U.S. Department of Justice
Federal Bureau of Investigation

FBI COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP NEWSLETTER

October 2011

A message from Tom Weldon

Welcome to another edition of our Newsletter. Supply chain integrity is an increasing concern among our partners, both in the private business sector and academe. With same in mind, we are highlighting it here in the hopes that, together, we can proactively engage it with an aim towards neutralizing this threat in the future.

Inside this issue:

Noted Scientist Pleads Guilty to Attempted Espionage

US Department of Justice Press Release *— September 7, 2011*

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.

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.

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."

Nozette informed the

Scientist Pleads Guilty to Attempted Espionage

(Continued from page 1)

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.

After providing information on three separate occasions, 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.

"FBI" and "IC3" Phishing Scams

There is an increasing trend of phishing scams purportedly from the FBI and the Internet Crime Complaint Center (IC3). The scammers commonly use names of agents, high ranking executives and the IC3. Several recent phishing attempts involving names of FBI personnel claim to be an "official order" from the FBI Anti-Terrorist and Monetary Crimes Division, or from an alleged FBI unit in Nigeria, confirming an inheritance or containing a lottery notification, or informing recipients that they have been named the beneficiary of millions of dollars. In order to claim the money, individuals are asked to furnish Personally Identifiable Information (PII) and are often threatened with some type of penalty, such as prosecution, if they fail to comply. Specific PII information requested includes, but is not limited to, the individual's legal name, bank account information, telephone numbers, and passport information.

The FBI does not send unsolicited emails. FBI executives are briefed on certain investigations but do not personally contact the public regarding particular investigations. Neither does the IC3 send threatening letters to the public demanding payment for Internet crimes and threatening prosecution if you do not reply.

What to Do When Targeted by Phishing Scams

Do Not Respond.

Never give out personally identifiable information to unknown or unverified sources.

Do not open suspicious email attachments.

If you discover your name involved in a phishing scam, report the incident to IC3, and if it is work related, immediately contact your chief security officer.

Do not respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.

Make sure your computer is using legitimate, up-to-date antivirus software.

If you become a victim of Internet crime, file a complaint at www.ic3.gov.

Leader of International Conspiracy Convicted of Defrauding the Military

US Department of Justice Press Release—*September 7, 2011*

WASHINGTON – Roger Charles Day Jr. was found guilty late yesterday of leading an international conspiracy to sell more than $4.4 million in **nonconforming and defective parts** to the Department of Defense (DOD).

After a nine-day trial, Day, 47, formerly of Long Valley, N.J., was found guilty by the jury on all counts. Day was charged in July 2008 with conspiracy to commit wire fraud, wire fraud, conspiracy to engage in international money laundering, and conspiracy to smuggle gold out of the United States. Day was extradited from Mexico in December 2010. Day's sentencing is scheduled for Dec. 15, 2011.

According to the evidence at trial and court documents, over a four-year period Day led a conspiracy to bid on and win contracts to provide parts to the U.S. military through the Defense Logistics Agency (DLA), including through the DLA's Defense Supply Center in Richmond, Va. The parts included "critical application items," which are essential to weapons system performance or operation or to the preservation of life or safety of operation personnel. Under DOD's procurement procedures, contractors were permitted to submit electronic invoices upon shipment of the needed parts, and were paid electronically by the Defense Finance and Accounting Service.

In the course of the scheme, Day and other conspirators, operating in the United States, Canada, Mexico and Belize, formed at least 18 separate companies that posed as legitimate contractors and collectively used a computer program to win nearly 1,000 lucrative contract awards for the various companies. Day and his conspirators then shipped defective parts to the DOD on more than 300 of those contracts, receiving more than $4.4 million in payment on parts that Day purchased for less than $200,000. In all known cases, the parts sent by Day and his conspirators could not be used for their intended purpose.

Day and his co-conspirators concealed their identities through the use of multiple nominee companies and by assuming others' identities to operate the companies. When DOD requested proof that the companies had purchased and intended to supply the correct parts from approved manufacturers, Day and others submitted fabricated documents that falsely represented that the correct parts had been purchased. When DOD debarred several of the companies from doing further business with the military, Day directed his conspirators to discontinue bidding through those companies and instead formed and used new companies.

Day directed his conspirators to transfer the scheme's proceeds to offshore bank accounts and ultimately to purchase more than 3,500 ounces (over $2.2 million) in gold bars and coins. Day directed his conspirators to bring the gold bars and coins to his residence in Lo De Marcos, Mexico. On one occasion he directed them to hide the gold bars in the modified bumper of a 1979 Toyota Land Cruiser and on another occasion in the rear hatch door panel of a 1971 Austrian Pinzgauer military transport vehicle.

At sentencing, Day faces a maximum of 20 years in prison for each count of conspiracy to commit wire fraud and each count of wire fraud, 10 years in prison for each count of conspiracy to engage in international money laundering, and five years in prison for each count of conspiracy to smuggle gold out of the United States.

Prior to Day's trial, five defendants in this conspiracy pleaded guilty. Nathan Francis Victor Carroll was sentenced on Nov. 8, 2007, to 94 months in prison and was ordered to pay nearly $3.7 million in restitution. Gregory Allen Stewart was sentenced on April 29, 2008, to 75 months in prison and was ordered to pay nearly $3.7 million in restitution. Susan Crotty Neufeld was sentenced on May 14, 2008, to five years of probation and ordered to pay $47,600 in restitution for the gold coins she received. Juerg Mehr was sentenced to five years of probation on March 27, 2009. Glenn Teal was sentenced on Sept. 22, 2009, to 90 days in prison.

Know Your Supply Chain!

Top Ten Reasons for Counterfeits Entering the Supply Chain

Figure II-30: OCMs' Top Ten Reasons For Counterfeits Entering the Supply Chain	
Greater Reliance by brokers on gray market parts	42%
Greater reliance by independent distributors on gray market parts	37%
Less stringent inventory management by parts brokers	36%
Less stringent inventory management by independent distributors	28%
Insufficient chain of accountability	27%
Insufficient buying procedures	23%
Purchase of excess inventory on the open market	23%
Inadequate part purchase planning by OEMs	23%
Inadequate part purchase planning by contract manufacturers	23%
Greater reliance on contract manufacturers for procurement	23%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey, November 2009*

Maryland Man Sentenced to 30 Months in Prison for Importing and Selling Counterfeit Cisco Computer Networking Equipment

US Department of Justice Press Release *— August 18, 2011*

WASHINGTON – Donald H. Cone, 48, of Frederick, Md., was sentenced today in Alexandria, Va., to 30 months in prison for his role in a sophisticated conspiracy to import and sell counterfeit Cisco-branded computer networking equipment, announced U.S. Attorney Neil H. MacBride for the Eastern District of Virginia and Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division.

U.S. District Court Judge Gerald Bruce Lee also ordered Cone to pay $143,300 in restitution and to serve three years of supervised release following his prison term. A federal jury convicted Cone and a co-conspirator, Chun-Yu Zhao of Chantilly, Va., in May 2011 after a three-week trial. Zhao will be sentenced on Sept. 9, 2011.

According to the evidence introduced at trial, Zhao, Cone and Zhao's family members in China operated a large-scale counterfeit computer networking equipment business under the names of JDC Networking Inc. and Han Tong Technology (Hong Kong) Limited. JDC Networking Inc., located in Virginia, altered Cisco products by using pirated software, and created labels and packaging in order to mislead consumers into believing the products it sold were genuine Cisco products. To evade detection, Zhao used various names and addresses in importation documents, and hid millions of dollars of counterfeit proceeds through a web of bank accounts and real estate held in the names of family members in China.

The case was investigated by U.S. Immigration and Customs Enforcement's Homeland Security Investigations' Washington, D.C., office, as well as the Office of the Inspector General from the General Services Administration. U.S. Customs and Border Protection made a criminal referral to ICE after intercepting counterfeit products from China destined for addresses associated with Cone, Zhao and JDC Networking Inc.

Virginia Woman Sentenced to 60 Months in Prison for Importing and Selling Counterfeit Cisco Computer Networking Equipment

US Department of Justice Press Release—*September 9, 2011*

WASHINGTON – A Virginia woman was sentenced today to 60 months in prison for leading a sophisticated conspiracy to import and to sell counterfeit Cisco-branded computer networking equipment, laundering criminal proceeds and obtaining her citizenship through fraud, announced U.S. Attorney Neil H. MacBride for the Eastern District of Virginia and Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division.

At sentencing, U.S. District Court Judge Gerald Bruce Lee also ordered Chun-Yu Zhao, 43, of Chantilly, Va., to pay $2,709,238 in restitution and to pay a $17,500 fine. Zhao was also ordered to serve three years of supervised release following her prison term. In addition, Judge Lee stripped Zhao of her U.S. citizenship and ordered that the following assets be forfeited to the United States: four homes in Maryland and northern Virginia and three condominiums in Chantilly with a total value of more than $2.6 million; a Porsche Boxster, Porsche Cayenne and Mercedes sedan; and seven bank accounts containing more than $1.6 million. Zhao has been in federal custody since her July 22, 2010, arrest by agents of U.S. Immigration and Customs Enforcement (ICE).

In May 2011, following a three-week trial, a federal jury convicted Zhao of 16 felony counts, including conspiracy to commit importation fraud and to deal in counterfeit goods, importation fraud, dealing in counterfeit goods, obtaining citizenship by fraud, making false statements to law enforcement and money laundering. According to court documents, Zhao and her family members and other co-conspirators in China agreed to lie on declaration forms and to sell shipments of counterfeit Cisco-branded computer networking equipment. Zhao and her co-conspirators used counterfeit labels and packaging to mislead consumers into believing that they were purchasing genuine Cisco products. To evade detection, Zhao and her co-conspirators used various names and addresses in importation documents and hid millions of dollars of counterfeiting proceeds through a web of bank accounts and real estate held in the names of Zhao's family members. Zhao also fraudulently obtained United States citizenship based on lies on her citizenship application.

Global Impacts of Counterfeiting and Piracy

International Chamber of Commerce (ICC) report— *February 2011*

(Excerpts from the press release)

The total global economic and social impacts of counterfeit and pirated products are as much as US$775 billion every year. This includes impacts of lost tax revenue and higher government spending on law enforcement and health care. The figure is estimated to more than double to US$1.7 trillion by 2015, due in part to rapid increases in physical counterfeiting and piracy as measured by reported customs seizures and greater worldwide access to high speed Internet and mobile technologies.

International trade in fakes currently accounts for more than half of counterfeiting and piracy, and could grow to as much as US$960 billion by 2015.

"We believe that a critical element in the fight against counterfeiting and piracy is to do a better job communicating what IP [intellectual property] is and why it's such a valuable part of our economy," said ICC Secretary General Jean-Guy Carrier. "Greater recognition of the important benefits that come from IP and its protection – not just for business but for society in general – is essential in stopping the growing presence of counterfeit and pirated goods around the world."

"This illegal business activity deprives governments of revenues for vital public services, forces higher burdens on tax payers, dislocates hundreds of thousands of legitimate jobs and exposes consumers to dangerous and ineffective products." says Jeffrey Hardy, Coordinator of the ICC Business Action to Stop Counterfeiting and Piracy (BASCAP) initiative.

Supply Chain Infiltration

An excerpt from Gordon M. Snow's (Assistant Director, Cyber Division, Federal Bureau of Investigation)

Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit — *September 14, 2011*

The production, packaging, and distribution of counterfeit software or hardware used by financial institutions or critical financial networks by cyber criminals could result in the compromise of proprietary data, system disruption, or complete system failure. Gaining physical and technical access to financial institutions could be accomplished by compromising trusted suppliers of technical, computer, and security equipment, software, and hardware.

Financial firms have become regular targets of supply chain attacks. For example, ATMs have been delivered with malware installed on the systems, fake endpoints on the ATM networks have been created, and individuals have posed as ATM maintenance workers. Additionally, vendors who supply services to the banking and finance sector are constant targets of cyber criminals, including those who provide services like security, authentication, and online banking platforms.

Man Pleads Guilty to Foreign Economic Espionage

US Department of Justice Press Release—*August 30, 2011*

BOSTON—A Brookline man pleaded guilty today to foreign economic espionage. This is the first prosecution in Massachusetts for foreign economic espionage and only the eighth in the nation.

ELLIOT DOXER, 43, pleaded guilty before U.S. District Judge Denise J. Casper to one count of foreign economic espionage for providing trade secrets over an 18-month period to an undercover federal agent posing as an Israeli intelligence officer.

The parties stipulated in an agreed statement of facts that on June 22, 2006, Doxer sent an e-mail to the Israeli consulate in Boston stating that he worked in the finance department of Akamai Technologies, Inc., and was willing to provide any information that might help Israel. In later communications, Doxer said that his chief desire "was to help our homeland and our war against our enemies." He also asked for payment in light of the risks he was taking.

In September 2007, a federal agent posing as an undercover Israeli intelligence officer spoke to Doxer and established a "dead drop" where the agent and Doxer could exchange written communications. From October 2007 through March 2009, Doxer visited the dead drop at least 62 times to leave information, retrieve communications, and check for new communications.

Included in the trade secret information that Doxer provided the undercover agent were an extensive list of Akamai's customers; contracts between the company and various customers revealing contact, services, pricing, and termination date information; and a comprehensive list of the company's employees that revealed their positions and full contact information. Doxer also broadly described the company's physical and computer security systems and stated that he could travel to the foreign country and could support special and sensitive operations in his local area if needed. Because Akamai's information was disclosed only to an undercover agent from the beginning, the information was never in danger of actual exposure outside the company.

We acknowledge the government of Israel for their cooperation in this investigation, and underscore that the information does not allege that the government of Israel or anyone acting on its behalf committed any offense under U.S. laws in this case. We would also like to acknowledge and thank Akamai Technologies, Inc., for its assistance throughout all stages of the investigation and prosecution.

Doxer was arrested on October 6, 2010, on a complaint charging him with wire fraud.

That charge will be dismissed at the end of this case as part of the plea agreement. The charge of foreign economic espionage carries a maximum penalty of 15 years in prison, a three-year term of supervised release and a $500,000 fine. Judge Casper scheduled sentencing for November 30, 2011.

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

US Department of Justice Press Release—*September 28, 2011*

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.

Did You Know...

Long before it was acknowledged to be a significant criminal and national security threat, the FBI established a forward-looking organization to proactively address the issue of cyber crime.

Since its creation in 1997, the National Cyber Forensics and Training Alliance (NCFTA), based in Pittsburgh, has become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.

The NCFTA essentially works as an early-warning system. If investigators for a major banking institution, for example, notice a new kind of malware attacking their network, they immediately pass that information to other NCFTA members.

The organization draws its intelligence from hundreds of private-sector members, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's Internet Crime Complaint Center (IC3). That extensive knowledge base has helped in some of the FBI's most significant cyber cases in the past several years. Indeed, through NCFTA's efforts, hundreds of investigations have been launched, which otherwise would not have been addressed, with successful prosecutions of more than 300 cyber criminals worldwide. The NCFTA has also produced more than 400 cyber threat intelligence reports over the past three years alone.

The FBI Counterintelligence Strategic Partnership Program's Mission:

To work with academia, private industry and the intelligence community to foster proactive strategies to negate attempts by foreign adversaries to victimize US interests.

Each of the FBI's 56 field offices has a Counterintelligence Strategic Partnership Coordinator who works locally to further this mission. For additional information, assistance, or training, contact your local FBI office's Strategic Partnership Coordinator.

www.fbi.gov/about-us/investigate/counterintelligence/strategic-partnerships

Q: How do I know if my business has a counterfeiting problem?

A: Ask the following questions:

- Do we have a well-known or emerging brand?
- Have our brands captured a significant share of the market?
- Do we have a unique product that would be desired at a low price?
- Are we experiencing an unexplained increase in returns or consumer complaints?
- Are the reasons given for increased returns and complaints different than usual?
- Have we lost market share in a particular region or regions?

If you answered "yes" to any of these questions, someone may be counterfeiting your product. If you are not sure, or need to better understand the scope of your potential problem, you should:

- Analyze your returns, complaints, and market share trends for anomalies.
- Interview key members of your sales, marketing, and quality assurance teams to obtain their impressions.
- Perform market surveillance—or "covert buys"—in areas that have suspicious decreases in market share or increases in customer dissatisfaction.
- Survey the Internet for sales of your product at suspiciously low prices and from unauthorized sources.
- Investigate markets that you have not yet entered, because if your brand name has market share where you are not even doing business, it is pretty clear that you have a problem.
- Develop and implement anti-counterfeiting and piracy strategies and build them into daily business practices.

An introduction into the market of a single counterfeit product has the potential to undermine and damage years of building a business' goodwill and reputation.

Adapted from "Intellectual Property Protection and Enforcement Manual" Global Intellectual Property Center (p.3)