People’s Liberation Army on Track to Achieve Modern Regionally-Focused Military By 2020

In its Annual Report to Congress on the Military and Security Developments Involving the PRC for 2011, the Office of the Secretary of Defense begins its Executive Summary as follows:

“China’s rise as a major international actor is likely to stand out as a defining feature of the strategic landscape of the early 21st century. Sustained economic development has raised the standard of living for China’s citizens and elevated China’s international profile. This development, coupled with an expanding science and technology base, has also facilitated a comprehensive and ongoing military modernization program.”

Additionally, China has been assuming new roles in the international community, such as peace keeping, counter-piracy, and disaster relief. In support of such roles, the PLA is now engaged beyond China’s immediate territorial interest. What might this mean for the US, in particular our research and defense industries?

The report finds that “China relies on foreign technology, acquisition of key dual-use components, and focused indigenous research and development (R&D) to advance military modernization.”

China’s military industry is comprised of organizations with both military and civilian functions. “This network of government-affiliated companies and research institutes often enables the PLA to access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development.” The report highlights the PLA’s advances by military branch and technology.

This issue will present a little insight into the PLA, as well as news of US technology theft and hacking.

**True Story: Espionage in the Defense Industry**

During a social gathering held in 1970 at a commercial establishment in New York, one Sergey Viktorovich Petrov (fictitious name), a Russian citizen, happened to strike up a casual conversation with an individual employed as an engineer with the Grumman Aerospace Corporation.

In the course of their conversation, Petrov explained that he was Russian and was employed at the United Nations (UN) where he translated papers relating to various scientific affairs. He added that he lived in New York City with his wife and daughter, and that he was trained in aeronautical engineering. He also related that he had a five-year contract.

The engineer revealed his employment and noted that he was engaged in design planning relating to the F-14 fighter aircraft that was being developed by Grumman for the United States Navy. He explained that his company had been dismissing a large number of engineers, and therefore, his future employment prospects at Grumman were rather bleak. The American illustrated his points by commenting on certain economy measures he had undertaken in his personal spending habits due to his uncertain future.

Before the chance meeting was over, Petrov bought his new-found friend a drink. He told the engineer he would enjoy seeing him again in the near future at which time he could perhaps treat the American to a steak dinner. The engineer accepted Petrov’s invitation one week later. This was the beginning of a recruitment process for Petrov.

During the course of their relationship, Petrov continued to earn the engineer’s trust, and eventually convinced him to supply confidential information about the F-14 fighter aircraft in exchange for money. The American engineer had become a spy for the Russian government.

This story is only one of many examples that show how everyday people are recruited to spy on the United States. Con artists, like Petrov, target an individual who has access to the information they want, study the vulnerabilities of that individual, and exploit their human weaknesses in order to obtain what they’re after. But the con artists of today have a distinct advantage over the recruiters of the past: Social Networking.

**The Online Society**

There are over two hundred well known social networking sites up and running on the internet today\(^1\), and this number continues to grow rapidly as the popularity of internet communication increases. Its intense growth has even motivated businesses and corporations to dip into the social networking pool, using its easy accessibility and widespread use as a way to both advertise their products and draw the attention of potential employees. The internet has become commonplace for social interface and business transactions, creating an online society of inter-web relationships.

(Continued on Page 3)

DOES SOCIAL NETWORKING MAKE YOU A TARGET FOR SPY RECRUITMENT?

(Continued from Page 2)

On both the social and the corporate levels, the benefits of social networking are easy to identify. It allows people of all ages to keep in contact with friends, loved ones, colleagues, and peers on a constant and consistent basis, regardless of distance, time zones, and schedules. It has given internet users the ability to freely and effortlessly connect with people across the globe – to make new friends, to reunite with old friends, and to keep in touch with family. In the business world, social networking enables communication, connection, and the facilitation of advertising and promoting to a worldwide audience with little to no cost.

But what vulnerabilities surface when you actively participate in a network that caters to such an immense number of people? For those who work with U.S. Government and Military clientele, social networking can be used as a tool to target you for spy recruitment.

Social Engineering: Today’s Spy Recruitment

When users create a social networking profile, they are exposing their personal lives to spectators across the globe. These profiles are snapshots of someone’s identity – who they are, what they do, where they live, etc. This information can easily be used as targeting data by today’s spy recruiters: Social Engineers.

Social engineers specialize in exploiting personal connections through social networks. They use social interactions – in person, over the phone, or even in writing – to elicit specific information from unsuspecting individuals without giving them the feeling that they are being interrogated. Social engineers will take what they know about a person and use it to befriend them, gain their trust, and then influence them to deliver materials and information that should not be shared with others.

A social engineer who is eager to obtain sensitive, proprietary, and/or classified information can easily use social networks to find people who have access to that kind of material. A social networking profile can expose personal information that indicates whether or not a person has access to the wanted information. The list below gives examples of profile information that may make you a target of social engineering. (continued on Page 4)

WHAT MAKES YOU A TARGET?

- Employment Information (current and previous): Simply listing the companies you have worked for gives others an idea of the types of tools and information you handle and have handled in the past.
- Job Skills and Specialties: Specifying your knowledge of and experience with a particular subject matter easily makes you a target to foreign government entities who want to steal that information. Even listing an area of study or previous publications (educational and professional) exposes what you know and what you might have access to.
- Security Clearances: Even if you are not specific as to what kind of clearance you have, mentioning a security clearance gives others the impression that you may have access to sensitive, proprietary, and classified information.
- Friends and Colleagues: Exposing friends and colleagues who have access to certain information gives you access by association. Even if you do not directly claim to have access, a social engineer may approach you in order to work their way to a more direct target.
Not only will your social networking profile aid a social engineer in targeting you for recruitment, but it also allows them to learn about your personality and build a character approach that will make you more susceptible to their elicitation techniques. The more they know about you, the easier they can manipulate you into being more vulnerable to their elicitation techniques. The list below gives examples of information that could be exploited to manipulate you into eliciting information.

### WHAT MAKES YOU VULNERABLE?

- **Political and/or Religious Views**: A social engineer might appeal to your ideologies in order to bond with you and form a foundation for a relationship.
- **Financial Information**: Any indications of financial hardship gives a social engineer an avenue through which they can appeal to you. Money is a huge motivator!
- **Relationship Status**: It is not uncommon for recruitment procedures to be carried out through the guise of a romantic relationship. Seduction is often used to establish a relationship and begin the trust-building process. These targets are often people who express the desire to be in a relationship or are having trouble with a current relationship.
- **Hobbies and Likes/Dislikes**: A social engineer will look for ways to make him or herself attractive to you in order to become your friend. An easy way to accomplish this is to act as if you share commonalities – perhaps you enjoy the same activities, like the same types of food, music, etc.
- **Location**: Listing your location, whether permanent or temporary, allows the target to find and access you in order to start his or her recruitment process.

A social networking profile is like a cheat sheet for social engineers in targeting individuals to spy against the United States. As experts of manipulation, social engineers will conform their personalities to fit your lifestyle, basing their techniques on what you have made available to them online. In building a relationship with you, they slowly groom you to give them access to what they want. It is up to the men and women who work with sensitive, proprietary, and classified information to take the proper steps in ensuring its security and preventing successful spy recruitment. A simple way to fight social engineering is by monitoring your own social networking profiles. The next page lists a few measures you can take to help prevent the exploitation of your social networking site.

*Article written by IA Courtney Mikolaycik*
Monitor Your Social Networking Profile!

- Be thoughtful and limit the personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.

- Do not post anything that might embarrass you later or that you don’t want strangers to know.

- Limit your online social network to only include those you know personally. Do not accept requests from strangers.

- Look into the privacy settings that are available for each social networking site and properly employ them in order to monitor accessible information.

- Monitor what others are posting about you on their online discussions.

- Beware of unsolicited contact from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.

- Report any suspicious contact from an unknown entity to your employer.
Welcome to the Cyber Security Bundle!

All of us hear about the need for antivirus protection, but a recent study by a University of Michigan shows a 50% reduction in identity and credit card theft among those who use antivirus, antispyware, and anti-adware protection. Given the dangers of identity theft, there should be no excuse not to run all three forms of protection. http://www.homelandsecuritynewswire.com/dr20120320-triplethreat-computer-protection-reduces-identity-theft

An interesting article from About.com discusses “misuse cases.” Essentially, a misuse case asks “How can I use this access or information to do something I’m not supposed to?” It is a formal process for IT professionals to examine the security of their networks. By asking network administrators to think like hackers, you may expose some vulnerability in your internet connection before it is used to your detriment. The process is worth discussing, whether conducted in-house, or by hiring an outside company to perform a review. The process is explained in some detail here: http://netsecurity.about.com/od/newsandeditoria2/a/Combating-The-Insider-Threat-With-Misuse-Cases.htm

Hand-in-hand with building in system security, a study of passwords by Cambridge University’s Joseph Bonneau made some interesting (and frightening) discoveries. Using the largest dataset to date (70 million entries, with demographic information), he found several trends. For example: Older users tended to have better passwords than younger; passwords for credit cards were only slightly more secure than for online games; and worst, given ten tries and even a generic password library, over 1% of accounts could be hacked.

The article also discusses suggestions for improved passwords. Suggestions include using multi-word passwords or passphrases, which have their own weaknesses, or using mnemonic passwords. Mnemonic passwords are phrases, but instead of using the whole word, just the first letter in each word is used; Mpapbioutwwjtfliewiu is an example of a mnemonic built from the first letter of each word in the first part of this sentence.

Given other recent concerns regarding system and network security, there is little doubt that improving the security mindset behind the keyboard will continue to be one of the best ways to protect your network and information: http://www.economist.com/node/21550763?fsrc=rss|sct.

The 2012 Verizon Data Breach Investigations Report shows that the greatest danger of data compromise was “hacktivists” – hacker-activists rather than criminals motivated by money. This shift was likely due to the hacker group Anonymous’ activities and their high-profile, large-scale attacks. Given the recent arrest of a number of the leadership of that group, it is debatable whether hacktivism will continue to be such a threat in the future. Regardless of motivation, Verizon offers seven tips that will help prevent or reduce data breaches in the full article. The suggestions range from the common sense-like disposing of sensitive data you no longer need-to the technical, like using both an access card and a password for access.

Another noteworthy item: while many companies are worried about smartphones and “bring your own device” policies, 94% of all data compromised in the last year involved servers. As is sometimes the case, it appears that many companies begin working on a security solution to one problem, only to be distracted by the next threat. While understandable, this reinforces reporting we discussed last issue describing decade-old vulnerabilities that remain open to hackers.

One other suggestion from Verizon was “warn your security guards.” It appears there (Continued on Page 8)
has been a rise in hacking attacks that were physically assisted, so they caution security guards to be alert to unscheduled maintenance of network devices, or signs that something may have happened like a broken tamper-proof seal.

In order to address vulnerabilities, an intelligent, comprehensive IT security plan needs to be developed, implemented, and then followed through. It makes rational sense to address an immediate threat, but failing to go back and finish rectifying a previously-discovered vulnerability leaves your systems vulnerable to exploitation by anyone who remembers an old trick. See the full article regarding Verizon’s report here: http://www.networkworld.com/news/2012/032212-thwarting-hactivists-257530.html?source=nww_rss

Regardless of motivation, hacking continues to be a high-profile threat issue for the U.S. Government, based on the headlines of the last month. Between the heavy coverage a simulated cyber-attack on New York City received, the several high-ranking officials issuing warnings, and the discussions of competing cyber-security bills, cyber-security remains a very hot topic.

As reported in a Homeland Security News Wire article on March 12, 2012, the White House staged a mock cyber attack on New York City’s power supply in order to demonstrate to the U.S. Senate the significance a cyber attack can have. According to cyber security specialists, the exercise showed that such an attack could have potentially dire consequences including blackouts for an extended period of time and the resulting deaths of thousands of people.

The financial consequences, to say nothing of the lives lost, would be disastrous. For comparison, when the northeastern United States was without power for just four days in 2003, the economic losses were estimated at $10 billion. For coverage of the simulated attack, see: http://www.homelandsecuritynewswire.com/dr20120311-nyc-cyberattack-simulation-to-spur-senate-cybersecurity-legislation.

The Department of Homeland Security’s Industrial Control Systems Critical Emergency Response Team was formed specifically to address the threat represented by infrastructure attacks. The head of analysis for the control systems team claims that in 12 of 17 of the breaches the ICS has responded to, a lack of even basic network security would have detected or even prevented the attack. She goes on to list the three main types of attackers: “garden-variety” hackers that target known vulnerabilities; the various viruses, worms, and botnets; and “nation-state actors” intent on espionage.

The rise in attacks is particularly alarming: only nine attacks in 2009 became 198 last year, with 40% focused on water systems. There is alarming evidence that in many cases, the hackers were in the control systems, only discovered on their way out of the system (exfiltrating). Again, the dangers of remote access systems are highlighted, as there is also evidence many attacks are coming in via outside companies that provide services. See more from the DHS ICS here: http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?page=1

(Continued on Page 9)
Even the DoD is vulnerable, according to an interview with James Peery, Director of the Information Systems Analysis Center at Sandia National Laboratory. He claims that the military’s networks are already thoroughly compromised, and now we should focus on protecting the information. He wants to assume the enemy is in the network already, so we can focus on remaining in operation and protecting the information. Notably missing in the article is an explanation how an organization can possibly protect information if an adversary is in the machine the data is on. Also lacking are any suggestions for improving things he notes as substandard, which leaves readers with little hope for the military’s network systems. His comments here: http://www.mobiledia.com/news/134769.html.

Trend Micro has uncovered the person believed to be responsible for the Luckycat hacking activity. Symantec and Trend Micro have tracked this activity to China. The Luckycat campaign, operating since June of 2011, has focused on military research, aerospace, and energy industries, as well as Tibetan activists. The person believed responsible was once associated with the Information Security Institute of the Sichaun University in Chengdu, China, and now apparently works for China’s largest Internet portal company, Tencent.

His campaign was thorough, using different codes for each attack so he could track which target was compromised by which malware, organized in waves. He used several varieties of anonymity tools, but was tracked through an email address. More on their analysis here: http://www.networkworld.com/news/2012/033012-trend-micro-uneartshs-more-links-257832.html?source=nww_rss.

Finally, in an attempt at fairness to the rash of recent accusations against China, they have released their own report which shows the U.S. is the source of the majority of attacks against Chinese government and company websites. The National Computer Network Emergency Response Coordination Center of China claims 65% of the domain names used for illegal cyber activity were registered overseas, and that 3,300 IP addresses in the United States had backdoor control of 3,400 Chinese websites. More here: http://english.people.com.cn/90778/7765374.html.

*Cyber Bundle written by IOA Jonathan Sharps*
A March 15, 2012 Bloomberg article, “China Corporate Espionage Boom Knocks Wind Out of U.S. Companies,” highlights the difficulties which a U.S. based company, American Superconductor Corporation (ASC), experienced in its attempt to expand its business into China. Founded in 1987, ASC focused on developing power transmission lines made from superconductive material. After a period of time, ASC shifted its focus to the technology associated with wind-turbine control systems. As the development of ASC’s control systems gained momentum, ASC sensed an opportunity and began investigating the possibility of taking its technology to the vast market of China. This article provides details of ASC’s 2006 entry into the Chinese wind power industry and its attempts to form a partnership with Beijing-based Sinovel, the second-largest turbine maker in the world.

While determined to make this joint partnership work, ASC also went to great lengths to protect the intellectual property associated with its software. ASC designed its China operations in order to safeguard the technology. ASC’s Chinese employees were carefully selected to ensure there would be no internal threats. When ASC opened its China factory, ASC made sure firmware and other technology components were built in factories in the United States and then shipped to China. The software was secured at ASC’s research facility in Europe. The source code to the ASC control system sat on a secure server in Austria – a server not accessible from the Internet. ASC control systems would be shipped to China and paired with Sinovel’s hardware, the wind-turbine.

Sinovel was well connected politically and seemed to provide ASC the perfect entre into the Chinese market. By 2011, Sinovel became ASC’s biggest customer, accounting for more than two-thirds of the company’s $315 million in revenues. However, in March 2011, Sinovel abruptly and inexplicably began turning away the ASC shipments. ASC’s stock plummeted, falling 84 percent within four months.

By June 2011, ASC discovered the true source of its problems. After sending a team of ASC technicians to investigate the cause of a malfunction at ASC’s wind turbine farm in China’s Gobi Desert, ASC was advised that the Sinovel turbine was running on a stolen version of ASC’s software. To make matters worse, the software revealed Sinovel had complete access to ASC’s proprietary source code. The agreement of Sinovel providing the hardware, with ASC providing the electronic gadgetry worth $200,000 for each turbine, was now rendered useless. Sinovel no longer needed ASC.

After a series of internal investigations, ASC discovered that Sinovel had indeed breached ASC’s inner sanctum. According to court documents, Sinovel began recruiting a Serbian software engineer who worked at ASC’s Austria facility in 2010. In 2011, Sinovel had arranged for this engineer to travel to China, where the engineer provided the source code data to Sinovel employees. Sinovel was now in possession of ASC’s crown jewels.

ASC turned its evidence over to Austrian authorities, who took the engineer into custody. The engineer admitted to his illegal activities and ultimately pled guilty to charges of distribution of trade secrets, after investigators found a six-year $1.7 million consulting contract with Sinovel and a related company. This contract with the engineer was signed by Sinovel’s President.

Nonetheless, neither Sinovel nor the Chinese government is giving any ground. After providing the Beijing police with a case file documenting the details, the Beijing police declined to open a criminal investigation against the involved Sinovel employees identified by the engineer. ASC currently has four complaints in Chinese courts against Sinovel, seeking $1.2 billion in damages.

Review written by SA Steve Kaitcer

The entire Bloomberg article can be viewed through the following link:

Bloomberg Article
Ex-Marine Accused of Attempting to Export Sensitive Military Items

Noted Scientist Sentenced for Attempted Espionage, Fraud, and Tax Evasion

Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims

Australian Man Indicted in Plot to Export Restricted Military and Other U.S. Technology to Iran

U.S. and Chinese Defendants Charged in Connection with Conspiracy to Sell Trade Secrets to Chinese Companies

Former CIA Officer John Kiriakou Indicted for Allegedly Disclosing Classified Information, Including Covert Officer’s Identity, to Journalists and Lying to CIA’s Publication’s Board

California Resident and Company Plead Guilty to Conspiracy to Export Computer-Related Equipment to Iran

Former Bridgestone Americas Center Employee Arrested for Theft of Trade Secrets

Ex-Intel Employee Pleads Guilty to Theft Charges

Additional Export Violations in the News

- Hawk Missile Batteries to Iran
- Aircraft Components and Other Materials to Iran
- Military-Grade Thermal Weapon Sight and Rifle Scopes to Eastern Europe
- Components for IEDs to Iran and Iraq
EX-MARINE ACCUSED OF ATTEMPTING TO EXPORT SENSITIVE MILITARY ITEMS

March 05, 2012

LOS ANGELES—A retired Marine Corps staff sergeant, who until recently worked in the Marine Aviation Supply Office at Edwards Air Force Base, was arrested by federal agents this morning following an undercover probe that allegedly revealed he lied to the government as part of a scheme to sell sensitive military equipment to buyers around the globe.

Sean Elias Sayegh, 41, of Rosamond, was taken into custody at his residence by agents with U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI).

Sayegh, who retired from the Marine Corps in December 2011, was named in an indictment returned by a federal grand jury last Friday that charges him with four counts of making false statements. Specifically, the indictment alleges that on four occasions Sayegh made fraudulent claims on U.S. Postal Service customs declaration forms, stating that packages he was shipping contained camera lenses and other camera equipment, when the items were actually laser light interference filters (LIFs). The alleged violations, which occurred between December 2009 and February 2010, involved the shipment of more than 100 LIFs.

LIFs, which are used with military night vision goggles, are on the U.S. Munitions List and cannot legally be exported without a license issued by the Department of State. LIFs protect the optics inside night vision goggles from being damaged by lasers. The technology is considered sufficiently sensitive that the military requires that LIFs be destroyed when they reach the end of their service life.

The Defense Criminal Investigative Service (DCIS) initiated the probe into Sayegh’s activities after receiving a lead about the possible sale of Munitions List items on eBay. DCIS referred the matter to the Naval Criminal Investigative Service (NCIS). HSI joined the investigation, at the request of NCIS, because of the potential export violations. HSI carried out the undercover investigation.

Each false statement charge in the indictment carries a statutory maximum penalty of five years in federal prison. Therefore, if he is convicted of the four counts in the indictment, Sayegh would face a maximum sentence of 20 years in prison, as well as a $1 million fine.

Sayegh is expected to be arraigned on the indictment this afternoon in United States District Court in Los Angeles.

“These items may look innocuous, but their sophistication makes them highly sought after by our adversaries,” said Claude Arnold, special agent in charge for HSI Los Angeles. “They were developed to give America and its allies a strategic military advantage, which is why HSI will continue to work with its law enforcement partners to ensure such technology doesn’t fall into the wrong hands.”

(Continued on Page 12)
Jeffrey Morrow, special agent in charge for NCIS’ Southwest Field Office, stated, “One of the U.S. military’s greatest advantages is its ability to operate effectively at night when our adversaries cannot. In large part, this advantage is reliant on equipment and technologies like former SSGT Sayegh attempted to sell to unauthorized buyers abroad. Actions like this risk the technological advantage that the U.S. military maintains and for this reason this case is significant. NCIS will work aggressively with our law enforcement partners to stop the compromise of these important technologies.”

Chris Hendrickson, special agent in charge, DCIS, Western Field Office, commented, “DCIS will use all tools available—our ability to track worldwide financial dealings, our advanced cyber capabilities, and our worldwide law enforcement alliances—to protect America’s warfighters and the taxpayers’ interests. DCIS and its law enforcement partners are committed to identifying and bringing to justice individuals intent on illegally exporting this country’s critical assets at the expense of America’s security.”

In addition to HSI, NCIS, and DCIS, the U.S. Postal Inspection Service (USPIS) and U.S. Customs and Border Protection (CBP) also played a prominent role in the case.

“This type of offense is unjustifiable,” said B. Bernard Ferguson, inspector in charge for the Los Angeles Division of the Postal Inspection Service. “U.S. Postal Inspectors will continue to aggressively investigate those who violate the laws meant to protect the Postal Service, its employees, and our nation’s citizens.”

In November 2009, the government announced the Export Control Initiative to streamline the complex system of U.S. export controls and enhance the coordination of efforts to address current security threats. As part of those ongoing reforms, HSI recently established the Long Beach-based Counter Proliferation Investigations Center (CPIC). CPICs are located in strategic cities where the threat of illegal exportations is greatest. The goal of these centers is to better facilitate regional enforcement efforts to target the illegal exportation of sensitive weapons and technology. In addition to DCIS, NCIS, USPIS, and CBP, other federal agencies currently participating in the HSI-led initiative include the Department of Commerce’s Office of Export Enforcement; the Air Force Office of Special Investigations; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the FBI; and the National Aeronautics Space Agency (NASA) Office of Inspector General. The center enables the participating agencies to pool their resources, expertise, and intelligence to pursue cases involving export enforcement.
WASHINGTON—Stewart David Nozette, 54, 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, was sentenced today to 13 years in prison for attempted espionage, conspiracy to defraud the United States, and tax evasion.

The sentence covered charges in two cases. In one, Nozette pleaded guilty in September 2011 to attempted espionage for providing classified information to a person he believed to be an Israeli intelligence officer. In the other, he pleaded guilty in January 2009 to fraud and tax charges stemming from more than $265,000 in false claims he submitted to the government.

The sentencing, which took place this morning in the U.S. District Court for the District of Columbia, was announced by Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; Lisa Monaco, Assistant Attorney General for National Security; and Principal Deputy Assistant Attorney General John A. Di Cicco of the Tax Division.

Joining in the announcement were James W. McJunkin, Assistant Director in Charge of the FBI’s Washington Field Office; Paul K. Martin, Inspector General for the National Aeronautics and Space Administration (NASA OIG); Eric Hylton, Acting Special Agent in Charge of the Washington Field Office of the Internal Revenue Service-Criminal Investigation (IRS-CI); and John Wagner, Special Agent in Charge of the Washington, D.C. Office of the Naval Criminal Investigative Service (NCIS).

In addition to the prison term, the Honorable Paul L. Friedman ordered that Nozette pay more than $217,000 in restitution to the government agencies he defrauded.

Nozette has been in custody since his arrest for attempted espionage on October 19, 2009. At the time, he was awaiting sentencing on the fraud and tax evasion charges. FBI agents arrested Nozette following an undercover operation in which he provided classified materials on three occasions, including one that formed the basis for his 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’s greed exceeded his loyalty to our country,” said U.S. Attorney Machen. “He wasted his talent and ruined his reputation by agreeing to sell national secrets to someone he believed was a foreign agent. His time in prison will provide him ample opportunity to reflect on his decision to betray the United States.”

“Stewart Nozette betrayed his country and the trust that was placed in him by attempting to sell some of America’s most closely-guarded secrets for profit. Today, he received the justice he deserves. 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. “I thank the many agents, analysts, and prosecutors who worked on this important case.” (Continued on Page 14)
“As this case demonstrates, those who attempt to evade their taxes by abusing the tax-exempt status of non-profit entities will be investigated, prosecuted, and punished,” said Principal Deputy Assistant Attorney General DiCicco.

“Today’s sentencing demonstrates that espionage remains a serious threat to our national security,” said Assistant Director in Charge McJunkin. “The FBI and our partners in the defense and intelligence communities work every day to prevent sensitive information from getting into the wrong hands, and I commend the hard work of the dedicated agents, analysts, and prosecutors who spent a significant amount of time bringing this case to resolution.”

“We are particularly proud that NASA OIG’s fraud investigation of Nozette, which began in 2006, served as the catalyst for further investigation and today’s outcome,” said NASA Inspector General Martin.

“IRS-Criminal Investigation provides financial investigative expertise in our work with our law enforcement partners,” said Acting Special Agent in Charge Hylton. “Pooling the skills of each agency makes a formidable team as we investigate allegations of wrongdoing. Mr. Nozette decided to betray his country to line his own pockets rather than play by the rules. He now is being held accountable for his actions.”

“Federal agents take an oath to protect our nation ‘against all enemies, foreign and domestic.’ That would include ‘insider threats’ like Stewart Nozette,” said Special Agent in Charge Wagner. “NCIS is committed to working with our law enforcement partners and prosecutors to find and hold accountable those like Nozette who put personal gain above national security.”

Nozette received a Ph.D. in planetary sciences from the Massachusetts Institute of Technology. Beginning in at least 1989, he held sensitive and high-profile positions within the U.S. government. He worked in various capacities on behalf of the government in the development of state-of-the-art programs in defense and space. During his career, for example, Nozette worked at the White House on the National Space Council, Executive Office of the President. He also worked as a physicist for the U.S. Department of Energy’s Lawrence Livermore National Laboratory, where he designed highly advanced technology.

Nozette was 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 (NRL) in Washington, D.C.; the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia; and NASA’s Goddard Space Flight Center in Greenbelt, Maryland.

In connection with the fraud and tax case, Nozette admitted that, from 2000 through 2006, he used ACT to defraud the NRL, DARPA and NASA by making and presenting more than $265,000 in fraudulent reimbursement claims, most of which were paid. He also admitted that, from 2001 through 2005, he willfully evaded more than $200,000 in federal taxes. In addition, he admitted using ACT, an entity exempt from taxation because of its non-profit status, to receive income and to pay personal expenses, such as mortgages, automobile loans, sedan services, and other items. (Continued on Page 15)
The investigation concerning ACT led investigators to suspect that Nozette had misused government information. 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.

On September 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. That same day, Nozette informed the undercover employee that he had clearances “all the way to top secret/SCI” and that anything “that the U.S. has done in space I’ve seen.” He stated that he would provide classified information for money and a foreign passport to a country without extradition to the United States.

A series of contacts followed over the next several weeks, including meetings and exchanges in which Nozette took $10,000 in cash left by the FBI at prearranged drop-off sites. Nozette provided information classified as secret/SCI and top secret/SCI that related to national defense. Some of this information directly concerned satellites, early warning systems, means of defense or retaliation against large-scale attack, communications intelligence information, and major elements of defense strategy.

Nozette and the undercover employee met for the final time on October 19, 2009 at the Mayflower Hotel. During that meeting, Nozette pushed to receive larger payments for the secrets he was disclosing, declaring that, “I gave you even in this first run some of the most classified information that there is...I’ve sort of crossed the Rubicon.”

Nozette was arrested soon after he made these statements.

The investigation of the fraud and tax evasion case was conducted by NASA OIG, NCIS, the Defense Criminal Investigative Service (DCIS), IRS-CI, the IRS Tax Exempt and Government Entities Group, the Naval Audit Service, the Defense Contract Audit Agency, and the FBI’s Washington Field Office.

The prosecution of the fraud and tax evasion case was handled by Assistant U.S. Attorney Michael K. Atkinson from the Fraud and Public Corruption Section of the U.S. Attorney’s Office for the District of Columbia and Trial Attorney Kenneth C. Vert from the Department of Justice’s Tax Division.

The investigation of the attempted espionage case was conducted by the FBI’s Washington Field Office, with assistance from NCIS; Naval Audit Service; National Reconnaissance Office; Air Force Office of Special Investigations; Defense Computer Forensics Laboratory; Defense Advanced Research Projects Agency; DCIS; Defense Contract Audit Agency; U.S. Army 902nd Military Intelligence Group; NASA Office of Counterintelligence; NASA OIG; Department of Energy Office of Intelligence and Counterintelligence; IRS-CI; IRS Tax Exempt and Government Entities group; U.S. Customs and Border Protection; and the U.S. Postal Inspection Service, as well as other partners in the U.S. intelligence community. The prosecution of that case was handled by Assistant U.S. Attorney Anthony Asuncion, from the National Security Section of the U.S. Attorney’s Office for the District of Columbia, and Trial Attorneys Deborah A. Curtis and Heather M. Schmidt, from the Counterespionage Section of the Justice Department’s National Security Division.
Five computer hackers in the United States and abroad were charged today, and a sixth pled guilty, for computer hacking and other crimes. The six hackers identified themselves as aligned with the group Anonymous, which is a loose confederation of computer hackers and others, and/or offshoot groups related to Anonymous, including “Internet Feds,” “LulzSec,” and “AntiSec.”

RYAN ACKROYD, a/k/a “kayla,” a/k/a “lol,” a/k/a “lolspoon”; JAKE DAVIS, a/k/a “topiary,” a/k/a “aptopiary”; DARREN MARTYN, a/k/a “pwnsauce,” a/k/a “raepsauce,” a/k/a “networkkitten”; and DONNCHA O’CEARRBHAIL, a/k/a “palladium,” who identified themselves as members of Anonymous, Internet Feds, and/or LulzSec, were charged in an indictment unsealed today in Manhattan federal court with computer hacking conspiracy involving the hacks of Fox Broadcasting Company, Sony Pictures Entertainment, and the Public Broadcasting Service (“PBS”). O’CEARRBHAIL is also charged in a separate criminal complaint with intentionally disclosing an unlawfully intercepted wire communication.

HECTOR XAVIER MONSEGUR, a/k/a “Sabu,” a/k/a “Xavier DeLeon,” a/k/a “Leon,” who also identified himself as a member of Anonymous, Internet Feds, and LulzSec, pled guilty on August 15, 2011 in U.S. District Court to a 12-count information charging him with computer hacking conspiracies and other crimes. MONSEGUR’S information and guilty plea were unsealed today. The crimes to which MONSEGUR pled guilty include computer hacking conspiracy charges initially filed in the Southern District of New York. He also pled guilty to the following charges: a substantive hacking charge initially filed by the U.S. Attorney’s Office in the Eastern District of California related to the hacks of HBGary, Inc. and HBGary Federal LLC; a substantive hacking charge initially filed by the U.S. Attorney’s Office in the Central District of California related to the hack of Sony Pictures Entertainment and Fox Broadcasting Company; a substantive hacking charge initially filed by the U.S. Attorney’s Office in the Northern District of Georgia related to the hack of Infragard Members Alliance; and a substantive hacking charge initially filed by the U.S. Attorney’s Office in the Eastern District of Virginia related to the hack of PBS, all of which were transferred to the Southern District of New York, pursuant to Rule 20 of the Federal Rules of Criminal Procedure, in coordination with the Computer Crime and Intellectual Property Section (“CCIPS”) in the Justice Department’s Criminal Division.

Late yesterday, JEREMY HAMMOND, a/k/a “Anarchaos,” a/k/a “sup_g,” a/k/a “burn,” a/k/a “yohoho,” a/k/a “POW,” a/k/a “tylerknowsthis,” a/k/a “crediblethreat,” who identified himself as a member of AntiSec, was arrested in Chicago, Illinois and charged in a criminal complaint with crimes relating to the December 2011 hack of Strategic Forecasting, Inc. (“Stratfor”), a global intelligence firm in Austin, Texas, which may have affected approximately 860,000 victims. In publicizing the Stratfor hack, members of AntiSec reaffirmed their connection to Anonymous and other related groups, including LulzSec. For example, AntiSec members published a document with links to the stolen Stratfor data titled, “Anonymous Lulzxmas rooting you proud” on a file sharing website.

(Continued on Page 17)
The following allegations are based on the indictment, the information, the complaints, and statements made at MONSEGUR’s guilty plea:

**Hacks by Anonymous, Internet Feds, and LulzSec**

Since at least 2008, Anonymous has been a loose confederation of computer hackers and others. MONSEGUR and other members of Anonymous took responsibility for a number of cyber attacks between December 2010 and June 2011, including denial of service (“DoS”) attacks against the websites of Visa, MasterCard, and PayPal, as retaliation for the refusal of these companies to process donations to Wikileaks, as well as hacks or DoS attacks on foreign government computer systems.

Between December 2010 and May 2011, members of Internet Feds similarly waged a deliberate campaign of online destruction, intimidation, and criminality. Members of Internet Feds engaged in a series of cyber attacks that included breaking into computer systems, stealing confidential information, publicly disclosing stolen confidential information, hijacking victims’ e-mail and Twitter accounts, and defacing victims’ Internet websites. Specifically, ACKROYD, DAVIS, MARTYN, O’CEARRBHAIL, and MONSEGUR, as members of Internet Feds, conspired to commit computer hacks including: the hack of the website of Fine Gael, a political party in Ireland; the hack of computer systems used by security firms HBGary, Inc. and its affiliate HBGary Federal, LLC, from which Internet Feds stole confidential data pertaining to 80,000 user accounts; and the hack of computer systems used by Fox Broadcasting Company, from which Internet Feds stole confidential data relating to more than 70,000 potential contestants on “X-Factor,” a Fox television show.

In May 2011, following the publicity that they had generated as a result of their hacks, including those of Fine Gael and HBGary, ACKROYD, DAVIS, MARTYN, and MONSEGUR formed and became the principal members of a new hacking group called “Lulz Security” or “LulzSec.” Like Internet Feds, LulzSec undertook a campaign of malicious cyber assaults on the websites and computer systems of various business and governmental entities in the United States and throughout the world. Specifically, ACKROYD, DAVIS, MARTYN, and MONSEGUR, as members of LulzSec, conspired to commit computer hacks including the hacks of computer systems used by the PBS, in retaliation for what LulzSec perceived to be unfavorable news coverage in an episode of the news program “Frontline”; Sony Pictures Entertainment, in which LulzSec stole confidential data concerning approximately 100,000 users of Sony’s website; and Bethesda Softworks, a video game company based in Maryland, in which LulzSec stole confidential information for approximately 200,000 users of Bethesda’s website.

**The Stratfor Hack**

In December 2011, HAMMOND conspired to hack into computer systems used by Stratfor, a private firm that provides governments and others with independent geopolitical analysis. HAMMOND and his co-conspirators, as members of AntiSec, stole confidential information from those computer systems, including Stratfor employees’ e-mails as well as account information for approximately 860,000 Stratfor subscribers or clients. HAMMOND and his co-conspirators stole credit card information for approximately 60,000 credit card users and used some of the stolen data to make unauthorized charges exceeding $700,000. HAMMOND and his co-conspirators also publicly disclosed some of the confidential information they had stolen. (Continued on Page 18)
The Hack of International Law Enforcement

In January 2012, O’CEARRBHAIL hacked into the personal e-mail account of an officer with Ireland’s national police service, the An Garda Siochana (the “Garda”). Because the Garda officer had forwarded work e-mails to a personal account, O’CEARRBHAIL learned information about how to access a conference call that the Garda, the FBI, and other law enforcement agencies were planning to hold on January 17, 2012 regarding international investigations of Anonymous and other hacking groups. O’CEARRBHAIL then accessed and secretly recorded the January 17 international law enforcement conference call, and then disseminated the illegally-obtained recording to others.

MONSEGUR, 28, of New York, New York, pled guilty to three counts of computer hacking conspiracy, five counts of computer hacking, one count of computer hacking in furtherance of fraud, one count of conspiracy to commit access device fraud, one count of conspiracy to commit bank fraud, and one count of aggravated identity theft. He faces a maximum sentence of 124 years and six months in prison.

ACKROYD, 23, of Doncaster, United Kingdom; DAVIS, 29, of Lerwick, Shetland Islands, United Kingdom; and MARTYN, 25, of Galway, Ireland, each are charged with two counts of computer hacking conspiracy. Each conspiracy count carries a maximum sentence of 10 years in prison.

O’CEARRBHAIL, 19, of Birr, Ireland, is charged in the indictment with one count of computer hacking conspiracy, for which he faces 10 years in prison. He is also charged in the complaint with one count of intentionally disclosing an unlawfully intercepted wire communication, for which he faces a maximum sentence of five years in prison.

HAMMOND, 27, of Chicago, Illinois, is charged with one count of computer hacking conspiracy, one count of computer hacking, and one count of conspiracy to commit access device fraud. Each count carries a maximum sentence of 10 years in prison.

DAVIS is separately facing criminal charges in the United Kingdom, which remain pending, and ACKROYD is being interviewed today by the Police Central e-crime Unit in the United Kingdom. O’CEARRBHAIL was arrested today by the Garda.

The case is being prosecuted by the U.S. Attorney’s Office for the Southern District of New York. The investigation was initiated and led by the FBI, and its New York Cyber Crime Task Force, which is a federal, state, and local law enforcement task force combating cybercrime, with assistance from the PCeU; a unit of New Scotland Yard’s Specialist Crime Directorate, SCD6; the Garda; the Criminal Division’s CCIPS; and the U.S. Attorneys’ Offices for the Eastern District of California, the Central District of California, the Northern District of Georgia, and the Eastern District of Virginia; as well as the Criminal Division’s Office of International Affairs.

The charges contained in the indictment and complaints are merely accusations, and the defendants are presumed innocent unless and until proven guilty.
WASHINGTON—An Australian man and his company have been indicted today by a federal grand jury in the District of Columbia for conspiring to export sensitive military and other technology from the United States to Iran, including components with applications in missiles, drones, torpedoes, and helicopters.

The five-count indictment charges David Levick, 50, an Australian national, and his company, ICM Components Inc., located in Thorleigh, Australia, each with one count of conspiracy to defraud the United States and to violate the International Emergency Economic Powers Act (IEEPA) and the Arms Export Control Act; as well as four counts of illegally exporting goods to an embargoed nation in violation of IEEPA; and forfeiture of at least $199,227.41.

The indictment was announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; John J. McKenna, Special Agent in Charge of the Commerce Department’s Office of Export Enforcement Boston Field Office; James W. McJunkin, Assistant Director in Charge of the FBI’s Washington Field Office; Kathryn Feeney, Resident Agent in Charge of the Defense Criminal Investigative Service (DCIS) Resident Agency in New Haven, Connecticut; and Bruce M. Foucart, Special Agent in Charge of U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI) in Boston.

Levick, who is the general manager of ICM Components, remains at large and is believed to be in Australia. If convicted, Levick faces a potential maximum sentence of five years in prison for the conspiracy count and 20 years in prison for each count of violating IEEPA.

According to the indictment, beginning as early as March 2007 and continuing through around March 15, 2009, Levick and ICM solicited purchase orders from a representative of a trading company in Iran for U.S.-origin aircraft parts and other goods. This person in Iran, referenced in the charges as “Iranian A,” also operated and controlled companies in Malaysia that acted as intermediaries for the Iranian trading company.

The indictment alleges that Levick and ICM then placed orders with U.S. companies on behalf of Iranian A for aircraft parts and other goods that Iranian A could not have directly purchased from the United States without U.S. government permission. Among the items the defendants allegedly sought to procure from the United States are the following:

- VG-34 Series Miniature Vertical Gyroscopes. These are aerospace products used to measure precisely and/or maintain control of pitch and roll in applications such as helicopter flight systems, target drones, missiles, torpedoes, and remotely piloted vehicles. They are classified as defense articles by the U.S. government and may not be exported from the United States without a license from the State Department or exported to Iran without a license from the Treasury Department.

(Continued on Page 20)
(Continued from Page 19)

- K2000 Series Servo Actuators designed for use on aircraft. The standard Servo Actuator is designed
to be used for throttle, nose wheel steering, and most flight control surfaces. High-torque Servo Actua-
tors are designed to be used for providing higher torque levels for applications such as flaps and land-
ing gear retraction. These items are classified as defense articles by the U.S. government and may not
be exported from the United States without a license from the State Department or exported to Iran
without a license from the Treasury Department.

- Precision Pressure Transducers. These are sensor devices that have a wide variety of applications in
the avionics industry, among others, and can be used for altitude measurements, laboratory testing,
measuring instrumentations, and recording barometric pressure. These items may not be exported to
Iran without a license from the Treasury Department.

- Emergency Floatation System Kits. These kits contained landing gear, float bags, composite cylinder,
and a complete electrical installation kit. Such float kits were designed for use on Bell 206 helicopters
to assist the helicopter when landing in either water or soft desert terrain. These items may not be ex-
ported to Iran without a license from the Treasury Department.

- Shock Mounted Light Assemblies. These items are packages of lights and mounting equipment de-
dsigned for high vibration use and which can be used on helicopters and other fixed wing aircraft.
These items may not be exported to Iran without a license from the Treasury Department.

According to the charges, Levick and ICM, when necessary, used a broker in Florida to place orders for
these goods with U.S. firms to conceal that they were intended for transshipment to Iran. The defendants
also concealed the final end-use and end-users of the goods from manufacturers, distributors, shippers,
and freight forwarders in the United States and elsewhere, as well as from U.S. Customs and Border Pro-
tection. To further conceal their efforts, the defendants structured payments between each other for the
goods to avoid restrictions on Iranian financial institutions by other countries.

The indictment further alleges that Levick and ICM wired money to companies located in the United
States as payment for these restricted goods. Levick, ICM, and other members of the conspiracy never
obtained the required licenses from the Treasury or State Department for the export of any of these
goods to Iran, according to the charges.

In addition to the conspiracy allegations, the indictment charges the defendants with exporting or at-
ttempting to export four specific shipments of goods from the United States to Iran in violation of IEEPA.
These include a shipment of 10 shock mounted light assemblies on Jan. 27, 2007; a shipment of five
precision pressure transducers on Dec. 20, 2007; a shipment of 10 shock mounted light assemblies on
March 17, 2008; and a shipment of one emergency floatation system kit on June 24, 2008.

This investigation was jointly conducted by agents of the Department of Commerce Office of Export En-
forcement, FBI, DCIS and ICE-HSI. The prosecution is being handled by Assistant U.S. Attorneys John W.
Borchert and Ann Petalas of the U.S. Attorney’s Office for the District of Columbia; and Trial Attorney Jon-
athan C. Poling of the Counterespionage Section of the Justice Department’s National Security Division.

The public is reminded that an indictment contains mere allegations. Defen-
dsants are presumed
innocent unless and until proven guilty in a court of law.
SAN FRANCISCO—A federal grand jury in San Francisco has charged five individuals and five companies with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of companies controlled by the government of the People’s Republic of China (PRC), announced U.S. Attorney Melinda Haag; Lisa Monaco, Assistant Attorney General for National Security at the Department of Justice; and Stephanie Douglas, Special Agent in Charge of the FBI San Francisco Division.

According to the superseding indictment, the government of the PRC identified as a priority the development of chloride-route titanium dioxide (TiO2) production capabilities. TiO2 is a commercially valuable white pigment with numerous uses, including coloring paint, plastics, and paper. To achieve that goal, companies controlled by the PRC government, specifically the Pangang Group companies named in the superseding indictment, and employees of those companies conspired and attempted to illegally obtain TiO2 technology that had been developed over many years of research and development by E.I. du Pont de Nemours & Company (DuPont).

According to the superseding indictment, the Pangang Group companies were aided in their efforts by individuals in the United States who had obtained TiO2 trade secrets and were willing to sell those secrets for significant sums of money. Defendants Walter Liew, Christina Liew, Robert Maegerle and Tze Chao obtained and possessed TiO2 trade secrets belonging to DuPont. Each of these individuals allegedly sold information containing DuPont TiO2 trade secrets to the Pangang Group companies for the purpose of helping those companies develop large-scale chloride route TiO2 production capability in the PRC, including a planned 100,000 ton TiO2 factory at Chongqing, PRC.

According to the superseding indictment, the Liews, USA Performance Technology Inc. (USAPTI), and one of its predecessor companies, Performance Group, entered into contracts worth in excess of $20 million to convey TiO2 trade secret technology to Pangang Group companies. The Liews allegedly received millions of dollars of proceeds from these contracts. The proceeds were wired through the United States, Singapore and ultimately back into several bank accounts in the PRC in the names of relatives of Christina Liew.

The five individuals charged in the indictment are:

Walter Lian-Heen Liew, aka “Liu Yuanxuan,” 54, of Orinda, Calif. Mr. Liew is a naturalized U.S. citizen and co-owner of USAPTI. Mr. Liew is charged with conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, attempted economic espionage, attempted theft of trade secrets, possession of trade secrets, conveying trade secrets, conspiracy to obstruct justice, witness tampering, conspiracy to tamper with evidence, and false statements. Mr. Liew was charged in August 2011 with obstruction of justice and making false statements to the FBI. (Continued on Page 22)
He was arrested at that time and has been ordered detained pending trial based on a finding by Magistrate Judge Nathanael Cousins that he is a flight risk. Mr. Liew’s next scheduled court appearance is before the Honorable Jeffrey S. White on Feb. 9, 2012, at 2:00 p.m.

- Christina Hong Qiao Liew, aka “Qiao Hong,” 49, of Orinda. Mrs. Liew is a naturalized U.S. citizen and co-owner with her husband, Walter Liew, of USAPTI. Mrs. Liew is charged with conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, attempted economic espionage, attempted theft of trade secrets, witness tampering, conspiracy to tamper with evidence, and false statements. Mrs. Liew also was charged in August 2011 with obstruction of justice and making false statements to the FBI. She was released by the court on conditions that include travel restrictions and electronic monitoring. Mrs. Liew’s next scheduled court appearance is before the Honorable Jeffrey S. White on Feb. 9, 2012, at 2:00 p.m.

- Hou Shengdong, 42, a citizen of the PRC. Hou was the vice director of the Chloride Process TiO2 Project Department for the Pangang Group Titanium Industry Company Ltd. According to the superseding indictment, Hou and other Pangang Group employees requested DuPont blueprints as a condition of working on the Pangang Group project. Hou is charged with conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, and attempted economic espionage. A warrant has been issued for Hou’s arrest.

- Robert Maegerle, 76, of Harbeson, Del. Maegerle was employed by DuPont as an engineer from 1956 to 1991. According to the superseding indictment, Maegerle had access to DuPont TiO2 trade secrets, including specific information regarding DuPont’s TiO2 facility at Kwan Yin, Taiwan. Maegerle is charged with conspiracy to commit theft of trade secrets, attempted theft of trade secrets, conveying trade secrets, and conspiracy to obstruct justice. Maegerle was arrested this morning in Harbeson.

- Tze Chao, 77, of Newark, Del. Chao was employed by DuPont from 1966 to 2002. Chao is charged with conspiracy to commit economic espionage. Chao was served with a summons to appear in court in San Francisco on March 1, 2012, at 9:30 a.m. for arraignment on the superseding indictment.

The superseding indictment also names five companies as defendants:

- Pangang Group Company Ltd. Pangang Group is a state-owned enterprise controlled by the State-Owned Assets Supervision and Administration Commission of the PRC State Council and located in Sichuan Province, PRC.

- Pangang Group Steel Vanadium & Titanium Company Ltd. (PGSVTC). PGSVTC is a subsidiary of the Pangang Group.

- Pangang Group Titanium Industry Company Ltd. Pangang Group Titanium is a subsidiary of PGSVTC and was the entity directly responsible for constructing the 100,000 ton chloride-route TiO2 factory at Chongqing, PRC. Pangang Group Titanium entered into an agreement with USAPTI in 2009 under which USAPTI conveyed DuPont TiO2 technology to Pangang Group Titanium and its employees.

- Pangang Group International Economic & Trading Co. (PIETC). PIETC is a subsidiary of PGSVTC and is responsible for financial matters related to the construction of the Chongqing TiO2 factory. PIETC signed a 2009 agreement with USAPTI under which DuPont technology was transferred.

(Continued on Page 23)
USA Performance Technology Inc. (USAPTI). USAPTI is an Oakland, Calif.-based engineering consulting company owned and operated by Walter and Christina Liew. According to the superseding indictment, USAPTI succeeded two other companies owned by the Liews—Performance Group USA and LH Performance—which also were used in the conspiracy to convey DuPont trade secrets to PRC-based companies.

Each of the five corporate defendants named in the superseding indictment are charged with conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets, and attempted economic espionage. Summonses were issued to each corporate defendant requiring them to appear in court in San Francisco on March 1, 2012, at 9:30 a.m. for arraignment on the superseding indictment.

DuPont is a company based in Wilmington, Del., that manufactures a wide variety of products, including TiO2. DuPont invented the chloride-route process for manufacturing TiO2 in the late-1940s and since then has invested heavily in research and development to improve that production process. The global titanium dioxide market has been valued at roughly $12 billion, and DuPont has the largest share of that market.

The chloride-route process is more efficient and cleaner than the sulfate-route process prevalent in the PRC. The superseding indictment alleges that the object of the defendants’ conspiracy was to convey DuPont’s secret chloride-route technology to the PRC companies for the purpose of building modern TiO2 production facilities in the PRC without investing in time-consuming and expensive research and development.

DuPont reported information to the FBI that its TiO2 trade secrets had been misappropriated. The FBI opened an investigation in March 2011.

“As today’s case demonstrates, technology developed by U.S. companies is vulnerable to concerted efforts by competitors—both at home and abroad—to steal that technology,” said U.S. Attorney Haag. “Fighting economic espionage and trade secret theft is one of the top priorities of this Office and we will aggressively pursue anyone, anywhere who attempts to steal valuable information from the United States.”

Assistant Attorney General Monaco said, “The theft of America’s trade secrets for the benefit of China and other nations poses a substantial and continuing threat to our economic and national security, and we are committed to holding accountable anyone who robs American businesses of their hard-earned research. I thank the agents and prosecutors who helped bring about this important case.”

FBI Special Agent in Charge Stephanie Douglas stated, “The conduct alleged in the superseding indictment reveals a methodical effort by foreign interests to misappropriate valuable U.S. technology by using individuals operating within our borders. The goal of this scheme was to obtain the benefit of research and development investments by U.S. companies, without making the same investment of time and money. This is not only unfair, but it does great damage to the U.S. economy and as a result undercuts on national security. The FBI is committed to rooting out commercial espionage that puts U.S. companies at a disadvantage in the global market.” (Continued on Page 24)
The maximum statutory penalty for each of the charges alleged in the superseding indictment is as follows:

- Count One, conspiracy to commit economic espionage: 15 years in prison, $500,000 fine and restitution. The fine for an organizational defendant is not more than the greatest of $10,000,000 or twice the pecuniary gain or loss.
- Count Two, conspiracy to commit theft of trade secrets: 10 years in prison, $250,000 fine or twice the gross gain or loss, and restitution. The fine for an organizational defendant is not more than the greatest of $5,000,000 or twice the pecuniary gain or loss.
- Count Three, attempted economic espionage: 15 years in prison, $500,000 fine and restitution. The fine for an organizational defendant is not more than the greatest of $10,000,000 or twice the pecuniary gain or loss.
- Count Four, attempted economic espionage: 15 years in prison, $500,000 fine and restitution. The fine for an organizational defendant is not more than the greatest of $10,000,000 or twice the pecuniary gain or loss.
- Count Five, attempted theft of trade secrets: 10 years in prison, $250,000 fine or twice the gross gain or loss, and restitution. The fine for an organizational defendant is not more than the greatest of $5,000,000 or twice the pecuniary gain or loss.
- Counts Six and Seven, possession of trade secrets: 10 years in prison, $250,000 fine or twice the gross gain or loss, and restitution. The fine for an organizational defendant is not more than the greatest of $5,000,000 or twice the pecuniary gain or loss.
- Count Eight, conveying trade secrets: 10 years in prison, $250,000 fine or twice the gross gain or loss, and restitution. The fine for an organizational defendant is not more than the greatest of $5,000,000 or twice the pecuniary gain or loss.
- Count Nine, possession of trade secrets: 10 years in prison, $250,000 fine or twice the gross gain or loss, and restitution. The fine for an organizational defendant is not more than the greatest of $5,000,000 or twice the pecuniary gain or loss.
- Count 10, conspiracy to tamper with witnesses and evidence: 20 years in prison, $250,000 fine or twice the gross gain or loss, and restitution.
- Counts 11 and 12, witness tampering: 20 years in prison, $250,000 fine or twice the gross gain or loss, and restitution.
- Count 13, conspiracy to tamper with evidence: 20 years in prison, $250,000 fine or twice the gross gain or loss, and restitution.
- Count 14, false statements in a matter within the jurisdiction of the executive branch: five years in prison, $250,000 fine, and restitution.

The case is being prosecuted by the Special Prosecutions and National Security Unit of the U.S. Attorney’s Office in San Francisco, and the Counterespionage Section of the U.S. Department of Justice. The investigation, which is ongoing, is being conducted by the FBI.

Please note, an indictment contains only allegations and, as in all cases, the defendants must be presumed innocent unless and until proven guilty.
ALEXANDRIA, Va. – Former CIA officer John Kiriakou was indicted today for allegedly repeatedly disclosing classified information to journalists, including the name of a covert CIA officer and information revealing the role of another CIA employee in classified activities, Justice Department officials announced. Kiriakou was charged in a five-count indictment returned by a federal grand jury in the Eastern District of Virginia, after he was initially charged in a criminal complaint and arrested in January 2012.

The indictment charges Kiriakou with one count of violating the Intelligence Identities Protection Act for allegedly illegally disclosing the identity of a covert officer and with three counts of violating the Espionage Act for allegedly illegally disclosing national defense information to individuals not authorized to receive it. The indictment also charges him with one count of making false statements for allegedly lying to the Publications Review Board of the CIA in an unsuccessful attempt to trick the CIA into allowing him to include classified information in a book he was seeking to publish.

Kiriakou, 47, of Arlington, Va., was a CIA intelligence officer between 1990 and 2004, serving at headquarters and in various classified overseas assignments. He remains free on bond and is expected to be arraigned on April 13, 2012, in U.S. District Court in Alexandria, Va.

The charges result from an investigation that was triggered by a classified defense filing in January 2009, which contained classified information the defense had not been given through official government channels, and, in part, by the discovery in the spring of 2009 of photographs of certain government employees and contractors in the materials of high-value detainees at Guantanamo Bay, Cuba. The investigation revealed that, on multiple occasions, one of the journalists to whom Kiriakou is alleged to have illegally disclosed classified information, in turn, disclosed that information to a defense team investigator, and that this information was reflected in the classified defense filing and enabled the defense team to take or obtain surveillance photographs of government personnel. There are no allegations of criminal activity by any members of the defense team for the Guantanamo Bay detainees.

The indictment alleges that Kiriakou made illegal disclosures about two CIA employees and their involvement in classified operations to two journalists on multiple occasions between 2007 and 2009. In one case, by revealing an employee’s name as a CIA officer, Kiriakou allegedly disclosed classified information – as the employee was and remains covert (identified in the indictment as “Covert Officer A”). In the second case, Kiriakou allegedly disclosed the name and contact information of another CIA employee, identified in the indictment as “Officer B,” whose participation in an operation to capture terrorism subject Abu Zubaydah in 2002 was then classified.  

(Continued on Page 26)
Kiriakou’s alleged disclosures occurred prior to a June 2008 front-page story in The New York Times disclosing Officer B’s alleged role in the Abu Zubaydah operation.

The indictment was announced by Patrick J. Fitzgerald, U.S. Attorney for the Northern District of Illinois, who was appointed Special Attorney in 2010 to supervise the investigation. He announced the charges with James W. McJunkin, Assistant Director in Charge of the Washington Field Office of the FBI. Together, they thanked the CIA for its very substantial assistance in the investigation, as well as the Air Force Office of Special Investigations for its significant assistance.

The Justice Department’s National Security Division, working with the FBI, began the investigation. To avoid the risk of encountering a conflict of interest because of the pending prosecutions of some of the high-value detainees, Mr. Fitzgerald was assigned to supervise the investigation conducted by a team of attorneys from the Southern District of New York, the Northern District of Illinois and the Counterespionage Section of the National Security Division who were not involved in pending prosecutions of the detainees.

The count charging violation of the Intelligence Identities Protection Act, as well as each count of violating the Espionage Act, carries a maximum penalty of 10 years in prison, and making false statements carries a maximum prison term of five years. Each count carries a maximum fine of $250,000. If convicted, the court must impose a reasonable sentence under federal sentencing statutes and the advisory U.S. Sentencing Guidelines.

An indictment contains only allegations 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.

The government is being represented in court by Assistant U.S. Attorneys Iris Lan (Southern District of New York) and Mark E. Schneider (Northern District of Illinois), and Trial Attorney Ryan Fayhee, of the Counterespionage Section of the Justice Department’s National Security Division. Assistant U.S. Attorney Lisa Owings (Eastern District of Virginia) will assist in the matter under local court rules.
WASHINGTON – Massoud Habibion, 49, aka “Matt Habibion” and “Matt Habi,” a U.S. citizen and co-owner of a Costa Mesa, Calif., company, Online Micro LLC, pleaded guilty today in the District of Columbia to conspiracy to illegally export computers from the United States to Iran through the United Arab Emirates (UAE). Additionally, Mohsen Motamedian, 44, aka “Max Motamedian” and “Max Ehsan,” a U.S. citizen and co-owner of Online Micro, pleaded guilty to obstruction of justice.

The guilty pleas were announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; John Morton, Director of U.S. Immigration and Customs Enforcement (ICE); David W. Mills, Assistant Secretary for Export Enforcement, Department of Commerce; and Adam Szubin, Director of the Office of Foreign Assets Control (OFAC), Department of the Treasury.

At a hearing today before U.S. District Judge Ellen S. Huvelle, Habibion and Online Micro each pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act and to defraud the United States. Motamedian pleaded guilty to obstruction of justice. Judge Huvelle set sentencing for May 16, 2012. The maximum sentence for Habibion and the company is five years in prison and $1 million. The maximum sentence for Motamedian is 20 years in prison.

Under the terms of the plea and related civil settlements with the Department of Commerce’s Bureau of Industry and Security (BIS) and OFAC, Habibion and his company have agreed to forfeiture of a money judgment in the amount of $1.9 million. In addition, Habibion and Online Micro are denied export privileges for 10 years, although the denial order will be suspended provided that neither Habibion nor Online Micro commit any export violations during the 10-year probationary period and comply with the terms of the criminal plea agreements and sentences. Motamedian separately agreed to a $50,000 monetary penalty to settle a civil charge that he solicited a false statement to federal law enforcement agents.

Habibion and Motamedian were arrested on a criminal complaint in California on April 7, 2011. The defendants and their company were later indicted on April 21, 2011.

Habibion and Online Micro today admitted that they willfully conspired with a company operating in Dubai, UAE, and Tehran, Iran, to procure U.S.-origin computers from the United States and export those computers from the United States to Iran through Dubai without first obtaining licenses or authorizations from OFAC.

In or around May 2007, Online Micro purchased 1,000 computer units from Dell Inc. for approximately $500,000. Later that year, Dell began receiving service calls concerning Dell computer units from individuals in Iran, and after conducting an internal investigation, suspended Online Micro from placing further orders with Dell.

(Continued on Page 28)
Beginning around Nov. 9, 2009, and continuing through December 2010, Habibion and Online Micro conspired with Company X, a firm operating in Dubai and Tehran, to procure U.S.-origin computer-related goods and export those goods to Iran via the UAE. During the scope of the conspiracy, defendants Online Micro and Habibion sold and exported from the United States to Company X numerous shipments of computer-related goods, worth a total of more than $4,904,962, with knowledge that the majority of those goods were destined for Iran.

Online Micro also caused Shipper’s Export Declarations to be filed with U.S. Customs and Border Protection falsely identifying the ultimate destination of the goods as the UAE. During the course of the investigation, Habibion and Motamedian told a government cooperator (Individual A) to lie to U.S. law enforcement officials about the transactions.

Specifically, the defendants told Individual A to lie about Iran being the true ultimate destination for the goods and counseled him to tell U.S. law enforcement agents that the computer-related goods remained in Dubai.

Motamedian and Habibion also acknowledged to Individual A that the sanctions “are serious” and “were not a joke.” Yet Motamedian told Individual A to “Say, ‘I sold over there’ and have your guys make up invoices;” and “[d]efinitely delete your communication with [Company X’s agent in Iran] on Yahoo.” Similarly, Habibion stated to Individual A that he should tell U.S. law enforcement agents that the computer-related goods remained in Dubai: “Well, you can say, ‘I kept the goods there.’ How does he know what happened?”

This investigation was conducted by the ICE’s Homeland Security Investigations (HSI) field offices in San Diego and Orange County, Calif. U.S. Customs and Border Protection and the U.S. Department of Commerce’s BIS Los Angeles Field Office also assisted in the investigation.

Senior Attorney Adrienne Frazier from the U.S. Department of Commerce’s BIS, and Assistant Director of Enforcement Michael Geffroy and Enforcement Officer Elizabeth Beam from OFAC handled the civil settlements for their agencies, respectively.

The prosecution is being handled by Assistant U.S. Attorneys T. Patrick Martin and Anthony Asuncion from the U.S. Attorney's Office for the District of Columbia, and Trial Attorney Jonathan C. Poling from the Counterespionage Section of the Justice Department’s National Security Division.
FORMER BRIDGESTONE AMERICAS CENTER EMPLOYEE ARRESTED FOR THEFT OF TRADE SECRETS

March 22, 2012

CLEVELAND, OH — The FBI arrested Dr. Xiaorong Wang for the theft of Trade Secrets on March 22, 2012. Wang is accused of stealing proprietary information from his former employer, Bridgestone Americas Center for Research and Technology in Akron, Ohio after being terminated from his position on April 14, 2010.

To read the entire article from Action 19 News, Cleveland, Ohio, please click on the following link:

Former Bridgestone Americas Center Employee Arrested for Theft of Trade Secrets

EX-INTEL EMPLOYEE PLEADS GUILTY TO THEFT CHARGES

April 7, 2012

SAN FRANCISCO, CA — Former Intel Corp employee Biswamohan Pani pleaded guilty to five counts of wire fraud on April 6, 2012. Pani downloaded company secrets in 2008 estimated to be worth at least $200 million to $400 million.

To read the entire article from Huffington Post, please click on the following link:

Biswamohan Pani, Ex-Intel Employee Pleads Guilty to Theft Charges
Hawk Missile Batteries to Iran

On Feb. 24, 2012, British businessman Christopher Tappin, of Orpington, Kent, was extradited from the United Kingdom to the Western District of Texas (El Paso, Texas) to face charges in connection with an alleged scheme to illegally export to Iran specialized zinc/silver oxide reserve batteries used in the Hawk Air Defense Missile. On Feb. 7, 2007, Tappin was charged in a federal indictment with one count each of conspiracy to illegally export defense articles; aiding and abetting the illegal export of defense articles, and conspiracy to conduct illegal financial transaction. Tappin allegedly wire transferred $25,000 from a London account to undercover ICE agents as payment for the batteries and also allegedly arranged for the transfer of the batteries to the U.K. without a license through his specifically designated freight forwarders. Two conspirators charged along with Tappin for their roles in the scheme have already been convicted and sentenced. On Nov. 9, 2007, Robert Caldwell was sentenced in the Western District of Texas to 20 months in prison and two years supervised release for his role in the scheme. Robert Gibson was sentenced on Aug. 24, 2007 to a two-year prison term for his role in the scheme. The case was investigated by ICE.

Aircraft Components and Other Materials to Iran

On Feb. 6, 2012, Ulrich Davis, a former manager of a Netherlands-based freight forwarding company, pleaded guilty in the District of New Jersey to an information charging him with conspiracy to defraud the United States by facilitating the illegal export of goods to Iran. Davis was first arrested on Aug. 6, 2011, on charges of conspiring to illegally export goods to Iran in violation of the International Emergency Economic Powers Act. In October 2007, the Commerce Department issued a Temporary Denial Order (TDO) denying export privileges to the company of a co-conspirator of Davis. The TDO prohibited any person, including Davis, from directly or indirectly exporting or re-exporting to or on behalf of the coconspirator. The coconspirator, located in another country, purchased U.S. origin goods from a New Jersey firm for businesses and governmental agencies of Iran. The New Jersey firm was in the business of reselling chemicals, lubricants, sealants and other products used in the aircraft industry. As part of the conspiracy, Davis and his coconspirator directed a New York freight forwarding company to arrange for a trucking company to pick up commodities from the New Jersey company and transport them to New York on behalf of the coconspirator’s company. Davis admitted that in November 2007, he completed an air waybill that represented certain acrylic adhesives and spray paint coatings obtained from a New Jersey company were to be forwarded on behalf of the co-conspirator’s company to Iran after issuance of the TDO. Davis acknowledged that at no time was any relief, exception, or other authorization sought from the TDO. The investigation was conducted by BIS, ICE, and DCIS.
Components for IEDs to Iran and Iraq

On Feb. 10, 2012, a Singapore court ruled that four individuals held in Singapore may be extradited to the United States to face prosecution for their alleged roles in conspiracies to defraud the United States. One of these conspiracies allegedly caused 6,000 radio frequency modules to be illegally exported from the United States to Iran via Singapore, at least 16 of which were later found in Improvised Explosive Devices (IEDs) in Iraq. On Oct. 25, 2011, prosecutors in the District of Columbia unsealed a Sept. 15, 2010 indictment which charged these four individuals, another individual in Iran, and four companies with various violations, including conspiracy to defraud the United States, smuggling, illegal export of goods to Iran, illegal export of defense articles, false statements and obstruction of justice. The charged defendants are Iranian national Hossein Larijani, and his companies Paya Electronics Complex, based in Iran, and Opto Electronics Pte, Ltd., based in Singapore. Also charged was Wong Yuh Lan, an agent of Opto Electronics who was allegedly supervised by Larijani from Iran. The indictment also charges NEL Electronics Pte. Ltd., a company in Singapore, along with NEL’s owner and director, Lim Yong Nam. Finally, the indictment charges Corezing International Pte. Ltd., a company in Singapore that maintained offices in China, as well as Lim Kow Seng, an agent of Corezing, and Hia Soo Gan Benson, a manager, director and agent of Corezing. On Oct. 24, 2011, authorities in Singapore arrested Wong, Nam, Seng and Hia pursuant to a U.S. extradition request. Larijani remains a fugitive in Iran. The indictment alleges that, between June 2007 and February 2008, the defendants fraudulently purchased and caused 6,000 modules to be illegally exported from the Minnesota company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. The defendants allegedly told the Minnesota firm and the U.S. government that a telecommunications project in Singapore was the final destination of the goods. The alleged recipient of all 6,000 modules in Iran was Larijani. The indictment alleges that, in May 2008, December 2008, April 2009, and July 2010, Coalition forces found no less than 16 of these 6,000 modules in Iraq where they were being used as part of the remote detonation devices of unexploded IEDs. The indictment further charges Seng, Hia, and Corezing with a separate fraud conspiracy involving the illegal export of two types of military antenna from the United States. The indictment alleges that these defendants conspired to defraud the United States by causing a total of 55 cavitybacked spiral antennas and biconical antennas to be illegally exported from a Massachusetts company to Singapore and Hong Kong without the required State Department license. Larijani was also charged with false statements in connection with his alleged business dealings with Majid Kakavand, an accused Iranian procurement agent who has been indicted in the United States for illegally exporting goods to Iran, including to military entities in Iran involved in that nation’s nuclear and ballistic missile programs. In coordination with the criminal actions, the Commerce Department announced the addition of 15 persons located in China, Hong Kong, Iran and Singapore to the Commerce Department's Entity List in connection with this procurement network. This investigation was conducted by ICE, FBI, and Department of Commerce’s BIS.
Telemarketing Fraud

While there are many legitimate companies that use the telephone for marketing, consumers and business lose millions of dollars to telemarketing fraud each year. It's sometimes hard to tell the difference between reputable telemarketers and criminals who use the phone to rob people. You can protect yourself by learning how to recognize the danger signs of fraud. If you are a victim or attempted victim of telemarketing fraud, it's important to report the scam quickly so that law enforcement agencies can shut the fraudulent operation down.

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

Here are some warning signs of telemarketing fraud—what a caller may tell you:

- "You must act 'now' or the offer won't be good."
- "You've won a ‘free’ gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.
- "You don't need any written information about their company or their references."
- "You can't afford to miss this 'high-profit, no-risk' offer."

If you hear these or similar "lines" from a telephone salesperson, just say "no thank you" and hang up the telephone.
Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.

Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.

Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.

Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.

Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"

Don't pay in advance for services. Pay services only after they are delivered.

Be wary of companies that want to send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.

Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.

Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.

Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.

Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.

Never respond to an offer you don't understand thoroughly.

Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

Be aware that your personal information is often brokered to telemarketers through third parties.

If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.

If you have information about a fraud, report it to state, local, or federal law enforcement agencies.
Common Telephone Scams

- Buying Club Memberships
- Charities & Fundraising Fraud
- Credit & Loan Offers
- Government Grant Scams
- Medical Discount Plans
- Reloading Scams
- Robocalls
- Sweepstakes & Lotteries
- Travel Scams
- Work-at-Home & Business Opportunities
The National Do Not Call Registry gives you an opportunity to limit the telemarketing calls you receive. Once you register your phone number, telemarketers subject to the FTC's Telemarketing Sales Rule must stop calling you.

Most legitimate telemarketers respect the Registry and won't call a number on it. But scammers are willing to violate the Registry restrictions. If your number is on the Registry, be suspicious of any telemarketing calls, unless they are from companies with which you already do business or that are allowed to call under an exception to the rule.

HOW TO REGISTER YOUR NUMBER

Two easy ways:

- Visit DoNotCall.gov Enter your phone number and email address. Click Submit. Confirm your information and click Register. Open your email message from Register@donotcall.gov. Click on the link to complete your registration.

- Call 1-888-382-1222 from the number you wish to register.

EXCEPTIONS TO THE Telemarketing SALES RULE

Placing your number on the National Do Not Call Registry will stop most telemarketing calls, but not all. Once your number has been on the registry for 31 days, you still may get:

- Calls from - or on behalf of - political organizations, charities, polls, and surveys
- Calls from companies with whom you have an existing business relationship (18 months after you make a purchase or three months after you submit an inquiry or application)
- Calls from companies you've given permission to call
- Business-to-business calls

WHAT ABOUT CELL PHONES?

The National Do Not Call Registry accepts personal cell phones and home numbers. There is no deadline to place a cell or home number on the Registry. Federal Communications Commission (FCC) regulations prohibit telemarketers from using automated dialers to call cell phone numbers, so most telemarketers don't cold-call consumers on their cell phones.

YOUR REGISTRATION DOES NOT EXPIRE!

The Federal Trade Commission will not drop any telephone numbers from the National Do Not Call Registry unless they have been disconnected and reassigned to other customers.

NOT SURE IF YOU'RE ALREADY REGISTERED?

Visit DoNotCall.gov or call 1-888-382-1222 to verify.

*Additional information regarding Telemarketing Fraud may be found at www.fbi.gov and at www.ftc.gov*
The second largest intelligence organization in the PRC involved in HUMINT collection is the Military Intelligence Department (MID) of the PLA’s General Staff Department (GSD); it is most commonly referred to as the Second Department or 2PLA.

In his book *Chinese Intelligence Operations*, Nicholas Eftimiades finds that 2PLA collection activities support three types of military intelligence requirements: tactical, strategic, and technological. The responsibilities of the 2PLA can be divided into categories, as listed: order of battle; military geography; military doctrine; intentions; military economics; biographical intelligence; nuclear targeting; military intelligence watch centers. Eftimiades points out that at the time of publication, 2PLA efforts were primarily tactical. However, he opined that the focus would likely move toward politico-military and military-economic as the PRC worked at securing a more prominent role in regional affairs.

It should be noted that the 2PLA is also active in the field of high technology, especially where there are military applications. Thus, Eftimiades also opines that “the Second Department likely has some measure of authority in the planning and conduct of intelligence operations designed to acquire foreign military technology.”

The 2PLA conducts the following four types of strategic intelligence operations: collecting information on foreign military forces, acquiring technology with military applications, identifying foreign markets for Chinese arms exports, and conducting covert action campaigns. Military attachés serve as “open collectors” the world over. However, there have been cases of their involvement in covert collection operations as well. Eftimiades cites several FBI investigations which exposed 2PLA intelligence officers working under diplomatic cover.

The 2PLA also identifies foreign markets for PRC arms sales and recruits dealers. At the time of publication, Eftimiades identified several PRC customers, including India, Iran, Iraq, North Korea, Pakistan, Saudi Arabia, and Syria, among others. In several cases, he found that the technology had been used to develop nuclear capabilities.

Additionally, the 2PLA has a long history of trying to exert influence in foreign countries through covert action. Eftimiades found that the PLA had been most active throughout Southeast Asia and Africa, and more recently, the Middle East and South East.

The 2PLA is divided into seven bureaus, which include two collection bureaus, four analysis bureaus, and one science and technology research bureau.

The First Bureau focuses its collection efforts on Hong Kong and Taiwan, but collects worldwide. The First Bureau’s collection requirements are divided among five geographic divisions. For example, Nanjing collects against the US and Beijing is responsible for targeting visiting foreigners. These divisions also conduct clandestine intelligence operations overseas.

The Fifth Bureau, or the America/Western Nations Analysis Bureau, makes use of open-source publications in its political and economic analysis. Among its favorite sources are congressional reports and papers produced by American research institutes and think tanks.
KANG was born in 1898 as Zhao Jung, the son of a wealthy landlord; however, he left his family as a teen and adopted the name Kang Sheng as a protest against his father’s exploitation of peasants. As a university student in the early 1920s, he was among the early members of the Chinese Communist Party (CCP). His skills in espionage brought him to the attention of leadership. He had organized an informal operation to discover police spies and dissidents within the CCP.

TAI was born in 1895 to a poor peasant family. At the age of 14, he joined a warlord army and later joined up with Nationalist leader Chiang Kai-Shek.

In 1927, KANG and TAI clashed during the communist uprisings in Shanghai, and the two became hated rivals.

In 1931, Chiang Kai-Shek named TAI head of the Bureau of Information and Statistics, the Nationalist Party’s intelligence agency. Reportedly, TAI recruited over 300,000 agents across China, creating a network directed against the communists. Meanwhile, KANG had been named head of the Department of Special Tasks, the CCP intelligence service. KANG organized his own network of agents to infiltrate TAI’s service.

In 1938, KANG was sent to the Soviet Union at Stalin’s invitation to receive KGB training. During his time there, KANG came to the opinion that the Soviet Union was not a true supporter of Chinese communism, as the KGB was actively recruiting within the CCP and targeting Chairman MAO Zedong. KANG’s concerns were shared with MAO, marking the beginning of what would become the Sino-Soviet split.

KANG returned to China to assist in the effort against Japanese invasion. KANG and TAI did not join forces against their common enemy; instead, they spent most of their efforts trying to neutralize each others’ services.

TAI sought an alliance with the Americans through a successful international campaign which portrayed the Nationalist Party as the true representative of the Chinese people and recruited Chinese-Americans, forming the influential “China Lobby.”

During World War II, both KANG and TAI worked at infiltrating the network of agents established by the American OSS. KANG learned that the US was working on an atomic bomb and immediately began an operation to recruit Chinese-American scientists, especially those involved in nuclear physics. He successfully brought two back to work on the Chinese atomic bomb.

TAI died in 1946 in a mysterious plane crash, believed to be orchestrated by KANG.

In 1949, the communist forces succeeded in taking the Chinese mainland and the People’s Republic of China was founded. KANG became the intelligence master of China. He was responsible for organizing ideological purges and “reeducation centers” across China. Later, he organized the Cultural Revolution. He died in 1975 of cancer. In 1980, the new leadership posthumously expelled KANG from the CCP, calling him “an enemy of the Chinese people.”

Meihong Xu was inducted into the People’s Liberation Army in the summer of 1981, when she was seventeen. She was selected as one of an elite group of twelve young women selected to study at the most prestigious military intelligence school in China, the PLA Institute for International Relations, located in Nanjing. This is the school which trains officers for the Second Bureau, the intelligence unit of the Army. Xu states, “There was a greater need for military intelligence officers proficient in English who could work with our new American counterparts and friends.” Further noting, “...specially trained young women might have the capability of making contacts and gathering intelligence from Americans when male operatives could not.”

This group of ladies became known as “the Twelve Pandas”, indicating that they were PLA “treasures.” They received four years of training in military science, guerrilla and conventional warfare, survival techniques, weapons utilization, Communist Party doctrine, politics, intelligence and counterintelligence operations, formal and colloquial English, technical translation, and Western history and culture.

Following graduation, some would be assigned to the office of the defense attaché in foreign embassies, thus serve openly and in uniform. The elite would serve covertly. “They might work for travel agencies, airlines or newspapers or become students or visiting scholars, entrepreneurs or business representatives.” Some would be called back within a few years, “... having made contacts, established information networks and opened avenues of information and identified and cultivated ‘friends’ of China ... One or two of this elite group, however, would be required to keep new identities all their lives, establishing contacts, marrying, taking foreign citizenship and starting families that would be useful in the next generation or even the one after that.”

In the summer of 1988, Xu was selected to study at the Center for Chinese and American Studies, an educational joint venture between Nanjing University and Johns Hopkins University. It was there that Xu made her first foreign contact, a contact which changed her life ...

Xu’s memoir not only recounts her PLA training, but also offers insight into the affect of communist doctrine on a young mind. Additionally, her story includes some interesting use of tradecraft.

I found Xu’s book personally intriguing, as I studied Chinese at Nanjing University in the spring of 1989 ... Could our paths have ever crossed? However, as a trained counterintelligence agent, her account raises several red flags with me ... those I leave to the readers to discover for themselves.

Review written by SA Michaela Ludwick
WHO’S WHO?

1. What do these men have in common: Christopher Marlowe, Daniel Defoe, Edgar Allan Poe, W. Somerset Maugham, Ian Fleming, and Graham Greene?

TRADECRAFT

2. In 1956, soldiers raided an underground tunnel in East Berlin that was used by American and British agents to tap into East German phone lines to Moscow. In fact, the Soviets had known about the tunnel since it began operations in 1954. Why didn’t they move earlier to shut it down?

CODES

3. How big is a microdot, and how much information can it contain?

Through the Strategic Partnership Program, the FBI offers counterintelligence-related training and presentations.

As part of the Strategic Partnership Program, the Los Angeles FBI is able to:

- Provide a counterintelligence vulnerability assessment
- Provide awareness training to employees, lawyers, and managers
- Provide brochures and literature about threats
- Provide presentations designed to promote a better understanding of espionage vulnerabilities and concerns
- Serve as a resource for questions and concerns (such as matters involving export controls)
- Provide specific threat information, if available
- Provide invitations to regional counterintelligence meetings with the other businesses, academics, and US intelligence community personnel

Our goal is to foster communication and build awareness through our partnerships. Through these cooperative efforts, we are identifying the research and programs targeted by our adversaries. An ongoing dialogue and information exchange between us is critical to protecting our country’s sensitive information and technologies, which, if compromised, have a dramatic effect on our national security.

The Los Angeles Division appreciates the assistance extended to us through the Strategic Partnership Program. Representatives from our Strategic Partnership Program are available to visit your business or organization to provide presentations for your selected audience. Contact may be made with our Strategic Partnership Program Coordinators:

Steve Kaitcer  
Special Agent  
Main: 310-477-6565  
Blackberry: 405-919-2807  
Steven.Kaitcer@ic.fbi.gov

Michaela Ludwick  
Special Agent  
Main: 310-477-6565  
Blackberry: 310-345-4493  
Michaela.Ludwick@ic.fbi.gov

Lance Woo  
Subject Matter Expert  
Retired FBI Special Agent  
Main: 310-477-6565  
Lansing.Woo@ic.fbi.gov
The Greater Los Angeles Industrial Security Awareness Council (ISAC) invites you to attend a half day Security Seminar

Wednesday, May 2, 2012
7:00 – 11:00
Boeing Facility
5301 Bolsa Avenue, Huntington Beach, CA 92647

AGENDA
7:00 - 8:00  Registration and Continental Breakfast

8:00 – 8:10  Welcome and Administrative Remarks
Michael Heller, Facility Security Officer, Boeing
Harriet Aldava, ISAC Seminar Committee Chair

8:10 – 9:00  Counterintelligence Briefing
Rene B. Lopez
Defector/Former Cuban Intelligence Officer

9:00 – 9:10  Break

9:10 – 10:00  ODAA Update
Joseph Webb, ISSP
Timothy Weaver, Western Region ODAA

10:00 – 10:50  DSS and New Rating Matrix Update
Ehren Thompson, DSS
Pasadena Field Office

10:50 – 11:00  Closing Remarks and Raffle
Registration Form

Greater Los Angeles Industrial Security Awareness Council (ISAC)
Half-Day Training Seminar
Boeing Company
5301 Bolsa Avenue
Building 28
Huntington Beach, CA 92647
Wednesday, May 2, 2012

NAME: 
TITLE: 

FACILITY NAME: 

ADDRESS: 

CITY: STATE: 

ZIP: EMAIL ADDRESS: 

TELEPHONE: ( ) FAXIMILE (Optional): ( ) 

The seminar registration fee is $30.00 payable to Greater Los Angeles ISAC. Mail-in registration ends Friday, April 27, 2012. No refunds will be given after this date. Payment will also be accepted at the door. Receipts will be provided to attendees at the seminar. Registration and payment should be mailed to:

Harriet Aldava
RAND Corporation
1776 Main Street
Santa Monica, CA 90407-2138

Tax Exempt Status - Greater Los Angeles, ISAC, Inc. is incorporated as a tax-exempt non-profit organization in the State of California. IRS ID No. 33-0372620.

For questions contact Harriet Aldava 310-393-0411, x6870, email aldava@rand.org.
Directions to
The Boeing Company
5301 Bolsa Avenue
Building 28
Huntington Beach, CA

Driving Directions

Driving South: Driving south from L.A. / Long Beach on the I-405, exit Springdale, turn right and head south to Bolsa Ave. Turn right on Bolsa Ave, proceed to Building 28, which is on Bolsa Ave on the right. It is on the southern portion of the HB campus.

Driving North: Driving north from the San Diego, Newport Beach, on the I-405, exit Goldenwest / Bolsa Ave, and proceed west on Bolsa Ave until reaching the HB campus. Proceed to Building 28, which is on Bolsa Ave on the right. It is on the southern portion of the HB campus.
The Society of Industrial Security Professionals (known as NCMS, Inc) was founded by a group of government and industry security classification managers in 1964 as a way to advance the practice of classification management as a profession. As the society has grown over the years, so has its scope and focus. NCMS now provides professional development for its members in the fields of classification management, information security, personnel security, computer security, operations security (OPSEC), facility security and technology security.

While NCMS has a national board and a national presence, much of the work to advance the society’s goals and objectives happens at the local chapter level. Each chapter features a number of elected officials and members who come together several times a year to network and to share information of value to the community.

Toward that end, the Southern California NCMS Chapter will hold its annual half-day seminar on Friday, April 27 at the Aerospace Corporation in El Segundo. This will be a half-day seminar that will begin with registration at 7:00am and will finish at 11:50am. This will be a very informative event! Formal topics of discussion will include workplace violence, cyber security, and the new Defense Security Service Ratings matrix. Attendees will receive three continuing education units toward their Industrial Security Professional recertification.

The cost is $25 for NCMS members, $30 for non-members, and $30 at the door. Agenda and maps can be found at NCMS’ Southern California website. Please contact Precious Haines (precious.haines@ngc.com, 310-813-2936) to register.
Territory / Jurisdiction

The Los Angeles Division of the FBI covers the Central District of California, which consists of seven counties across 40,000 square miles: Los Angeles, Orange, Riverside, San Bernardino, San Luis Obispo, Santa Barbara, and Ventura.

Resident Agencies
Along with our main office in Los Angeles, we have 10 satellite offices known as resident agencies in the area. See the map below:

Hours
Although we operate 24 hours a day, seven days a week, our normal business hours are from 8:15 a.m. to 5:00 p.m., Monday through Friday. If you are calling a satellite office after normal business hours, and it is an emergency, please contact our Los Angeles office at (310) 477-6565.

FBI LOS ANGELES
11000 Wilshire Boulevard
Suite 1700
Los Angeles, CA 90024
Phone: (310)477-6565
Fax: (310)996-3359
Meet the Staff

SA Steve Kaitcer has 20 years investigative experience as a Special Agent with the FBI. During his FBI career, Steve has worked Public Corruption, Securities Fraud, Civil Rights violations, Financial Institution Fraud, and Espionage matters. Steve recently transferred to the Los Angeles office after almost 19 years in the FBI’s Oklahoma City office.

SA Michaela Ludwick is a Counterintelligence agent with 11 years investigative experience. She has a BA in International Studies/East Asia and a Graduate Certificate in Advanced International Affairs. Michaela spent many years in Asia and speaks Mandarin Chinese. Her interests include history and the arts.

SME Lansing S. Woo retired after 30 years of FBI service working Foreign Counterintelligence. Upon retirement he became the FBI Los Angeles Counterintelligence Program Branch Chief. For the past 5 years, he has served as a contract consultant to the FBIHQ Espionage Section.

IA Courtney Mikolaycik has worked with the Los Angeles FBI since 2010. She is an intelligence analyst for the Field Intelligence Group specializing in the Counterintelligence Program. Courtney is a graduate of Loyola University Chicago, where she earned her BA in Psychology and Criminology.

IOA Jonathan Sharps is an Investigative Operations Analyst who has gained a variety of intelligence experience from serving in the United States Marine Corps as well as interning at Department of State’s INR section. He has a BA in Political Science, and has traveled to a number of countries throughout the world.
In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only. Use does not reflect official endorsement by the FBI. Reproduction for private use or gain is subject to original copyright restrictions. Individuals interested in subscribing to this publication, or interested in further information, should send an email to SA Steve Kaitcer at Steven.Kaitcer@ic.fbi.gov or SA Michaela Ludwick at Michaela.Ludwick@ic.fbi.gov. For additional information, please call SA Steve Kaitcer at 310-996-5104 or SA Michaela Ludwick at 310-996-5103.