Defendant's relevant actions during the limitations period that were proved by direct evidence included:

(1) downloading, inputting, and organizing SDS

specification materials;

(2) traveling to China in 2003;

(3) writing a letter to Gu Weihao in 2003;

(4) possessing a huge library of Boeing's and Rockwell's proprietary information; and

(5) disposing of Boeing technical documents by hiding them between the pages of newspapers, which he deposited in the trash. Sufficient circumstantial evidence ties that conduct to Chinese direction or control.

[3] There is, to begin, ample evidence that, in the mid- to late-1980s, Defendant gathered and delivered technical information regarding the structural design of aircraft in specific response to requests from Chinese officials. Although a foreign official's directions to an agent are not necessarily perpetual in duration, here the trier of fact reasonably could find that Defendant was still responding to those directions during the limitations period. Gu Weihao was the Chinese official who, in the 1980s, requested information from Defendant. In 1987, Gu Weihao wrote a letter to Defendant that fairly can be read as passing Defendant on to Chi Mak as his new "handler."

After Gu Weihao's purported retirement, Defendant continued to collect similar technical information and, it could be inferred, conspired with Chi Mak to transfer this information to China; Chi Mak was himself convicted of being an unregistered foreign agent.

Moreover, Defendant began to download the SDS documents before traveling to China in 2002; after that trip to China, he downloaded more documents and spent a great deal more time indexing them in 2003. A rational trier of fact could find that he performed this tedious task because someone in China wanted him to. Given his history and the nature of the material, a rational fact-finder could disbelieve Defendant's assertion that he planned to write a book and could instead conclude that his purpose was to assist his principal in the course of his unregistered agency.

[4] In summary, a rational finder of fact could conclude that Defendant was continuing to work for China under the direction or control of Chinese officials. Accordingly, we affirm Defendant's conviction for acting as an unregistered foreign agent.

2. Violations of the EEA

[5] Defendant was convicted of six counts of violating the EEA. The EEA provides, in pertinent part: Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; shall . . . be fined not more than $500,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831(a)(3).

Of the 300,000 pages of Boeing documents that were found in Defendant's home, the government identified six that allegedly contained trade secrets. Each document underlies a separate EEA count in the indictment. Four of the documents relate to a phased array antenna that Boeing developed for the space shuttle. The other two documents describe technology that Boeing developed for the Delta IV Rocket.

Defendant argues that the documents related to the phased array antenna did not contain trade secrets. He further contends that the government failed to prove beyond a reasonable doubt that, during the limitations period, he possessed any of the trade secret documents with the intent to benefit China.

a. The Definition of "Trade Secret"

[6] We start with whether there was sufficient evidence that the documents were trade secrets under the EEA. The EEA defines "trade secret" as information that "the owner thereof has taken reasonable measures to keep . . . secret," and that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." Id.

§ 1839(3).

Thus, the government must prove three elements:

(1) that the information is actually secret because it is neither known to, nor readily ascertainable by, the public;

(2) that the owner took reasonable measures to maintain that secrecy; and

(3) that independent economic value derived from that secrecy.

Until now, this court has had no occasion to interpret the EEA's definition, and the case law in other circuits is sparse.

The EEA's definition, however, is derived from the definition that appears in the Uniform Trade Secrets Act ("UTSA"), 7 a model statute which permits civil actions for the misappropriation of trade secrets. Thus, we consider instructive interpretations of state laws that adopted the UTSA definition without substantial modification.

With regard to the element of actual secrecy, the comment to section 1 of the UTSA explains that "information is readily ascertainable if it is available in trade

journals, reference books, or published materials." The EEA's text, however, deviates from the UTSA by identifying "the public," as opposed to "persons who can obtain economic value from [the proprietary information's] disclosure or use," as the set of parties who might know or readily ascertain the information.

There is some conflict between circuits as to whether that deviation alters the "readily ascertainable" analysis. Compare United States v. Lange, 312 F.3d 263, 267 (7th Cir. 2002) (interpreting "the public" as not necessarily meaning the "general public," but potentially "the economically relevant public" (emphasis in original)), with United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998) (observing that "the EEA alters the relevant party from whom proprietary information must be kept confidential"). Because Defendant does not contend that the secret information in this case was readily ascertainable, we need not weigh in on this issue.

As for the second element, reasonable measures for maintaining secrecy "have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on [a] 'need to know basis', and controlling plant access, Security measures, such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures.

With regard to the third element, whether the information derives independent economic value from being kept secret, courts most often consider the degree to which the secret information confers a competitive advantage on its owner.

Some courts also have considered the cost and effort necessary to develop the secret information. In any event, the analysis is fact-intensive and will vary from case to case.

b. Phased Array Antenna Documents

In the 1990s, NASA contemplated replacing the space shuttle's dish antenna with a phased array antenna. Boeing competed with other companies to supply the antenna. But Boeing was the sole-source contractor at the time for integrating technologies, including the new antenna, into the shuttle. The proposed communications upgrade required Boeing's engineers to determine the feasibility of installing the new antenna at the existing antenna locations on the shuttle's forward fuselage by enlarging or adding an opening. Those potential structural changes required conducting the appropriate stress analyses.

Additionally, engineers had to figure out how to dissipate the heat generated by the new antenna—either by reducing the number of "elements" used in the antenna or by installing an active cooling system—so that the shuttle could reenter the atmosphere safely. Ultimately, however, NASA opted not to place a phased array antenna on the shuttle.

Defendant possessed four documents related to the phased array antenna project. Two documents listed the tasks and hours necessary to complete the integration project. Those documents underlie counts 2 and 4 of the indictment. The other two documents, which underlie counts 3 and 5, were slide presentations about the communications upgrade.

Among the data contained in the slides was a list of the antenna's specifications, including the proposed number of elements in the antenna.

[7] First, we look to whether the phased array antenna documents were secret and not readily ascertainable. The government points out, and Defendant does not contest, that the tasks-and-hours lists underlying counts 2 and 4 were never made public. With regard to the slide presentations underlying counts 3 and 5, Defendant correctly argues that the documents contain information similar to that presented by Boeing engineers at a NASA-sponsored conference that was attended by Boeing's competitors. But the portions of those documents relating to the number of elements in the phased array antenna were not disclosed at the conference. Therefore, sufficient evidence supports the conclusion that all four phased array antenna documents contained secret information. Moreover, as we previously noted, Defendant does not contend that the secret information in those four documents was readily ascertainable.

[8] Next, we consider whether Boeing took reasonable measures to maintain the four documents' secrecy. Although none of the documents was kept under lock and key, Boeing implemented general physical security measures for its entire plant. Security guards required employees to show identification before entering the building, and Boeing reserved the right to search all employees' belongings and cars. Boeing also held training sessions instructing employees not to share documents with outside parties, and it required employees, including Defendant, to sign confidentiality agreements. Further, two of the four phased array documents (underlying counts 3 and 5) were marked as proprietary. Thus, there was sufficient evidence to support the conclusion that Boeing took reasonable measures to keep all four phased array antenna documents secret.

[9] Finally, Boeing derived some economic value from keeping the phased antenna array documents secret. The documents underlying counts 2 and 4 listed the tasks and hours necessary for the antenna's integration into the space shuttle.

Boeing engineer Emad Farag testified that the estimates of hours, tied to the list of tasks, would tip off competitors to more than just the costs associated with this specific project.

Although Boeing had no competitors for the integration project itself, Farag suggested that a competing company might bid against Boeing for integration work when the sole-source contract ran out. Moreover, the documents would show a competitor how Boeing operates, "not just related to the integration. . . , but it has implication for everything else we're working on." The documents, he testified, would give a competitor who studies them the advantage of knowing how Boeing accomplishes its work, including engineering and processing, and would reveal Boeing's relative costs for performing each type of work. A reasonable inference is that the information could assist a competitor in understanding how Boeing approaches problem-solving and in figuring out how best to bid on a similar project in the future, for example, by underbidding Boeing on tasks at which Boeing appears least efficient.

The antenna documents underlying counts 3 and 5 contained information regarding the number of elements in the antenna. Farag testified that such information was significant because it established that Boeing could install antenna modules on the space shuttle without a system for active cooling.

The information was economically significant, according to Farag, because it would give competitors insight into the efficiency that Boeing had obtained and because the number of elements affected the cost of developing the antenna. Importantly, Farag also testified that, unlike the integration project, the development of the antenna itself was not pursuant to a sole-source contract. That project was open to competition from other companies, and Farag specifically identified a potential competitor. Consequently, Boeing derived economic value from keeping secret the information regarding the number of elements in its proposed antenna.

[10] Viewing the evidence in the light most favorable to the prosecution, we therefore conclude that there was sufficient evidence to support the district court's finding that the documents underlying counts 2 through 5 contained trade secrets.

c. Delta IV Rocket Documents

Defendant also possessed two documents related to the Delta IV Rocket, a booster rocket that is designed to launch manned space vehicles. His possession of those documents underlies counts 6 and 7 of the indictment. Defendant does not contest the district court's finding that the Delta IV documents contained trade secrets.

d. Defendant's Intent to Benefit China

[11] To convict under § 1831 of the EEA, the government must prove that Defendant acted with the intent to benefit a "foreign government, foreign instrumentality, or foreign agent." 18 U.S.C. § 1831(a). Unlike the foreign agent count, which required evidence of a foreign government's direction or control, criminal liability under the EEA may be established on the basis of Defendant's intent alone.

We hold that there was sufficient evidence to support the district court's finding that Defendant possessed the relevant trade secret documents during the limitations period with the intent to benefit China. The government presented ample evidence

that, during the 1980s, Defendant intended to benefit China by providing technical information responsive to requests from Chinese officials and by delivering presentations to Chinese engineers. Defendant also delivered a presentation on the space shuttle to Chinese engineers in 2001. Five years later, federal agents discovered that Defendant possessed thousands of Boeing's technical documents, some of which he had downloaded and catalogued in 2003, and some of which contained trade secrets.

[12] Defendant argues that there is insufficient evidence to prove that his intent to benefit China extended to the possession of trade secrets, as opposed to technical documents in general. Given Defendant's history of passing technical documents to China, however, a rational trier of fact reasonably could infer from Defendant's more recent possession of similar documents that his intent to benefit China persisted well into the limitations period and extended to his possession of the trade secrets.

Moreover, given Defendant's history of delivering information to China, and the absence of any evidence (other than his own exculpatory testimony) regarding his scholarly or literary intentions, a rational fact-finder could reasonably discount

Defendant's explanation that he possessed the documents because he intended to write a book.

Thus, viewing the evidence in the light most favorable to the prosecution, there was sufficient evidence to conclude, beyond a reasonable doubt, that Defendant possessed the trade secret documents with the intent to benefit China. We therefore affirm Defendant's convictions for violating the EEA.

3. Conspiracy to Violate the EEA Defendant argues that there is not sufficient evidence to prove beyond a reasonable doubt that, during the limitations period, he conspired with others to violate the EEA. We disagree.

To prove a criminal conspiracy, the government must show: "

(1) an agreement to engage in criminal activity,

(2) one or more overt acts taken to implement the agreement, and

(3) the requisite intent to commit the substantive crime."

[13] Again, the record amply demonstrates that Defendant agreed to collect and transmit technical information to China in the 1980s. In May 1987, Gu Weihao wrote to Defendant to request assistance on technical issues concerning aircraft and the space shuttle. He suggested that Defendant pass any information through Chi Mak because that "channel [was] much safer than others." In 1988, Gu Weihao wrote that he hoped Defendant would "provide information on advanced technologies" and that "there [was] no need to limit the scope that we proposed while we were in the United States."

Again, Gu Weihao suggested that Defendant should forward all information through Chi Mak because it would be "safer and faster."

Thus, the record demonstrates that Defendant, Gu Weihao, and Chi Mak agreed that Defendant would pass information on advanced technologies to China. Although there is no direct evidence that Defendant specifically agreed to pass trade secrets to China, a rational trier of fact could reasonably infer from Gu Weihao's letters and from Defendant's possession of the trade secret documents that Defendant did not intend to except such documents from the scope of the agreement.

[14] The difficult issue presented by this case is whether the agreement between Defendant, Gu Weihao, and Chi Mak continued into the limitations period. Viewing the evidence in the light most favorable to the prosecution, we conclude that there is insufficient evidence to support the finding that Defendant conspired with Gu Weihao during the limitations period. The bare fact that Defendant wrote to Gu Weihao in 2003 is insufficient to prove a continuing conspiracy, given that Gu Weihao last requested information in 1988 and purportedly retired in 1992. All subsequent correspondence between Defendant and Gu Weihao that appears in the record discusses only personal issues and makes no mention of technical information.

[15] By contrast, the record does support the district court's finding that Defendant conspired with Chi Mak to pass trade secrets to China during the limitations period. As recounted above, the record shows that Defendant agreed with Chi Mak in the 1980s to deliver information on advanced technologies to China. The government also presented evidence that Defendant downloaded shuttle design documents from a restricted Boeing database in 2002, approximately four months before the limitations period began. Chi Mak's name and telephone numbers were written in Chinese on one of those documents. During the limitations period, Defendant downloaded, indexed, and modified shuttle design specifications.

Although the government does not allege that the shuttle design documents contained trade secrets, a rational trier of fact could reasonably infer from Defendant's unauthorized collection of such data that Defendant continued to work with Chi Mak to pass technological information to China. It is equally reasonable to infer that Defendant's possession of the trade secret documents was part of that same effort.

Thus, viewing the evidence in the light most favorable to the prosecution, we conclude that a rational trier of fact could have found, beyond a reasonable doubt, that Defendant conspired with Chi Mak to violate the EEA after February 6, 2003.

4. False Statement

[16] We also hold that there was sufficient evidence to support Defendant's conviction under 18 U.S.C. § 1001.9 The district court correctly found that Defendant "knowingly and willfully" made a materially false statement to federal agents when he told them that his boss, William Novak, had given him permission to take work documents home. While being interviewed by federal

agents, Defendant claimed that, though engineers generally were not allowed to do so, Novak had made an exception for him. According to Agent Moberly, Defendant explained that, when his division was "closing up shop," Novak asked him if he wanted to take the documents home because, otherwise, they were going to be destroyed.

At trial, Novak testified that, when the shuttle group moved to a smaller facility in 1999, he instructed his engineers to dispose of obsolete data in designated dumpsters and to box up unneeded data to send to a secure storage facility. Novak further testified that he did not recall telling his engineers that they could take work documents home, nor did he recall Defendant making such a request. As to the general rule and any exceptions, Novak testified:

We weren't allowed to, but occasionally I'm sure some of us if we needed to finish an assignment or something, guys would take some stuff home with the expectation to bring it back the next day or the next few days or whatever.

[17] Defendant argues that Novak's testimony was insufficient to prove that Defendant lied because Novak testified only that he could not recall giving Defendant permission.

Defendant is correct that Novak's testimony does not squarely contradict Defendant's statement. But a rational trier of fact could reasonably infer, beyond a reasonable doubt, that Defendant had not obtained exceptional permission from Novak, given Boeing's general policy against taking work documents home permanently and the care with which Boeing disposed of the obsolete documents when Defendant's division closed. Also, several Boeing engineers testified that they could take documents home temporarily, but never permanently.

Thus, viewing the evidence in the light most favorable to the prosecution, a rational trier of fact could reasonably conclude, beyond a reasonable doubt, that Defendant falsely stated that he had permission to take Boeing documents home.

PORTIONS OF THE DECISION HAVE BEEN EDITED OUT OF THIS DOCUMENT

VIEW THIS DOCUMENT IN ITS ENTIRETY AT

http://www.ca9.uscourts.gov/datastore/opinions/2011/09/26/10-50074.pdf

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

National Cyber Security Awareness Month 2011

For the eighth year in a row, October has been designated National Cyber Security Awareness Month. The goal: to reinforce the importance of protecting the cyber networks that are so much a part of our daily lives. The theme of the observance, which is sponsored by the Department of Homeland Security, is "Our Shared Responsibility," reflecting the interconnectedness of our wired and wireless world and the role of all computer users in securing cyberspace.

There's no doubt that the security of cyberspace is vitally important to our nation. As FBI Director Robert Mueller has said, "We live in a wired world...but our reliance on these networks also makes us vulnerable. Criminals can use the Internet to commit fraud and theft on a grand scale and to prey upon our children. Spies and terrorists can exploit our networks to steal our secrets, attack our critical infrastructure, and threaten our national security. And because the web offers near-total anonymity, it is difficult to discern the identity, the motives, and the location of an intruder."

Since the capabilities of our cyber adversaries—primarily foreign intelligence services, terrorist groups, and criminal enterprises—are at an all-time high, cyber security continues to be a top priority of the FBI.

More Resources
- FBI Cyber Investigations and Initiatives
- Department of Homeland Security on National Cyber Security Awareness Month website
- FBI Cyber Crime Fugitives

Working closely with our local, state, national, and international partners, we gather, analyze, and share intelligence…conduct investigations….and implement initiatives that promote cyber security. Here are some examples of what we're doing to counter cyber threats:

- We have set up cyber squads in each of our 56 field offices, with more than 1,000 specially-trained agents, analysts, and forensic examiners running complex undercover operations and examining digital evidence.

- The FBI-led National Cyber Investigative Joint Task Force (NCIJTF) coordinates cyber activities among 20 law enforcement and intelligence

community agencies that work together to identify key cyber players and schemes. The NCIJTF operates through intelligence-driven Threat Focus Cells—groups of subject matter experts comprised of agents, officers, and analysts from different agencies who collaborate and address specific cyber threats, such as botnets.

- To combat the theft of so-called intellectual property—creative expressions like trade secrets, proprietary products and parts, literature, music, and films—we take part in the National Intellectual Property Rights Coordination Center, or IPR Center. The center, which is hosted by U.S. Immigration and Customs Enforcement (ICE), brings together 17 different U.S. federal law enforcement agencies (including the FBI, ICE, and U.S. Customs and Border Protection) charged with investigating these violations, along with global partners from Canada and Mexico.
- FBI agents are embedded in five foreign police agencies (Estonia, the Netherlands, Romania, the United Kingdom, and Colombia) to assist with cyber investigations.
- We partner with industry and academia through major initiatives like InfraGard, the Internet Crime Complaint Center, and the National Cyber-Forensics & Training Alliance.
- Each year, we train approximately 500 foreign law enforcement officers in cyber investigative techniques.

Our cyber partnerships and joint initiatives are paying off, especially in the national security realm. In 2010, we strengthened our efforts to counter state-sponsored cyber threats, increasing the number of national security computer intrusion cases by 60 percent. But we also continue to see successes on the criminal side, arresting a record 202 individuals—including five of the world's top cyber criminals—for computer intrusions.

In addition to the work being done by law enforcement, you can do your part to protect cyberspace by securing your own computers and other electronic devices. Here are suggested tips on how to do that, threats to be aware of, and details on how to report cyber crimes or scams:

- Report Cyber Crime
- Get Educated on Internet Fraud
- How to Protect Your Computer
- Emerging E-Scams
- Risks of Peer-to-Peer Networks
- Safe Online Surfing Website for Kids

Internet Crime Complaint Center's (IC3) Scam Alerts

http://www.ic3.gov/media/2011/110901.aspx

September 1, 2011

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

"Mass Joinder Lawsuits" Promising Home Mortgage Relief

The IC3 has received several complaints from individuals who reported they received a letter stating they were a potential plaintiff in a "Mass Joinder" lawsuit being filed by a law firm located in California, against their mortgage companies. Consumers stated they were requested to pay non-refundable, upfront fees of $2,000 to $5,000. The law firm made a wide variety of claims and sales pitches and offered legal and litigation services, with the goal of taking money from the victim.

Lawyers seeking plaintiffs to join a class for a class action lawsuit do not seek up front commission from their class clients. Class action lawyers are typically paid on a contingency basis. In a contingency fee arrangement, an attorney receives approximately 40% of any judgment or settlement amount obtained on the client's behalf.

Warnings have been posted on-line regarding "Mass Joinder" by the California Department of Real Estate; the Better Business Bureau; as well as consumers who have been scammed and posted their experiences, insights, and warnings.

On-line Auction Site PlayStation Bundle Ad Scam

The IC3 has received several complaints from individuals who reported they received an unsolicited e-mail stating their ad for a Sony Playstation 3 Metal Gear Solid 4 PS3 80 GB Bundle has been posted and a confirmation number was enclosed for the posting. In each instance the victim claimed they did not place an ad on an on-line auction site for the Sony Playstation Bundle. Some victims stated they did not even have an on-line auction account.

Warnings have been posted on-line to beware of auction site phishing e-mail scams and specifically mention the above-mentioned scam. One warning indicated the scam was first reported in January 2009.

Fraud Trends Affecting The eCommerce Community

Ethoca recently provided the IC3 information pertaining to the increase in fraud attempts incurred by on-line merchants. Ethoca was founded under the concept of safely sharing transaction data to fight on-line credit card fraud. The company serves as a data sharing platform for merchants to stop on-line fraud and is partnered with the National Cyber Forensics and Training Alliance (NCFTA). The data received by Ethoca remains private and is only used for fraud prevention. The following information is based on Ethoca's data collection and information sharing process.

Advisory on Military Addresses

On 07/11/2011, the hacker group Anonymous posted 90,000 e-mail addresses and passwords. As a result of this posting, merchants have reported some orders containing military e-mail addresses have been identified as fraudulent. Until this time, military e-mail addresses typically meant an order was less likely to be fraudulent. The increase in fraud orders has happened within the last 30 days.

E-mail Address Tumbling

E-mail address tumbling has been around for awhile and fraudsters have used it for many years. On the other side, good consumers utilize address tagging to identify orders.

The purpose of e-mail tagging is to allow consumers to have one e-mail address for every purpose. The attractive feature of e-mail tagging is it allows the consumer to vary their e-mail address to help differentiate when placing orders, shopping, working, schooling, etc., but automatically forwards to the primary e-mail address. This feature on Gmail works in two ways, either with a period or a plus sign. The period works by allowing the consumer to take an e-mail address, JohnDoe@gmail.com, and add as many periods as the consumer wants to the e-mail address, JohnDoe.....@gmail.com, J.o.h.n.D.o.e@gmail.com, etc.

The feature most often used is the + feature, which allows a user to add additional tags to their e-mail address to easily identify how someone obtained their name. Using the above example, when shopping on-line, a consumer can tag their e-mail as JohnDoe+081811OnlineRetailerName@gmail.com. This allows the user to know they shopped on-line with a merchant on that specific day.

These features can be used in combination with rules to route e-mails into different boxes, keeping inbox e-mail volume down, and helping users be more efficient.

Fraudsters have figured out this tip and use what has been termed e-mail address tumbling, so the fraudster does not have to create unique user accounts for their many fraud attempts. So far these features have only been found to work with Gmail accounts.

OCTOBER IN COUNTERINTELLIGENCE HISTORY

- 10/01/1919: Within the Bureau of Intelligence, a division was created to handle the investigation of radicalism and the dissemination of anarchistic propaganda.
- 10/01/1951: Communist Party USA leader Gus Hall was arrested by FBI Agents at the Texas/Mexico border after he jumped bail following his conviction under the Smith Act.
- 10/03/1984: Former FBI Agent Richard Miller was arrested for violation of U.S. Espionage laws. After three trials, Miller was found guilty on 10/09/1990 in a non-jury trial.
- 10/09/1941: Attorney General Biddle approved wiretapping by the FBI. He was quoted as saying "I think that if you don't tap wires your espionage work goes out the window." He further stated "Wiretapping is a dirty business, but so is espionage."
- 10/11/1996: The Economic Espionage Act of 1996 was signed into law. It strengthened the FBI's ability to work with private industry to safeguard proprietary information, prosecute the theft of trade secrets, and made economic espionage a federal crime.
- 10/14/1949: Eleven leading members of the Communist Party USA were convicted in New York City of conspiring to violate the Smith Act.
- 10/18/1946: The paymaster of the Ludwig Ring, a Nazi spy ring operating out of South America during World War II, was arrested. Teodoro Erdmann Erich Lau was a German-born citizen of Argentina.
- 10/20/1938: A memo from FBI Director J. Edgar Hoover was sent on this date to the Attorney General and forwarded to President Roosevelt. President Roosevelt approved the memo which detailed the proposed scope of FBI Intelligence efforts relating to Subversion. Areas covered included maritime, government, industry; general strike; armed forces; educational institutions; Fascists; Nazis; organized labor; strikes and newspapers.
- 10/24/1997: Kurt Alan Stand, Theresa Marie Squillacote, and James Michael Clark were arrested and charged with conspiracy to commit espionage. The three were accused of supplying information to the Soviet Union and later South Africa over a 20 year period. A sting operation caught the three supplying classified DOD and CIA documents to undercover agents. In January 1999 Squillacote received a 21 year sentence, Stand 17 years, and Clark a 12 year sentence, all having been convicted of espionage charges.

- 10/31/1966: FBI Agents arrested Air force Staff Sergeant Herbert W. Boeckenhaupt at March Air Force Base in Riverside, CA. He was charged with conspiracy to commit espionage and was sentenced to 30 years imprisonment.

PRESENTATIONS AND OUTREACH

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