FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

November 1, 2011
Volume 3 Issue 11

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

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

GHOST STORIES

On Halloween day the FBI published a treasure trove of information, documents, and videos pertaining to the investigation and the arrest of the 10 Russian "Sleeper" Agents arrested in 2010. The information was released as a result of a freedom of information request. As you are undoubtedly aware, press and media coverage of this news has been extensive.

At the FBI's public web site you will find videos showing surveillance of these agents, some of the methods and techniques they used to operate, their tradecraft, and court filings detailing the case against these agents.

We have reprinted the information at the web site within this newsletter, including hypertext links to the videos and documents. We strongly encourage you to visit the www.fbi.gov web site to view this information in its original form, as well as to view numerous historical documents pertaining to espionage and other related National security investigations. A direct link to the "Ghost Stories" information follows below:
http://www.fbi.gov/news/stories/2011/october/russian_103111/russian_103111

Russian spy Christopher Metsos, right, swaps information in a "brush pass" with an official from the Russian Mission in New York in 2004. The image from a video is part of a trove of documents, photos, and surveillance released by the FBI as part of a Freedom of Information Act (FOIA) request.
FBI Vault: Videos | Photographs | Documents

Operation Ghost Stories
Inside the Russian Spy Case

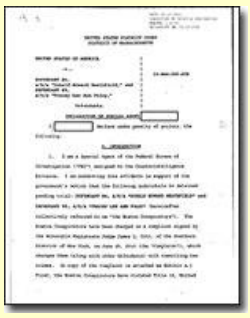
10/31/11

The arrests of 10 Russian spies last year provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended. The highly publicized case also offered a rare glimpse into the sensitive world of counterintelligence and the FBI's efforts to safeguard the nation from those who would steal our vital secrets.

Our case against the Russian Foreign Intelligence Service (SVR) operatives—dubbed Operation Ghost Stories—went on for more than a decade. Today we are releasing dozens of still images, surveillance video clips, and documents related to the investigation as part of a Freedom of Information Act request.

Photo Gallery

Video Gallery



Documents

Ghost Stories

"The Russian government spent significant funds and many years training and deploying these operatives," said one of our counterintelligence agents who worked on the case. "No government does that without expecting a return on its investment."

Our agents and analysts watched the deep-cover operatives as they established themselves in the U.S. (some by using stolen identities) and went about leading seemingly normal lives—getting married, buying homes, raising children, and assimilating into American society. Using surveillance and sophisticated techniques, aided by support from intelligence analysts, investigators gathered information to understand the threat posed by the spies as well as their methods, or tradecraft.

The SVR was in it for the long haul. The illegals were content to wait decades to obtain their objective, which was to develop sources of information in U.S. policymaking circles. (See sidebar.)

Although the SVR "illegals," as they were called, never got their hands on any classified documents, their intent from the start was serious, well-funded by the SVR, and far-ranging.

Spotting and Assessing

The deep-cover Russian spies may not have achieved their objective, but they were not idle. They collected information and transmitted it back to Russia, and they were actively engaged in what is known in the spy business as "spotting and assessing."

They identified colleagues, friends, and others who might be vulnerable targets, and it is possible they were seeking to co-opt people they encountered in the academic environment who might one day hold positions of power and influence.

Perhaps the most famous example of this tactic—the Cambridge Five—took place in Great Britain. Soviet intelligence "talent spotters" were able to recruit Cambridge University students in the 1930s—including future spy Kim Philby—who would later rise to power in the British government and become Soviet operatives during World War II and into the 1950s.

"We believe the SVR illegals may well have hoped to do the same thing here," said a counterintelligence agent.

Although they didn't achieve that objective, the agent said, "without us there to stop them, given enough time they would have eventually become successful." After years of gathering intelligence and making sure we knew who all the players were, we arrested the illegals on June 27, 2010. Weeks later, they pled guilty in federal court to conspiring to serve as unlawful agents of the Russian Federation within the U.S.

The plea represented the culmination of a remarkable effort on the part of countless Bureau personnel, including agents, analysts, surveillance teams, linguists, and others.
"Operation Ghost Stories sends a message to foreign intelligence services that espionage threats to the U.S. will not be tolerated," our agent said. "The FBI's counterintelligence mission is to identify, disrupt, and defeat the activities of foreign espionage agents, and we take that job very seriously."

Usually, the critical work of our Counterintelligence Division is carried out in conjunction with our partners in the U.S. intelligence community with the utmost secrecy. Because the public rarely hears about those efforts, it would be easy to forget how real the threat of espionage is.

"And the threat is not limited to the Russians," the agent said. "There are a lot of foreign services who want what we have, and that's why we have agents and analysts in FBI field offices across the country working with other intelligence community partners every day to address these threats."

Resources:
- Ghost Stories: Russian Foreign Intelligence Service (SVR) Illegals
- Foreign Counterintelligence Stories

Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry

The Defense Security Service (DSS) has recently published its annual report, Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry, the 2011 edition. It can be read online in its entirety at the following web link: http://www.dss.mil/counterintel/2011-unclassified-trends.pdf .

We strongly encourage you to review this publication. Security educators as well as security managers will gain valuable insights into the multifaceted threats targeting the defense industry. This report shows growing trends in the collection efforts targeting the industry.

We are extracting one focus area contained within this report, and reprinting it within this newsletter. This particular area, Targeting Autonomous Underwater Vehicle Technologies, has been discussed in detail in ABC news reports as well as in print. This sample clearly shows the quality of the report in its totality.
We highly recommend you contact your DSS representatives to discuss this report and to seek opportunities for you and your employees to receive DSS briefings on this report, or other security educational training.

REPORT EXTRACT FOLLOWS:

Targeting Autonomous Underwater Vehicle Technologies

SPECIAL FOCUS AREA:

TARGETING AUTONOMOUS UNDERWATER VEHICLE TECHNOLOGIES

1. OVERVIEW

Autonomous underwater vehicles (AUVs) are a class of underwater vessels capable of submerged, self-propelled locomotion using various enabling technologies to navigate and perform diverse tasks.

AUVs have a variety of military and commercial uses. The U.S. Navy identifies nine areas for its AUV programs: intelligence, surveillance and reconnaissance (ISR); mine counter measures (MCM); anti-submarine warfare (ASW); inspection and identification; oceanography; communication/navigation network node; payload delivery; information operation; and time-critical strike.

Commercial applications include underwater surveys, fisheries research, search and recovery, wreck and navigational hazard mapping, and water profile sampling.

Many AUVs can be configured for a variety of underwater missions, and some commercial and military missions are similar in nature.

AUVs provide navies with a cost-effective way to modernize their ability to affect underwater battlespace and protect key ports and installations.

The Defense Security Service (DSS) intends this special focus area assessment to alert cleared industry to the increasing foreign threat to AUV technology and assist in countering that threat.

2. TREND ANALYSIS

As of late 2009, there were approximately 630 AUVs worldwide. Experts anticipate the AUV market will grow exponentially by 2020, with roughly 1,400 AUVs being built over the next decade to meet worldwide demands. They project global expenditures on AUVs to total 2.3 billion U.S. dollars from 2010 to 2019.

Military applications of AUVs have lagged behind commercial ones; however, military research and funding is increasing at a rapid pace throughout the world

as more countries realize the potential value of AUVs and invest in research and development (R&D). By 2020, maritime experts expect militaries to provide roughly half of all AUV funding. Obtaining sensitive U.S. information regarding AUVs will provide other countries with needed information to advance their indigenous AUV programs and their production of countermeasures to U.S. military systems.

Foreign interest in U.S. AUV technologies has risen over the past several years, as indicated by increased collection attempts.

Industry reporting from fiscal year 2010 (FY10) reflects this trend: foreign entities that actively targeted cleared contractors working on AUV issues showed a particularly strong interest in transforming and upgrading their naval forces. Foreign collectors employed a variety of collection techniques to gain access to sensitive, classified, or export-controlled information. Common methods of operation (MOs) included requests for information (RFIs), suspicious network activity (SNA), solicitation or marketing, and seeking employment with cleared contractors.

3. COLLECTOR ORIGINS

During FY10, of those targeting AUV platforms and associated technologies, entities from East Asia and the Pacific led the way with 72 percent of the total, followed by others from the Western Hemisphere, Near East, Europe and Eurasia, and South and Central Asia, none with more than 13 percent of the total.

EAST ASIA AND THE PACIFIC

The geography of the East Asian and Pacific region contributes to interest in expanding and improving naval capabilities. AUVs can provide both offensive and defensive capabilities in both littoral waters and further offshore.

Some East Asian and Pacific countries have contentious relationships with each other. When one country demonstrates an aggressive interest in developing a new naval technology such as AUVs, this can spur a parallel interest in other regional neighbors, targeting the same technologies, and extending even to the use of similar MOs.

None of the regions have achieved the U.S. level of overall industrial development nor the capability for military applications of technology. Access to more advanced AUV technology would allow the regions to both accelerate the implementation of improved underwater systems and save time and money by obtaining and reverse-engineering U.S. AUV technologies.

East Asia and the Pacific was the most prolific region in reported collection attempts directed at U.S. AUV technologies in FY10, accounting for over 70 percent of all AUV-related suspicious contact reports (SCRs) worldwide.

Analyst Comment: The U.S. Navy's ability to establish and maintain underwater battlespace dominance is of special importance in this region. Successful development of AUVs for East Asian and Pacific military purposes would likely pose a threat to that dominance by increasing foreign understanding U.S. AUV technologies, potentially enabling them to develop effective countermeasures. (Confidence Level: Moderate)

Based on past practice, the East Asian and Pacific region also represents a significant risk of unauthorized transfer of AUV technology, not only within the region but also to other regions. Such transfer might be motivated by either commercial profit or geostrategic goals, and could be performed deliberately or inadvertently, the latter the result of less-than-robust export control systems.

THE NEAR EAST

Near East AUV programs lag behind those of the United States and East Asia and the Pacific. Collection efforts originating in the region remain at a relatively low level. However, those efforts do continue, as evidenced by industry reporting, and are likely to represent an increasing priority over the next decade. AUVs have particular value for regional powers, as asymmetric naval strategies can threaten sea lines of communication at their most vulnerable points.

4. AFFILIATIONS AND METHODS OF OPERATION

East Asian and Pacific collectors primarily depended on commercial entities to obtain sensitive U.S. technology in FY10.

Suspicious entities used RFIs in more than half of the AUV-related SCRs, with emails, faxes, or phone calls to seek price quotes and technical information being most prevalent. SNA accounted for a quarter of the incidents targeting cleared facilities working on AUV technology in FY10.

AUVs are a dual-use technology and brokers often claimed that the technologies sought were for commercial use. Commercial entities falsified documents and misrepresented end users to collect controlled U.S. technologies.

Analyst Comment: If AUV suppliers were to ship such technology, such purchasers would likely provide it to government or military end users, either for

employment on an existing AUV platform or for longer-term reverse engineering. (Confidence Level: Moderate)

Similarly, collecting entities such as government-affiliated universities often used academic solicitation, describing the sensitive AUV information targeted as having solely scientific and educational purposes with little to no apparent military application. Personnel affiliated with academic institutions sought to sponsor exchanges of personnel or information, submit research papers for peer review, or send students to participate in classified or sensitive research projects.

Analyst Comment: Suspicious entities successful in establishing such relationships would almost certainly seek to exploit them to gain access to sensitive or classified U.S. AUV information and technology. (Confidence Level: High)

Other government-affiliated entities from East Asia and the Pacific that engaged in AUV technology collection efforts in FY10 included state-sponsored R&D agencies.

UNDERWATER GLIDERS

Gliders are a type of AUV designed specifically for oceanic missions that require long endurance: weeks, or even months. By comparison, other AUVs tend to conduct limited-duration missions lasting hours, or at most days.

Underwater gliders make use of a variety of auxiliary driving mechanisms, such as ocean thermal energy, to quietly "glide" in the water with minimal energy consumption. While not as fast as standard AUVs, gliders using buoyancy-based propulsion have a significantly greater range and mission duration than AUVs propelled by electric motors. This makes them ideal for ISR. Diving abilities depend on the specific glider, but most range between 200 and 1,500 meters; deeper-diving gliders are under development.

Underwater gliders typically carry sensors such as sonar, hydrophones, and thermal sensors used for mapping or monitoring the ocean environment and wildlife. The U.S. Navy uses gliders for battlespace reconnaissance and mapping. Flotillas of gliders can establish a sensing network in an operational area of interest to provide commanders with the data to support their mission planning. Industry reporting indicates that foreign targeting of underwater glider technology significantly increased in FY10 when compared to FY09.

Near Eastern collections, in contrast, were more likely to depend on individuals targeting AUVs, using RFIs. Nonetheless, Near East entities also used academic solicitation in their attempts to collect information. Non-traditional collectors such

as individual university students sought research positions or placement at various U.S. universities or facilities where they might gain access to U.S. AUV programs.

Such supposedly unaffiliated students also attended international trade shows, solicited vendors, and attempted to integrate themselves into the scientific community.

5. TARGETED TECHNOLOGIES

DSS analysis of FY10 industry reporting demonstrated the wide range of AUV technology collection attempts. Reporting indicated interest in not only conventional AUVs, but gliders as well, and not only AUVs themselves but all aspects of AUV enabling technologies, such as various types of underwater sensors. Countries wishing to develop a robust military AUV capacity need to improve both overall AUV capabilities and enabling technologies. Such capabilities and technologies include navigation, communications, design and construction, sensors, propulsion, and power.

Similarly, collectors ranged from sophisticated producers in industrially advanced countries seeking specialized sub-systems to emerging third-world countries seeking entire AUV systems for military modernization programs.

6. ANALYTICAL FORECAST
Reporting from industry confirms that U.S. AUVs and related technologies are of significant interest to the rest of the world.

Commercial, individual, and government affiliated entities are likely to continue using a variety of MOs, especially RFI and SNA, to collect U.S. AUV technology and information. (Confidence Level: Moderate)

Any technologies or information acquired will likely help foreign governments develop their indigenous AUVs, assist foreign navies in countering U.S. AUVs, and increase the threat to U.S. undersea battlespace dominance. (Confidence Level: Moderate)

Based on trends in the AUV industry, DSS assesses that it is very likely that demand for AUVs will increase dramatically over the next several years, especially as more military and commercial capabilities develop. DSS assesses that, as the technology advances, foreign collectors will almost certainly increase their efforts to satisfy that demand by targeting U.S. cleared contractors working on AUVs or related systems. (Confidence Level: High)

CASE STUDY

In 2010, a U.S. cleared contractor received an email from an East Asian and Pacific company requesting to purchase one of the cleared contractor's military AUVs and other related components, including batteries and a communications antenna. The requestor did not specify either the intended use or the end users.

This collection attempt should be considered in the context of a pattern of similar reported incidents that demonstrated the substantial East Asian and Pacific interest in acquiring AUV technology. Over the course of seven months in FY10, ostensibly commercial entities and academic institutions from the region made five separate requests to purchase export controlled AUV technology.

Analyst Comment: Records of such collection attempts capture the number and diversity of East Asian and Pacific commercial entities submitting RFIs for AUVs or enabling technologies.

Any such AUV technology obtained by these companies, although dual-use, would probably find its way to military applications, providing much-needed assistance to indigenous AUV programs. Such acquisitions would likely assist collecting countries in understanding current levels of U.S. AUV technology, thus aiding in their development of countermeasures. (Confidence Level: Moderate)

END OF REPORT EXTRACT

Visitors: Risks & Mitigations

http://www.fbi.gov/about-us/investigate/counterintelligence/risks-mitigations-of-visitors

Reprinted below is a new FBI produced CI Awareness brochure designed to provide best practices for mitigating the risks posed by visitors entering your facilities.

We are reprinting the brochure in this month's newsletter because of its strong potential of being an important tool in your security program. We highly encourage you to download, reprint, and disseminate to your employees the brochure in its original form.

This brochure, in its original form, may be downloaded at the link below.

Download printable version (pdf):
http://www.fbi.gov/about-us/investigate/counterintelligence/Risks%20-%20Mitigations%20of%20Visitors%20Brochure.pdf

Visitors entering your facility could pose a security risk to your intellectual property or competitive edge. It is an opportunity for competitors to collect information that is not readily available to them. Some visitors may be trained to verbally elicit information, some may brazenly ignore the security parameters of a tour, and others may use concealed recording devices all in order to obtain restricted information. Some information they collect may seem innocuous, such as the facility layout, but could be very valuable to them and give them clues about your products or how to run their own facility better. Do not tell competitors how to squeeze past you in the economic race, and do not help thieves steal your information.

A visitor played with his wristwatch in a manner that made the host suspicious that a micro camera might be in the watch.

Foreign visitors put double-sided tape on the soles of their shoes in order to collect slivers of metal alloys from the floor of a production plant for US military planes. They later analyzed the slivers to determine the exact metallic components used in the planes.

Security during Facility Tours

There are a number of commercially available audio and video recording devices disguised as pens, sunglasses, buttons, key fobs, cigarette packs, etc. It may be nearly impossible to keep such devices from entering your facility. Keep this in mind when planning tours.

■Brief all employees on threat issues surrounding visitors
■Brief appropriate personnel (escorts, those briefing visitors, and those whose workspace will be toured) on the scope of the visit
■Ensure the number of escorts per visitor is adequate to properly supervise and control visitors
■Confirm escorts are trained and knowledgeable about possible techniques of visitor theft
■Make sure employees know when visitors will be in their space and remind them to shield proprietary information from the visitors' view
■Ensure visitors are easily identifiable (visitor badge, visitor vest, etc.)
■Notify visitors of appropriate security and safety protocols prior to their visit, to include the consequences for not complying with those protocols
■Do not hesitate to end the tour and escort visitors out of the facility for non-compliance or other security concerns

Indicators that a visitor may be trying to obtain restricted information during a tour:

■Makes last minute additions or changes to the visitor roster
■Attempts (or succeeds) to bring unauthorized electronic or recording devices into sensitive/ prohibited areas
■Attempts to photograph items with cell phones or micro cameras (fiddling or apparent positioning of a watch, pen, or other personal item)
■Does not adhere to the stated purpose of the visit
■Asks questions outside the scope of the approved visit Acts offended or belligerent when confronted about a security or protocol incident
■Wanders off route or pretends to get lost during the tour
■If a request for a sensitive or classified tour is denied, a request for a less sensitive or commercial tour is made
■Makes repeated visits to the facility
■Foreign visitors are escorted by a Foreign Liaison Officer or embassy official who attempts to conceal his/her official identity during a supposed commercial visit

Security during Long-term Visits and Joint Ventures

Long-term visits or joint ventures may provide an even greater opportunity for a competing company to obtain restricted information. They may also provide an opportunity for visitors to spot, assess, and befriend employees that may assist (either wittingly or unwittingly) in collecting restricted information for a visitor during the time of the visit or in the future.

Foreign visitors from a "partnering" university photographed, without approval, every item in another university's established research lab, to include the make and model of the equipment. The two labs were supposed to be collaborating, but the

established lab's director eventually realized his lab was the only one sharing information.

■Educate employees extensively on the scope of the project and how to report security concerns
■Provide employees with training on how to detect elicitation and recruitment attempts
■Brief employees prior to the arrival of visitors on visitor access limitations, potential collection techniques, economic espionage indicators, and to whom to report security concerns
■Provide periodic and sustained reminders on the scope of the project and elicitation detection
■Brief visitors on their obligations and responsibilities including limitations on access or use of computers, copiers, or fax machines, and access limitations to buildings or rooms
■Require visitors to sign an agreement that they will comply with listed security requirements; the agreement should state the consequences for non-compliance
■Share the minimum amount of information appropriate to the scope of the joint venture
■Ensure penalties for noncompliance or negligence by employees and visitors are well known
■Label proprietary and classified information
■Refuse to accept unnecessary representatives into the facility
■Do not allow visitors to use networked computers; provide stand-alone computers if needed
■Review all documents visitors fax, mail, or email, and translate them when necessary
■Periodically interview employees who have frequent contact with visiting personnel to check for indicators of economic espionage or elicitation/ recruitment attempts
■Conduct regular computer audits to detect any efforts by visitors or employees to exceed their approved computer access

Under the pretext of reading a text message, a visitor used his cell phone camera to photograph a trade secret device. The photos were emailed to engineers who were then able to design and produce a similar product.

Indicators that long-term visitors may be trying to obtain restricted information:

■A company entices you to provide large amounts of technical data as part of the bidding process, only to cancel the contract
■Potential technology sharing agreements during the joint venture are one-sided
■The partnering company sends more representatives than is necessary for the project
■The visitors single out company personnel to elicit information outside the scope of the project
■Visitors want access to the local area network
■Visitors want unrestricted access to the facility
■A visitor faxes or emails documents to an embassy or another country
■A visitor tries to attach an unapproved thumb drive or other device to a computer
■Visitors continually forget security protocols, or need to be reminded "you can't do that"

Additional Indicators that a Visitor is Trying to Obtain Restricted Information

Foreign visitors dipped their ties into chemical solutions in order to obtain samples of the product. They also fanned out in different directions and photographed everything they could in the facility. The host company was subsequently unable to find a market for its product in that country.

■Inadvertent disclosure of sensitive, proprietary, or project information
■Improper wearing of security identification badge
■Non-existent security identification badge or "forgets" identification badge
■Photographs or keeps security identification badge
■Requests or gains access to an area that is beyond the scope of their visit
■Requests information that is beyond the scope of their access
■Requests information that is classified, dual-use, or otherwise controlled
■Missing or unaccounted for equipment or documentation

■Asks questions about programs using acronyms specific to the program that they should not necessarily know about
■Use of social manipulation or elicitation techniques to gain more information

Post-Visit Protocols

■Change passwords, locks, and access controls to rooms, buildings, and computers that long-term visitors used
■Brief employees on what information can and cannot be shared once the long-term visit or joint venture is completed
■Educate employees on the policies regarding subsequent contacts from the visitors (the policy may need to provide guidance on contacts via business email, personal email, telephone, in person, social networking sites, etc.); train employees on how to appropriately handle contact with prior visitors

A joint venture contract allowed three employees from one company to work in the facility of the other. When the venture was terminated, the three employees attempted to take proprietary information out of the host's facility in boxes labeled as their personal belongings.

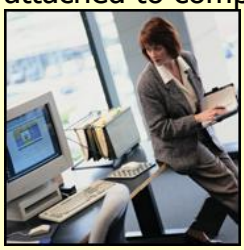
Indicators that previous visitors may be trying to obtain restricted information:

■A prior visitor invites an employee to provide a lecture or receive an award at the visitor's overseas company
■An unsolicited email from an associate of a prior visitor requests information or a service that should be directed to another department or person (e.g. sales department)
■Social contact (via email, telephone, social networking sites, or in person) that is inappropriate or manipulative
■A prior visitor requests favors or additional information
■A prior visitor requests sensitive information on projects outside the scope of their visit
■A visitor, or visitor's organization, sends a request to complete surveys or questionnaires
■A prior visitor advises the recipient not to worry about security concerns, or asks the recipient to ignore a request if it causes a security concern

General Guidance

■Do not leave sensitive information unattended
■Obtain approval from a supervisor before sharing any sensitive, proprietary, or project information; ensure the recipient is authorized to receive such information

■If authorized to share sensitive or proprietary information, do not discuss it in an unsecured/ open environment
■Discard sensitive information in a safe manner (e.g. shred)
■Lock computer workstations when unattended
■Do not store passwords and login instructions at workstations
■Do not share access codes, user names, or passwords with anyone
■Do not leave electronic storage devices unattended (external hard drives, thumb drives, laptops etc.)
■Do not allow personal software or hardware (thumb drives) to be installed or attached to company networks without written permission



If you notice any suspicious behavior or activity, immediately report it to your security officer. Let security determine if an incident is innocent. For additional information or training, contact the FBI.

Trade Secret = all types of information (financial, business, scientific, technical, economic, or engineering information including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, codes – whether tangible or intangible) which: (1) the owner has taken reasonable measures to keep secret, and (2) has independent economic value.

Proprietary Information = information that is not available to the public, has been developed by the holder, and is viewed as the property of the holder, but does not rise to the level of a trade secret.

Sensitive Information = information not shared publicly, but is not proprietary. It may include information that is export controlled or has publication restrictions.

About InfraGard and the Research and Technology Protection InfraGard Special interest Group (SIG)

Readers of this newsletter who do not belong to InfraGard are strongly encouraged to become members.

InfraGard members affiliated with the scientific and technological research and development fields (designed for companies and universities involved in original research) are eligible to become members of the Research and Technology Protection InfraGard Special interest Group (SIG).

The Research and Technology Protection InfraGard SIG enhances the efforts to protect research and technology made by private industry, academia and government through information-sharing networks with a private secure portal of communication.

The Research and Technology Protection InfraGard SIG is a collaborative effort of the Foreign-Counterintelligence and Cyber Divisions of the FBI. It is intended to enhance the sharing of information among private sector stakeholders who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting the innovation that drives our national economy.

Membership in the Research and Technology Protection InfraGard SIG is only open to members of InfraGard. Information about InfraGard and membership follows:

http://infragard.org/about.php?mn=1&sm=1-0

19-Oct-2011

45,007 MEMBERS (Including FBI)

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and

the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.

Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.

Provide members value-added threat advisories, alerts, and warnings.

Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.

Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

Each FBI Field Office has a Special Agent Coordinator who gathers interested individuals to form a chapter. Any individual can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer:

Training and education initiatives

A local newsletter

A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board established several committees to address issues such as membership, incorporation, and partnerships with other private sector association / organizations.

Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

The InfraGard secure website provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members.

Welcome to InfraGard Tampa Bay

InfraGard is a national education and information sharing program created by and between the Federal Bureau of Investigation (FBI) and the private/public sector. There are InfraGard groups in cities around the country. Their individual and combined objectives include the mitigating of local, state and national vulnerabilities which terrorists might attempt to exploit. By their implementation, these objectives also provide increased protection against criminal activities found in our cities and towns, corporate environments, and our personal lives.

InfraGard Tampa Bay > Home
infragardtampabay.org/
The **Tampa Bay Infragard** Group is a non-profit 501(c)3 Corporation affiliated with **Infragard** National formed to provide a working group of cyber-security industry **...**

About

InfraGard is an information sharing and analysis effort **...**

InfraGard Tampa Bay > Home

InfraGard Tampa Bay is committed to protecting your privacy **...**

How to Join

BECOME A MEMBER OF **INFRAGARD**. Help protect our **...**

Cyber Security

Florida is 2nd nationally in Computer Crime. Theft of trade **...**

Calendar

Tampa Chapter meetings 19 Jan 2006 16 Mar 2006 18 May **...**

Untitled Document

The **Tampa Bay Infragard** Group is a non-profit 501(c)3 **...**

Infragard Orlando Members Alliance, Inc.

The Tampa FBI Office covers most of Central Florida. Spanning 18 counties, from Cape Canaveral on the east coast to St. Petersburg on the west coast and stretching south to Naples. Tampa FBI participates in two InfraGard Chapters, Tampa Bay and Orlando.

http://infragardtampabay.org/

Membership

Before you fill out your application, please read the InfraGard Code of Ethics and browse the other Policies and Procedures. As a member of InfraGard, you will be expected to abide by these

guidelines.

To fill out an application:

1. Go to www.Infragard.net
2. Click on the "become a member" menu bar
3. Follow the instruction

Once submitted, your application will be processed as quickly as possible. You will be notified of your InfraGard membership status. While your application is being processed, you are encouraged to attend open chapter meetings.

The following United States Government-issued security clearances are qualified substitutes for the records check required for InfraGard membership:

- Confidential
- Secret
- Top Secret

An InfraGard applicant/member may submit evidence of their possession of one of the above clearances to expedite the initial processing and periodic renewal of their InfraGard membership.

Membership Information Request

If you have any questions regarding the application process, please submit the form below or contact Marie Wright at 813-253-1312.

First Name: *	
Last Name: *	
Daytime Phone:	
Evening Phone:	
Email: *	
Comments:	Enter comments here!

Submit Reset

InfraGard is an organization dedicated to the protection of the United States and the American people. In order to maintain a level of trust within the membership, all applicants undergo a background check performed by the FBI (for this reason InfraGard membership is currently limited to United States citizens). Applications are then screened according to defined criteria by the local FBI field office and in some instance the unit which oversees the InfraGard Program at FBI Headquarters.

Along with your InfraGard membership comes great responsibility. We value active members who are willing to devote their time, effort and talent to help build this organization and achieve our goals of protecting the American people. You will be a representative of the nation's largest volunteer organization dedicated to critical infrastructure protection.

ARRESTS, TRIALS AND CONVICTIONS

Five Individuals Indicted in a Fraud Conspiracy Involving Exports to Iran of U.S. Components Later Found in Bombs in Iraq

http://www.fbi.gov/minneapolis/press-releases/2011/five-individuals-indicted-in-a-fraud-conspiracy-involving-exports-to-iran-of-u.s.-components-later-found-in-bombs-in-iraq

Indictment Also Alleges Fraud Conspiracy Involving Illegal Exports of Military Antennas to Singapore and Hong Kong

U.S. Department of Justice October 25, 2011

Office of Public Affairs (202) 514-2007/TDD (202) 514-1888

WASHINGTON—Five individuals and four of their companies have been indicted as part of a conspiracy to defraud the United States that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq. Some of the defendants are also charged in a fraud conspiracy involving exports of military antennas to Singapore and Hong Kong.

Yesterday, authorities in Singapore arrested Wong Yuh Lan (Wong), Lim Yong Nam (Nam), Lim Kow Seng (Seng), and Hia Soo Gan Benson (Hia), all citizens of Singapore, in connection with a U.S. request for extradition. The United States is seeking their extradition to stand trial in the District of Columbia. The remaining individual defendant, Hossein Larijani, is a citizen and resident of Iran who remains at large.

The arrests and the indictment 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 the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE); Mark Giuliano,

Executive Assistant Director of the FBI's National Security Branch; Eric L. Hirschhorn, Under Secretary of Commerce; and David Adelman, U.S. Ambassador to Singapore.

"Today's charges allege that the defendants conspired to defraud the United States and defeat our export controls by sending U.S.-origin components to Iran rather than to their stated final destination of Singapore. Ultimately, several of these components were found in unexploded improvised explosive devices in Iraq," said Assistant Attorney General Monaco. "This case underscores the continuing threat posed by Iranian procurement networks seeking to obtain U.S. technology through fraud and the importance of safeguarding that technology. I applaud the many agents, analysts and prosecutors who worked on this extensive investigation."

"These defendants misled U.S. companies in buying parts that they shipped to Iran and that ended up in IEDs on the battlefield in Iraq," said U.S. Attorney Machen. "This prosecution demonstrates why the U.S. Attorney's Office takes cases involving misrepresentations regarding the intended use of sensitive technology so seriously. We hope for a swift response from Singapore to our request for extradition."

"One of Homeland Security Investigations' (HSI) top enforcement priorities is preventing sensitive technology from falling into the hands of those who might seek to harm American personnel or interests—whether at home or abroad," said ICE Director Morton. "This international investigation conducted by ICE's HSI and our law enforcement partners demonstrates the importance of preventing U.S. technology from falling into the wrong hands, where it could potentially be used to kill or injure our military members and our allies. Our agency will continue to work closely through our attachés to identify these criminals, dismantle their networks, and ensure they are fully prosecuted."

"This multi-year investigation highlights that acquiring property by deceit has ramifications that resonate beyond the bottom line and affects our national security and the safety of Americans worldwide," said FBI Executive Assistant Director Giuliano. "We continue to work side-by-side with our many partners in a coordinated effort to bring justice to those who have sought to harm Americans. We consider this investigation as the model of how we work cases—jointly with the Department of Homeland Security/Immigration and Customs Enforcement and the Department of Commerce/Office of Export Enforcement and collectively with our foreign partners to address the threats posed by Iranian procurement networks to the national security interests of the United States both here and abroad."

"These cases are the product of vigorous, cooperative law enforcement focused on denying to Iran items that endanger our coalition forces on the battlefield in Iraq," said Under Secretary of Commerce Hirschhorn. "We will continue

aggressively to go after such perpetrators—no matter where they operate—to guard against these types of threats."

U.S. Ambassador to Singapore, David Adelman, praised the cooperation within the U.S. executive branch agencies and with the Singaporean authorities. "Twenty-first century law enforcement is most effective when countries work collaboratively as evidenced by this strong, cooperative effort between the U.S. and Singapore. Congratulations to all the officials in both our countries who made this happen," he said.

The Charges

The indictment, which was returned in the District of Columbia on Sept. 15, 2010, and unsealed today, includes charges of conspiracy to defraud the United States, smuggling, illegal export of goods from the United States to Iran, illegal export of defense articles from the United States, false statements and obstruction of justice.

The charged defendants are Iranian national Larijani, 47, and his companies Paya Electronics Complex, based in Iran and Opto Electronics Pte, Ltd., based in Singapore. Also charged is Wong, 39, 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, Nam, 37. Finally, the indictment charges Corezing International Pte. Ltd., a company in Singapore that maintained offices in China, as well as Seng, 42, an agent of Corezing, and Hia, 44, a manager, director and agent of Corezing.

Wong, Nam, Seng and Hia allegedly conspired to defraud the United States by impeding U.S. export controls relating to the shipment of 6,000 radio frequency modules from a Minnesota company through Singapore to Iran, some of which were later found in unexploded IEDs in Iraq. Seng and Hia are also accused of conspiring to defraud the United States relating to the shipment of military antennas from a Massachusetts company to Singapore and Hong Kong. Singapore has agreed to seek extradition for Wong and Nam on the charge of conspiracy to defraud the United States relating to the components shipped to Iran, and to seek extradition for Seng and Hia on the charge of conspiracy to defraud the United States relating to the military antenna exports.

In coordination with the criminal actions announced today, 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 addition to the five individual defendants in this case, the Commerce Department named additional companies and individuals associated with this conspiracy. In placing these parties on the Entity List, the Commerce Department is imposing a licensing requirement for any item subject to Commerce regulation with a presumption that such a license would be denied.

Exports of U.S. Components Later Found in IEDs

According to the indictment, IEDs caused roughly 60 percent of all American combat casualties in Iraq between 2001 and 2007. The first conspiracy alleged in the indictment involved radio frequency modules that have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs.

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. In each transaction, the defendants allegedly told the Minnesota firm that Singapore was the final destination of the goods. The defendants also caused false documents to be filed with the U.S. government, in which they claimed that a telecommunications project in Singapore was the final end-use for the modules. In reality, each of the five shipments was routed from Singapore to Iran via air cargo. The alleged recipient of all 6,000 modules in Iran was Larijani, who had directed Wong, his employee in Singapore, to order them.

According to the indictment, the defendants profited considerably from their illegal trade. The defendants allegedly made tens of thousands of dollars for arranging these illegal exports from the United States through Singapore to Iran.

The indictment alleges that several of the 6,000 modules the defendants routed from Minnesota to Iran were later discovered by coalition forces in Iraq, where they were being used as part of the remote detonation systems of IEDs. In May 2008, December 2008, April 2009, and July 2010, coalition forces found no less than 16 of these modules in unexploded IEDs recovered in Iraq, the indictment alleges.

During this period, some of the defendants were allegedly communicating with one another about U.S. laws prohibiting the export of U.S.-origin goods to Iran. For example, between October 2007 and June 2009, Nam contacted Larijani in Iran at least six times and discussed the Iran prohibitions and U.S. prosecutions for violation of these laws. Nam later told U.S. authorities that he had never participated in illicit exports to Iran, even though he had participated in five such shipments, according to the indictment.

Exports of Military Antennas

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 cavity-backed spiral antennas and biconical antennas to be illegally exported from a Massachusetts company to Singapore and Hong Kong without the required State Department license.

These military antennas are controlled for export as U.S. munitions and are used in airborne and shipboard environments. The indictment states that the biconical antenna, for example, is used in military aircraft such as the F-4 Phantom, the F-15, the F-111, the A-10 Thunderbolt II and the F-16 combat jets.

Seng, Hia and Corezing are alleged to have, among other things, conspired to undervalue the antennas to circumvent U.S. regulations on the filing of shipper's export declarations to the U.S. government. They also allegedly used false names and front companies to obtain the antennas illegally from the United States.

Additional Misrepresentations

The indictment further alleges that Larijani, based in Iran, made false statements about doing business with an accused Iranian procurement agent and that he attempted to obstruct an official proceeding by the U.S. Department of Commerce.

In January 2010, the Department of Commerce placed Larijani's company, Opto Electronics, on the Entity List, which is a list of companies to which U.S. businesses cannot export controlled dual-use items without obtaining U.S. government licenses. In response, Larijani repeatedly contacted Commerce Department officials in Washington, D.C., from Iran, requesting that his company be removed from the Entity List, according to the indictment. Commerce officials advised Larijani that, in considering whether his firm should be removed from the list, he needed to disclose whether he or his firm had any involvement with Majid Kakavand or Evertop Services Sdn Bhd.

Kakavand is an accused Iranian procurement agent who has been indicted in the United States, along with his Malaysian company Evertop Services, for illegally exporting U.S. goods to Iran, including to military entities in Iran involved in that nation's nuclear and ballistic missile programs. Kakavand remains a fugitive and is believed to be in Iran.

According to the indictment, Larijani denied to Commerce officials on three occasions that he or his company, Opto Electronics, had done any business with Kakavand or Evertop Services. In fact, the indictment alleges that Larijani had been in communication with others about his business dealings with Kakavand on at least five occasions from 2006 through 2009.

This investigation was jointly conducted by ICE agents in Boston and Los Angeles; FBI agents in Minneapolis; and Department of Commerce, Bureau of Industry and Security agents in Chicago and Boston. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, particularly the Justice Department Attaché in the Philippines, as well as the FBI and ICE Attachés in Singapore.

U.S. law enforcement authorities thanked the government of Singapore for the substantial assistance that was provided in the investigation of this matter.

The prosecution is being handled by Assistant U.S. Attorneys Anthony Asuncion and John W. Borchert of the U.S. Attorney's Office for the District of Columbia; and Trial Attorneys Jonathan C. Poling and Richard S. Scott of the Counterespionage Section of the Justice Department's National Security Division.

The public is reminded that an indictment contains mere allegations. Defendants are presumed innocent unless and until proven guilty in a court of law.

Richardson soldier arrested by U.S. Army Counterintelligence (CI) and Criminal Investigation Command (CID) Agents

http://www.armytimes.com/news/2011/10/army-richardson-soldier-arrested-espionage-probe-102911w/

As reported in the media, and based on statements from a spokesman for U.S. Army Alaska, Specialist William Millay has been arrested on suspicion of espionage on Friday, October 28th.

Specialist Millay was arrested by U.S. Army CI and CID agents at Joint Base Elmendorf-Richardson.

The FBI and Army Counterintelligence are continuing their investigations. Millay is being held by the Alaska Department of Corrections, as a federal inmate.

FBI Anchorage Special Agent in Charge Mary Rook was quoted as stating "Today's arrest was the result of the close working relationship between the FBI and its military partners in Alaska." "Through this ongoing partnership, we are better able to protect our nation."

Actual and potential charges have not yet been disclosed.

Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets

http://www.justice.gov/usao/ins/press_releases/Pressrelease11/Huang.20111018.pdf

FOR IMMEDIATE RELEASE CRM/NSD

TUESDAY, OCTOBER 18, 2011 (202) 514-2008

WWW.JUSTICE.GOV TDD (202) 514-1888

First Prosecution in Indiana for Foreign Economic Espionage

WASHINGTON – Kexue Huang, a Chinese national and a former resident of Carmel, Ind., pleaded guilty today to one count of economic espionage to benefit a foreign university tied to the People's Republic of China (PRC) and one count of theft of trade secrets.

The guilty plea was announced by Assistant Attorney General Lanny A. Breuer of the Criminal Division, Assistant Attorney General for National Security Lisa O. Monaco, U.S. Attorney Joseph H. Hogsett of the Southern District of Indiana, U.S. Attorney B. Todd Jones of the District of Minnesota, and Robert J. Holley, Special Agent in Charge of the Indianapolis Field Office of the FBI.

This is the first trade secret prosecution in Indiana under a provision of the Economic Espionage Act that prohibits trade secret theft intended to benefit a component of a foreign government. Since its enactment in 1996, there have been a total of eight such cases charged nationwide under the Economic Espionage Act.

Huang, 46, pleaded guilty to the charges before U.S. District Judge William T. Lawrence in the Southern District of Indiana. In July 2010, Huang was charged in an indictment filed in the Southern District of Indiana for misappropriating and transporting trade secrets to the PRC while working as a research scientist at Dow AgroSciences LLC. Today, a separate indictment filed in the District of Minnesota was unsealed, charging Huang with stealing a trade secret from a second company, Cargill Inc.

According to court documents, from January 2003 until February 2008, Huang was employed as a research scientist at Dow, a leading international agricultural company based in Indianapolis that provides agrochemical and biotechnology products. In 2005, Huang became a research leader for Dow in strain

development related to unique, proprietary organic insecticides marketed worldwide.

As a Dow employee, Huang signed an agreement that outlined his obligations in handling confidential information, including trade secrets, and prohibited him from disclosing any confidential information without Dow's consent. Dow employed several layers of security to preserve and maintain confidentiality and to prevent unauthorized use or disclosure of its trade secrets.

Huang admitted that during his employment at Dow, he misappropriated several Dow trade secrets. According to plea documents, from 2007 to 2010, Huang transferred and delivered the stolen Dow trade secrets to individuals in Germany and the PRC. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research with the intent to benefit foreign universities tied to the PRC. Huang also admitted that he pursued steps to develop and produce the misappropriated Dow trade secrets in the PRC, including identifying manufacturing facilities in the PRC that would allow him to compete directly with Dow in the established organic pesticide market.

According to court documents, after Huang left Dow, he was hired in March 2008 by Cargill, an international producer and marketer of food, agricultural, financial and industrial products and services. Huang worked as a biotechnologist for Cargill until July 2009 and signed a confidentiality agreement promising never to disclose any trade secrets or other confidential information of Cargill. Huang admitted that during his employment with Cargill, he stole one of the company's trade secrets – a key component in the manufacture of a new food product, which he later disseminated to another person, specifically a student at Hunan Normal University in the PRC.

According to the plea agreement, the aggregated loss from Huang's criminal conduct exceeds $7 million but is less than $20 million.

"Mr. Huang used his insider status at two of America's largest agricultural companies to steal valuable trade secrets for use in his native China," said Assistant Attorney General Breuer. "We cannot allow U.S. citizens or foreign nationals to hand sensitive business information over to competitors in other countries, and we will continue our vigorous criminal enforcement of economic espionage and trade secret laws. These crimes present a danger to the U.S. economy and jeopardize our nation's leadership in innovation."

"Today's plea underscores the continuing threat posed by the theft of business secrets for the benefit of China and other nations," said Lisa Monaco, Assistant Attorney General for National Security.

U.S. Attorney Hogsett noted that it is the first time economic espionage has been charged in the Southern District of Indiana. Hogsett remarked that "as U.S. Attorney, I am committed to working with Hoosier businesses who have been victimized and doing everything within our influence to protect Hoosier companies." Hogsett praised Dow for its cooperation with the investigation and prosecution, noting that "companies must first report and then work with federal investigators and prosecutors if we are to stem the illicit export of trade secrets vital to the economy not only of Indiana but the United States." Hogsett also stated, "the dual prosecutions from Indiana and Minnesota should serve as a warning to anyone who is considering robbing American companies of their information and weaken the American economy by selling that information to foreign governments or others that he will face severe consequences. The federal agents and prosecutors who worked tirelessly in these two cases are to be commended for their hard work and dedication."

FBI Special Agent in Charge Holley stated: "Among the various economic espionage and theft of trade secret cases that the FBI has investigated in Indiana, the vast majority involve an inside employee with legitimate access who is stealing in order to benefit another organization or country. This type of threat, which the FBI refers to as the Insider Threat, often causes the most damage. In order to maintain our competitive advantage in these sectors, industry must identify their most important equities, realize that they are a target, implement internal protection mechanisms to protect their intellectual property, and communicate issues of concern immediately to the FBI."

At sentencing, Huang faces a maximum prison sentence of 15 years on the economic espionage charge and 10 years on the theft of trade secrets charge.

The case is being prosecuted by Assistant U.S. Attorney Cynthia J. Ridgeway of the Southern District of Indiana, Trial Attorneys Mark L. Krotoski and Evan C. Williams of the Criminal Division's Computer Crime and Intellectual Property Section, and Assistant U.S. Attorney Jeffrey Paulsen of the District of Minnesota, with assistance from the National Security Division's Counterespionage Section.

Virginia Man Accused of Acting as Unregistered Agent of Syrian Government and Spying on Syrian Protestors in America

http://www.fbi.gov/washingtondc/press-releases/2011/virginia-man-accused-of-acting-as-unregistered-agent-of-syrian-government-and-spying-on-syrian-protestors-in-america

U.S. Department of Justice

October 12, 2011

Office of Public Affairs

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

WASHINGTON—Mohamad Anas Haitham Soueid, 47, a resident of Leesburg, Va., has been charged for his alleged role in a conspiracy to collect video and audio recordings and other information about individuals in the United States and Syria who were protesting the government of Syria and to provide these materials to Syrian intelligence agencies in order to silence, intimidate, and potentially harm the protestors.

The charges were announced by Lisa Monaco, Assistant Attorney General for National Security; Neil MacBride, U.S. Attorney for the Eastern District of Virginia; and James McJunkin, Assistant Director in Charge of the FBI Washington Field Office.

Soueid, aka "Alex Soueid" or "Anas Alswaid," a Syrian-born naturalized U.S. citizen, was charged by a federal grand jury on Oct. 5, 2011, in a six-count indictment in the Eastern District of Virginia. Soueid is charged with conspiring to act and acting as an agent of the Syrian government in the United States without notifying the Attorney General as required by law; two counts of providing false statements on a firearms purchase form; and two counts of providing false statements to federal law enforcement.

Soueid was arrested on Oct. 11, 2011, and will make an initial appearance before U.S. Magistrate Judge Theresa C. Buchanan today at 2:00 p.m. If convicted, he faces a maximum penalty of 15 years in prison on the conspiracy and foreign agent charges, 15 years in prison on the firearms purchase charges and 10 years in prison on the false statement charges.

"Today's indictment alleges that the defendant acted as an unregistered agent of the Syrian government as part of an effort to collect information on people in this

country protesting the Syrian government crack-down. I applaud the many agents, analysts and prosecutors who helped bring about today's case," said Assistant Attorney General Monaco.

"The ability to assemble and protest is a cherished right in the United States, and it's troubling that a U.S. citizen from Leesburg is accused of working with the Syrian government to identify and intimidate those who exercise that right," said U.S. Attorney MacBride. "Spying for another country is a serious threat to our national security, especially when it threatens the ability of U.S. citizens to engage in political speech within our own borders."

"Our national security is threatened when foreign governments use unregistered agents in an attempt to influence and intimidate those who live here lawfully," said FBI Assistant Director in Charge McJunkin. "Their alleged acts desecrate the values cherished in our fair and open society. The FBI will be counted on to detect and deter unregistered agents who attempt clandestine activities on behalf of a foreign political power and work to bring them swiftly to justice."

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

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

The indictment states that in late June 2011, the Syrian government paid for Soueid to travel to Syria, where he met with intelligence officials and spoke with President Bashar al-Assad in private.

He returned to the United States in early July 2011, and he was searched and questioned at Dulles International Airport upon his arrival. The indictment states

that Soueid communicated with his "boss," an unindicted co-conspirator (or UCC-1) who was working for the Mukhabarat, soon after to alert him of the search and questioning and to assure the individual that the airport encounter would not "stop the project."

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

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

The indictment states that the day following the interview, Soueid asked UCC-1 to inform the Mukhabarat about his FBI interview.

In addition, the indictment alleges that, when purchasing a Beretta pistol on July 11, 2011, Soueid listed a false current residence address on a firearms purchase application and in records that were kept by a licensed firearms dealer.

This investigation is being conducted by the FBI's Washington Field Office with assistance from the Loudon County, Va., Sheriff's Office. The prosecution is being handled by Assistant U.S. Attorneys Dennis Fitzpatrick and Neil Hammerstrom of the U.S. Attorney's Office for the Eastern District of Virginia and Trial Attorney Brandon L. Van Grack of the Counterespionage Section of the Justice Department's National Security Division.

The public is reminded that an indictment contains mere allegations and that a defendant is presumed innocent unless and until proven guilty.

Federal Grand Jury Indicts Six Defendants for Fraudulent Aircraft Repairs

http://www.justice.gov/usao/cae/news/docs/2011/09-29-11AircraftRepairIndictment.html

FOR IMMEDIATE RELEASE CONTACT: Lauren Horwood

September 29, 2011

PHONE: (916) 554-2706

www.usdoj.gov/usao/cae

usacae.edcapress@usdoj.gov

SACRAMENTO, Calif. — United States Attorney Benjamin B. Wagner announced that a federal grand jury returned a 36-count indictment today charging Jerry Edward Kuwata, 60, of Granite Bay; Michael Dennis Maupin, 58, of Arbuckle; Scott Hamilton Durham, 39, of Roseville; Christopher Warren MacQueen, 53, of Lincoln; Douglas Arthur Johnson, 52, of Granite Bay; and Anthony Vincent Zito, 47, of Saugus, with conspiracy and fraud involving aircraft parts in interstate commerce, and mail fraud. The defendants are all former executives and supervisors at WECO Aerospace Systems Inc., an FAA-certified air repair station based in Lincoln, which was purchased in 2007 by Gulfstream Aerospace Corporation.

The Federal Aviation Administration (FAA) regulates air travel and publishes regulations that FAA-certified repair stations are required to follow. These regulations include the use of parts that are approved for repairs, as well as tests and inspections that repair stations are required to conduct before a repaired part can be returned and reinstalled into an aircraft.

According to its repair station certificate, WECO was permitted to repair, among other items, rotables and converters. Rotables are generally parts that convert a mechanical drive into electrical output such as generators, alternators, and rotary and linear actuators. Converters are components that supply electrical power to the systems on an aircraft that need it. In repairing either of these types of parts, a certified repair station is required to use FAA-approved parts. According to the indictment, the defendants regularly directed WECO technicians to use unapproved parts in repairs. On one occasion, Maupin and MacQueen allegedly

used a paper clip instead of an approved part to complete a repair, and then returned that part to the customer after certifying that the repair had been done properly.

In addition, during the repair of an aircraft part, a certified- repair station is required to comply with the manufacturer's Component Maintenance Manual (CMM), a step-by-step guide for conducting a proper repair of the part that is prepared by the manufacturer and approved by the FAA. The CMM contains the steps that a repair shop must take to fix a part, as well as the tests and inspections that must be done before the part can be returned to service. The indictment alleges that the defendants regularly failed to follow the manufacturer's CMMs. Indeed, as alleged in the indictment, the defendants did not even have the equipment needed to perform many of the tests required by the CMMs. According to the indictment, the defendants nonetheless performed repairs or directed WECO technicians to perform repairs of parts and returned those parts to customers, falsely certifying for each one that the part had been repaired in accordance with FAA regulations.

There have been no known instances in which a fraudulent WECO repair resulted in an aircraft accident. Upon learning of the allegations, the FAA issued an emergency order suspending WECO's repair station certificate. In addition, since finalizing its purchase of WECO in 2008, Gulfstream has fully cooperated with law enforcement in the investigation and prosecution of this case. The conduct alleged in the indictment occurred prior to Gulfstream's acquisition of WECO, and none of the defendants is currently employed at WECO.

"The indictment alleges that these defendants knowingly cut corners in repairing aircraft parts and concealed the fact that they were not complying with FAA regulations. While it is fortunate that there are no aircraft crashes known to be associated with faulty repairs conducted by these defendants, their alleged conduct needlessly took risks with the safety of persons who used aircraft that they repaired," said U.S. Attorney Wagner. "FAA regulations are intended to ensure the safety of air travel, and those who disregard them in order to increase profits should face serious consequences."

"The indictment handed down today reflects the strong commitment of the Department of Transportation (DOT) and its Office of Inspector General to ensuring the safety of the nation's air transportation system," said Hank W. Smedley, DOT OIG Special Agent-in-Charge. "Working with the Federal Aviation Administration and our law enforcement and prosecutorial colleagues, we will

continue to vigorously pursue those who violate criminal laws, defraud the government, and undercut the integrity of our safety programs."

Herb Brown, Special Agent in Charge of the Sacramento FBI, said: "It is appalling that these defendants would put financial gain and reward ahead of the safety and well-being of the many people who could have fallen in harm's way as a result of these fraudulently repaired airplane parts. Everyone that boards or operates an aircraft, as well as the communities that aircraft fly over, should have peace of mind that all safety regulations and guidelines have been followed. The FBI will continue to work with our partners to ensure that aircraft parts companies are properly supplying approved aircraft parts for the safety of all."

This case is the product of an extensive investigation by the Inspector General for the Department of Transportation and the Federal Bureau of Investigation, along with the Inspectors General of the Department of Homeland Security, and Department of Defense. Assistant United States Attorney Kyle Reardon is prosecuting the case. Former Eastern District of California Assistant United States Attorneys Laura Ferris and Sean Flynn also handled aspects of the prosecution.

If convicted, the defendants face a maximum statutory penalty for the conspiracy to commit fraud and fraud involving aircraft parts in interstate commerce of 15 years in prison, a fine of $500,000, and three years of supervised release. The maximum statutory penalty for each count of mail fraud is 20 years in prison, a fine of $250,000, and a three-year term of supervised release. The actual sentence, however, will be determined at the discretion of the court after consideration of any applicable statutory factors and the Federal Sentencing Guidelines, which take into account a number of variables.

The charges are only allegations and the defendants are presumed innocent until and unless proven guilty beyond a reasonable doubt.

Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems

http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems

FBI Los Angeles

September 22, 2011

Public Affairs Specialist Laura Eimiller

(310) 996-3343

— filed under: Cyber Crimes, Press Release

LOS ANGELES—A member of the LulzSec hacking group was arrested this morning for his role in an extensive computer attack against the computer systems of Sony Pictures Entertainment, announced André Birotte Jr., the United States Attorney in Los Angeles; and Steven Martinez, Assistant Director in Charge of the FBI's Los Angeles Field Office.

Cody Kretsinger, 23, of Phoenix, Arizona, was arrested this morning by FBI agents without incident. On September 2, 2011, a federal grand jury returned an indictment filed under seal in U.S. District Court in Los Angeles charging Kretsinger with conspiracy and the unauthorized impairment of a protected computer. The federal indictment was unsealed this morning upon Kretsinger's arrest.

From approximately May 27, 2011, through June 2, 2011, the computer systems of Sony Pictures Entertainment were compromised by a group known as "LulzSec," or "Lulz Security," whose members anonymously claimed responsibility on LulzSec's website. Kretsinger, also known by the moniker "recursion," is believed to be a current or former member of LulzSec. The extent of damage caused by the compromise at Sony Pictures is under investigation.

According to the indictment, Kretsinger resided in Tempe, Arizona at the time the alleged criminal activity took place. In order to carry out the attack, Kretsinger allegedly used a proxy server in an attempt to mask or hide his Internet Protocol (IP) address. The indictment alleges that Kretsinger and other coconspirators obtained confidential information from Sony Pictures' computer systems using an "SQL injection" attack against its website, a technique commonly used by hackers to exploit vulnerabilities and steal information.

The indictment alleges that Kretsinger and his co-conspirators distributed the stolen information, including by posting the information on LulzSec's website, and then announced the attack via its Twitter account. The indictment further alleges that, in order to avoid detection by law enforcement, Kretsinger permanently erased the hard drive of the computer he used to conduct the attack on Sony Pictures.

LulzSec is known for its affiliation with the international group of hackers known as "Anonymous." Anonymous, according to the indictment, is a collective of computer hackers and other individuals located throughout the world that conduct cyber attacks, including the dissemination of confidential information stolen from victims' computers, against individuals and entities they perceive to be hostile to its interests.

In the recent past, LulzSec has been linked to the hacking or attempted hacking of numerous targets, including various websites that represent governmental or business entities, among others.

Kretsinger will make an initial appearance before a federal magistrate in U.S. District Court in Phoenix today. The government will request that Kretsinger be removed to Los Angeles, the district in which he was charged, to face prosecution. If convicted, Kretsinger faces a statutory maximum sentence of 15 years in prison. This investigation was conducted by the Electronic Crimes Task Force (ECTF) in Los Angeles. The ECTF is comprised of agents and officers from the FBI, United States Secret Service, Los Angeles Police Department, Los Angeles County Sheriff's Department, United States Attorney's Office, Los Angeles County District Attorney's Office, and the California Highway Patrol.

This case is being prosecuted by the United States Attorney's Office in Los Angeles.

An indictment merely contains allegations that a defendant has committed a crime. Every defendant is presumed innocent unless and until proven guilty at trial.

TECHNIQUES, METHODS, TARGETS

Charges against the subjects included smuggling real and phony drugs and other contraband into the U.S. along with counterfeit $100 bills.

Operation Smoking Dragon
Dismantling an International Smuggling Ring

http://www.fbi.gov/news/stories/2011/july/dragon_070511/dragon_070511

Operation Smoking Dragon
Dismantling an International Smuggling Ring

07/05/11

The judge who recently sentenced Yi Qing Chen noted that the smuggler "never saw a criminal scheme he didn't want a part of." The Southern California man was convicted last October of distributing methamphetamine, trafficking approximately 800,000 cases of counterfeit cigarettes, and conspiracy to import Chinese-made shoulder-fired missiles into the U.S.

Chen is now serving a 25-year prison sentence, and his case marks the end of a long-running investigation called Operation Smoking Dragon.

The Royal Charm and Smoking Dragon investigations were led by the FBI, but we had substantial assistance from partners including the Bureau of Alcohol, Tobacco, Firearms, and Explosives; U.S. Immigration and Customs Enforcement; and the U.S. Secret Service.

Smoking Dragon and a related case in New Jersey called Operation Royal Charm led to the indictment of 87 individuals from China, Taiwan, Canada, and the U.S.

The investigations uncovered—and dismantled—an international smuggling ring that could have threatened the country's national security.

Charges against the subjects included smuggling real and phony drugs and other contraband into the U.S. along with counterfeit $100 bills—believed to have been produced in North Korea—that were so nearly perfect and so much more sophisticated than typical counterfeit currency they were dubbed "Supernotes."

The Wedding Ruse

To coordinate arrests in the Operation Royal Charm case, agents came up with a clever ruse. Because many of the subjects lived outside the U.S., they were invited to a wedding aboard a yacht docked near Atlantic City, New Jersey. They were sent real invitations, but the wedding was a fake. When several of the individuals showed up for "transportation" to the ceremony, they were promptly arrested.

"One of the most important things about Operation Smoking Dragon was that it demonstrated the broad range of international criminal activity conducted by today's Asian organized crime groups," said Special Agent Bud Spencer, who worked the case in our Los Angeles office.

The eight-year investigation began when FBI undercover agents, posing as underworld criminals, helped make sure that shipping containers full of counterfeit cigarettes made it past U.S. Customs officers undetected. Over time, as undercover agents won the smugglers' trust, they were asked to facilitate other illegal shipments such as narcotics and millions of dollars in Supernotes. Later, the smugglers offered a variety of Chinese military-grade weapons, including the QW-2 surface-to-air missiles.

Some of the drugs—including methamphetamine and fake Viagra—were hidden in large cardboard boxes with false bottoms that contained toys. The Supernotes were placed between the pages of books or lined in large bolts of rolled-up fabric. All of the items were smuggled into the U.S. in 40-foot shipping containers.

The smugglers offered a variety of Chinese military-grade weapons, including surface-to-air missiles.

Between Smoking Dragon and Royal Charm, some $4.5 million in counterfeit currency was seized, along with more than $40 million worth of counterfeit cigarettes, drugs, and other real and phony items. The smugglers were also forced to forfeit a total of $24 million in cash, along with real estate, cars, and jewelry.

Most of the defendants were indicted in 2005 and have since pled guilty or been convicted. Chen was the final defendant to be sentenced relating to Operation Smoking Dragon. His was the nation's first conviction under a 2004 anti-terrorism statute that outlaws the importation of missile systems designed to destroy aircraft.

"There is only one purpose for shoulder-fired missiles like the QW-2, and that is to bring down aircraft," said Special Agent Omar Trevino, who worked the case from the beginning. "Smoking Dragon dismantled an international smuggling ring, and it illustrated that organized crime groups will stop at nothing to make a profit."

Mark Aveis, an assistant United States attorney in Los Angeles who prosecuted the Chen case, agreed with Agent Trevino. "Chen and his associates didn't care what they smuggled as long as they made money," he said. "This case highlights the FBI's ability to carry out successful long-term undercover investigations—and the continuing need for such investigations."

Operation Smoking Dragon
Part II: An Undercover Agent Tells His Story

07/18/11

Operation Smoking Dragon and a related case led to the indictment of 87 individuals and dismantled an international smuggling ring that brought illegal drugs, cigarettes, and counterfeit currency into the country—and conspired to bring in Chinese-made weapons as well.

Retired Special Agent Bob Hamer worked undercover on Operation Smoking Dragon and was instrumental in the investigation's success. During his 26-year career with the Bureau, Hamer specialized in covert work, posing as a drug dealer, screenwriter, friend of the Mafia, even a pedophile. Below, he talks about Operation Smoking Dragon and his work undercover.

Q: How did you get involved with Smoking Dragon?

Mr. Hamer: The case agent was looking for an undercover agent to help target an Asian organized crime group, and he contacted me. I met with the agent and his informant. The informant liked me and set up a meeting with the person we believed was the largest importer of counterfeit cigarettes on the West Coast. And that was it. I was in.

Q: How did you convince the target that you could be trusted?

Mr. Hamer: My story was that I had inherited my grandfather's trust and that I was a savvy investor. More importantly, I had a warehouse where they could store the cigarettes, and I had access to long-haul truck drivers and some contacts at the port that might be able to help them get their shipping containers into the country. The bad guys bought it.

Q: How was Smoking Dragon different from other undercover cases you worked?

Mr. Hamer: Most of my undercover assignments were pretty straightforward investigations, from point A to point B. Smoking Dragon was one of those cases that started at A and went all over the alphabet. We assumed it was just going to be about cigarettes. We never thought it would expand to surface-to-air missiles or counterfeit currency—the Supernotes. We didn't think drugs would be involved or other counterfeit goods.

Q: You started on the case in 2002 and worked it until indictments were handed down in 2005. Was this the longest undercover assignment you had?

Mr. Hamer: Yes. I was undercover on Smoking Dragon for almost three years. As the case progressed beyond the initial target, I was dealing with one target or another almost on a daily basis. I think we added it up once that I had over 1,000 separate conversations during those three years with all the various targets. It was a full-time assignment, although I was working two other undercover operations at the same time.

Q: Why was this case so important?

Mr. Hamer: I considered one of the targets to be the most dangerous man in America. Whatever we wanted, whatever we brought up, he was capable of getting. He brought us the weapons deal, the Supernotes deal. He was doing cigarettes, Ecstasy. He was talking about setting up a crystal meth lab. This guy could put you together with anybody to make any deal. He said he could get us any weapons—anything but nuclear weapons—and I think he could have. Whatever China had, this guy was capable of getting. To me he was dangerous, not in the sense that he could kill you with his bare hands, but because of his connections. He was a broker for everything.

Q: How did you get started doing undercover work?

Mr. Hamer: I reported to my first FBI office in San Diego in September 1979, and within six months I assumed my first undercover role. I always thought it would be exciting to be part of an undercover investigation. We were doing an organized crime case, and I volunteered to go undercover. An informant

introduced me to his colleague who would become our target. That very first meeting my knees were shaking so much—not from fear but from adrenaline—I prayed nobody would notice. I met the target, and we hit it off. I came away with an adrenaline high that lasted for the rest of my career. I loved the work and did 20 separate undercover assignments in all, some of which lasted a day or two and some that ran for years.

Q: What does it take to be good at undercover work?

Mr. Hamer: You have to build a story that you believe and that you can sell. You have to love the work and believe in yourself. You've got to be quick on your feet, but you can't dominate the conversation. You have to know who you are both in the real world and the undercover world, because you are on a high wire without a net. In Hollywood you get a chance to say your lines again if you make a mistake. There are no retakes in the real world. If you make a mistake on the street, you might blow the case or risk getting yourself killed.

Q: Do you develop an emotional connection to the people you are investigating?

Mr. Hamer: That's an issue, but it comes back to knowing who the real you is. You have to be one of the bad guys without becoming one of them. There is a line you can't cross. You have to walk up to that line, but you can't go over it.

Q: You retired at age 56, one year after the Smoking Dragon indictments were announced and one year before agents are required to retire. Do you miss the undercover life?

Mr. Hamer: Smoking Dragon was one of the biggest cases I worked. With only one year to go before mandatory retirement, I didn't think I could top Smoking Dragon, so I retired. I do miss the work. I miss the adrenaline rush of being undercover, but not to the point that I would go work for some private detective agency. If the FBI called me back, yeah, I would love it. I had 26 great years in the FBI.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Responding to the Cyber Threat

http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat

Shawn Henry

Executive Assistant Director

Federal Bureau of Investigation

Information Systems Security Association International Conference

Baltimore, Maryland

October 20, 2011

Good afternoon. I appreciate the opportunity to be here with you today to discuss the cyber threat, the challenges it presents, and some alternative ideas for mitigating it.

The Cyber Threat

Some of the most critical threats facing our nation today emanate from the cyber realm. We've got hackers out to take our personal information and money, spies who want to steal our nation's secrets and terrorists who are looking for novel ways to attack our critical infrastructure.

President Obama called the cyber threat one of the most serious economic and national security challenges we face as a nation.

I believe the cyber threat is an existential one, meaning that a major cyber attack could potentially wipe out whole companies. It could shut down our electric grid or water supply. It could cause serious damage to parts of our cities, and ultimately even kill people.

While it may sound alarmist, the threat is incredibly real, and intrusions into corporate networks, personal computers, and government systems are occurring every single day by the thousands.

We see three primary actors in the cyber world: foreign intelligence services, terrorist groups, and organized crime enterprises. Dozens of countries have offensive cyber capabilities, and their foreign intelligence services are generally the most capable of our cyber adversaries.

Their victims run the gamut from other government networks to cleared defense contractors to private companies from which they seek to steal secrets or gain competitive advantage for their nation's companies.

One company that was recently the victim of an intrusion determined it had lost 10 years worth of research and development—valued at $1 billion—virtually overnight.

Terrorist groups are interested in impacting this country through a digital attack the same way they've done historically through kinetic attack; they're always looking for creative ways to harm us. Some say they currently don't have the capability to do it themselves. But the reality is that capability is available on the open market. And as 9/11 taught us, we can't assume that just because something hasn't been done before, it isn't a possible threat.

Organized crime groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to the computer network. Rather than breaking into a bank with guns to crack the safe, they breach corporate networks and financial institutions to pilfer boatloads of data, including user credentials, personally identifiable information, and corporate secrets, which they can monetize.

These groups, often made up of individuals living in disparate places around the world, have stolen hundreds of millions of dollars from the financial services sector and its customers. Their crimes increase the cost of doing business, put companies at a competitive disadvantage, and create a significant drain on our economy.

The value of thefts via hacking the financial services sector or its customers far exceeds that of physical bank robberies many, many times over.

In one of the most sophisticated and organized attacks on the financial sector, an international network of hackers obtained access to a financial corporation's network and completely compromised its encryption. They were inside the system for months doing reconnaissance, which enabled them to steal millions of dollars in less than 24 hours when they finally took overt action.

Another major international hacking group used an Automated Clearing House (ACH) wire transfer system to access online commercial banking accounts and

distribute malicious software that led financial institutions to lose nearly $70 million.

These cases illustrate how the offense far outpaces the defense in the cyber realm. And, unfortunately, under the current Internet infrastructure, we haven't been able to "tech" our way out of it. It's very difficult to put a price tag on all this in the aggregate, but several consultancies have actually tried to quantify it.

The 2011 Norton Cybercrime Report put the global cost of cyber crime at nearly $400 billion a year, and found that there are more than one million victims of cyber crime every day.

And a study released in August by the Ponemon Institute found that the number of attacks on companies it surveyed this year were up 45 percent from last year and cost 70 percent more to fix. On average, each attack took 18 days and $416,000 to fix.

And that's only the tip of the iceberg, because what I've referred to so far relates to remote access attacks. The reality is our adversaries use multiple attack vectors, including the supply chain, trusted insiders, and proximity attacks to target the network and its very valuable data.

Mitigating the Threat

So now that I've painted this grim picture, you're probably asking, "What are we doing about it and what more *should* we be doing?"

Despite the fact that our adversaries' capabilities are at an all-time high, the good news is we have made combating this challenge a top priority not only of the FBI, but the entire U.S. government. We are devoting significant resources to it. And our partnerships among government, industry, and academia have also led to a dramatic improvement in our ability to mitigate the threat.

For our part, the FBI has formed cyber squads in each of its 56 field offices, with more than 1,000 advanced cyber-trained FBI special agents, intelligence analysts, and forensic examiners. We have increased the capabilities of our employees by selectively seeking candidates with technical skills and enhancing our cyber training.

As an agency with both national security and law enforcement responsibility, the FBI is well-positioned to address the cyber threat. The anonymity of the Internet often creates challenges in determining exactly who the adversary is, but our

authorities and capabilities allow us to investigate and target criminal, foreign intelligence, and terrorist actors alike.

Partnerships

But we recognize that we can't do it alone. Through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), we coordinate our efforts and bring to bear the resources of 20 agencies.

The task force operates using Threat Focus Cells—small groups of agents, officers, and analysts from different agencies. They are subject-matter experts who are focused on very specific threats.

Through the NCIJTF, the FBI has collected real-time intelligence that has been incredibly valuable for the protection of our networks.

We've also forged tremendous relationships with the private sector, and through much more robust information sharing, we've prevented attacks *before* they've occurred. I can't tell you how many times we've gone to a company and told them they were breached, and where the intruder was on their network, and they were shocked to hear it.

And because there is often a foreign nexus to cyber crime, we are working closely with our international law enforcement partners. In fact, we've physically embedded FBI agents in foreign police agencies around the world to investigate cyber intrusion jointly, including in Estonia, the Netherlands, Romania, and Ukraine.

Each year, we are training and collaborating with approximately 500 foreign law enforcement officers from more than 40 nations in cyber investigative techniques.

Return on Investment

I'm pleased to say we're having success. In 2010, we arrested 202 criminals specifically for cyber intrusion—up from 159 in 2009. In addition, our foreign law enforcement partners made dozens and dozens of arrests last year based on intelligence we've shared with them. And we obtained a record level of financial judgments for those cases in excess of $100 million.

Those arrests included five of the world's top cyber criminals. Among them were the perpetrators of the financial services company intrusion I mentioned earlier, which resulted in one of the first hackers extradited from Estonia to the United States.

We also worked with our industry partners and our law enforcement counterparts in the Ukraine, the United Kingdom, the Netherlands, and elsewhere to apprehend those responsible for the ACH fraud scheme I talked about. Operation Trident Breach targeted more than 50 of the world's most prolific cyber and organized crime subjects. We and our international partners carried out arrests, interviews, searches, and evidence seizures in 24 cities in 12 countries.

We are also employing novel ways of combating the threat. In Operation Coreflood, the FBI worked with our private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software. The malware on this Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. In an unprecedented move, the FBI seized domain names, re-routed the botnet to FBI-controlled servers, and responded to commands sent from infected computers in the United States, telling the zombies to stop the Coreflood software from running. The success of this innovative operation will help pave the way for future cyber mitigation efforts and the development of new "outside the box" techniques.

Going forward, the U.S. government as a whole is collaborating to sharpen our focus on the cyber threat.

In May, the White House issued a proposed package of legislation aimed at enhancing the security of the nation's networks and infrastructure and increasing penalties for cyber crime. The administration also released its International Strategy for Cyberspace, which outlines the U.S. government's vision for the future of cyberspace and sets an agenda for partnering with other nations to realize it.

Managing the Risk

But is all this enough? Because if we have to get involved in a response capacity, something bad has already happened.

Before it was created, the Internet was something very few people could have imagined. To keep pace with our adversaries, we have to continue to think on that level to mitigate the cyber threat.

This is arguably the greatest invention of our lifetime, but it can be a dangerous place, as we've all seen. I believe it's key that we recognize the risk in the environment we're working in and learn to manage that risk.

That means we must divide our resources and efforts to reduce each of the factors that put us at risk.

To do so, it's important to understand the classic risk formula, which states, *'risk equals threat times vulnerability times consequence.'*

If we lower any of those three variable factors, we lower the risk. If we can completely eliminate any of those variables, we eliminate risk. But that's virtually impossible, so we must adopt a defense-in-depth approach—lowering each of the three.

This is where we have to work together—kind of like a zone defense.

Think of the risk model in terms of protecting your house from being robbed: If there are no burglars in your area, you've dropped the threat to zero. So you wouldn't need to spend money on a security system. And you might even leave your doors unlocked to save yourself time getting in and out.

Not because you don't have any valuables, but it doesn't matter how vulnerable you are because you don't have any threat actors.

If, all of a sudden, you get reports that there are burglars operating in your area, and people's homes are being broken into, then you begin worrying about vulnerabilities because you know there's a threat. You start locking the doors. You leave the outside lights on. Maybe you put in an alarm system. You might move certain valuables out of your house to a safety deposit box, or even install a safe.

Or you create a community watch to look out for the bad guys and protect not just your own property, but the whole neighborhood. Maybe you even move to a gated community with a 24/7 security guard that checks IDs at the gate. You've reduced your threats and vulnerabilities to counter the risk.

Consequence management, then, assumes that despite your best efforts to eliminate the threat and reduce your vulnerabilities, the bad guy still gets in.

So now you manage those consequences—you purchase homeowner's insurance to replace the valuables you may lose. Or you might put in a hidden camera to catch the thief in the act. That won't stop your valuables from being stolen, but might lead you to be able to recover them afterward.

Translating those concepts to the cybersecurity realm, we've already established that the threats exist and are increasing. So we could reduce the threat by taking a law enforcement, intelligence, or economic action to prevent or deter an adversary from acting. We took 202 threats off the playing field last year, but clearly, the threat continues.

So how do we lower the vulnerabilities of the cyber threat? It requires hardening the targets, including protecting the supply chain. It could entail keeping certain pieces of information off the network—maybe in a physical safe. Do you really need the 100-year old recipe for the secret sauce stored on the network?

Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system.

An example would be encrypting data so the hacker can't read it, or having redundant systems that can readily be reconstituted in the event of an attack.

In all cases, those who have addressed these individual risk factors have an opportunity to share information with others in order to lower our collective risk.

Alternate Models

I said earlier that under the current Internet structure, we can't tech our way out of the cyber threat. But what if the playing field were changed?

There is a growing sense among a number of subject-matter experts that the current Internet environment is simply not sustainable.

One proposal has been to begin exploring alternate, highly secure Internet options that focus on more easily spotting and tracking the threat actors. And then providing the law enforcement and intelligence communities and others the tools they need to mete out justice and deter future attacks.

Going back to the concept of alternatives, let's think of it in terms of the crime in the neighborhood analogy. Some people live in communities that have heightened security by focusing on who can enter at guarded posts—only certain people get in, and the rules to do so are stringent. They look for bad guys and report them to the police. These types of alternate security models can translate meaningfully to the Internet as well.

The reason the Internet is the way it is now is based on decisions made by those who developed it. They purposely allowed for anonymity, and there are legitimate reasons for wanting to keep it that way for some users and for some uses of the Internet. There are users for whom maintaining their privacy is worth the risk of intrusions into their computers or networks.

But for those critical uses of the Internet where intrusions are entirely unacceptable because the risk of compromise is so high, market-driven factors need to be explored; businesses must seek the solutions and options they want and need.

Electric power grid operators, for example, would likely opt for higher-trust models that don't foster anonymity, but instead promote assurance and attribution.

Assurance allows the ability to detect changes in data or hardware, and attribution provides the ability to determine who's on the network and who made any changes on it.

Right now, computer security has become an endless game of defense, which is both costly and unsurvivable in the long term if the status quo remains. Going after the threat actor is an absolutely necessary part of the risk equation, and one that can be made far more effective with alternate architectures.

Under the current environment, victims are often focused on how to get malware off their systems and on finding out what was taken. But what they should be asking is, 'What was left behind? And did it change my data?' Most users have no idea whether their software, hardware, or data integrity has been altered. Our current networks were never designed to detect that type of deviation.

So it's critical to note that attribution without assurance is useless. It doesn't do you any good to know who did it if you don't know what they did and how to look for it.

A key question in establishing alternate Internet models is how you prevent users of both platforms from contaminating the secure one.

As many of you know, we've seen cases in which removable media have introduced malware from unclassified government systems onto classified ones.

To avoid this in alternate security environments, it would be critical that the networks lack interoperability. Imagine if you will a virtual version of the pumps at gas stations that offer both diesel and regular gasoline. You can't even fit the diesel nozzle into a regular gas tank. It's idiot-proof. If you don't provide that kind of barrier on your new system, you would always be susceptible to human error. All users would need to adopt the same standards.

The trend toward cloud computing and new environments could present an opportunity to begin trying and testing new architectures.

U.S. innovation and ingenuity created the Internet, which is now a global phenomenon that has provided tremendous opportunities. With it, however, have come tremendous security challenges to certain users. For them, the current system will never be good enough. But it's too late to disconnect. It's not possible to be offline anymore, and there's currently no alternative.

I don't have the answers about how to build greater choices in the security architectures used today, but I do feel strongly that the discussions must begin now. I'll leave the solution to the potential customers, the technologists, and the entrepreneurs. I've outlined just a few of the issues that should be considered. But I challenge you to continue the discussion about whether there is a need and enough demand to develop alternate networked environments that rely less on playing defense, and rely more on discovering and capturing threat actors so they change their own risk calculus on whether cyber crime pays.

We must continue to push forward, because our adversaries are relentless. They want our money, our property, and our secrets, and some seek to harm us well beyond that. Together, we can turn the tide against them and bolster the security of our nation's information, networks, and infrastructure. Thank you.

How Much Do You Cost On the Black Market?

http://ncix.gov/issues/cyber/identity_theft.html

The information many Americans have come to view as sacred, private components of their personal and financial security is increasingly available to criminals and U.S. adversaries on the thriving underground black market. Criminals most commonly obtain personal information through cyber intrusions and technical compromise.

Below is the current price list* for obtaining specific elements of your personal information on the black market. Your social security number, at $3, is less expensive than a McDonalds Happy Meal. That's a decline for cyber criminals, as last year the average cost of obtaining a U.S. Social Security Number was $5.

Black Market Price List*

Name and Password for your online bank account $1000

Mag-stripe data from a "secure" premium-level credit card $80

Your Mother's Maiden Name $6

Your Social Security Number $3

* Prices reflect the latest sample quotes according to, RSA, a security firm. Black market prices were originally published in the June 2011 issue of Consumer Reports.

DHS Information Technology Sector Report

The following is a sample of what The Department of Homeland Security publishes each Monday through Friday on its public web site (see below link). Individuals with responsibilities involving computer network protection and cyber security might find this a useful site to check on a recurring basis.

http://www.dhs.gov/xlibrary/assets/DHS_Daily_Report_2011-10-31.pdf

October 28, V3.co.uk – (International) **Apple fixes security flaws in Windows version of QuickTime.** Apple is advising Windows users to update their systems following the release of a patch for the QuickTime media player tool. The company said in a security advisory that QuickTime 7.7.1 addresses 12 vulnerabilities in the Windows version of the platform, but does not affect Mac OS X users. Ten of the flaws could be targeted by way of a maliciously crafted PICT or FlashPix movie file to cause an application crash and allow remote code execution. The update also fixes a cross-site scripting flaw that could allow an attacker to insert code into an HTML file, and a vulnerability which could allow an attacker to view a user's memory contents by way of malformed movie file. Apple urged Windows users to install the 7.7.1 update, which can be obtained through the Apple Software Update utility or manually downloaded from the Apple support site. The update supports Windows versions from XP to Windows 7.

Source: http://www.v3.co.uk/v3-uk/news/2120703/apple-fixes-security-flaws-windows-version-quicktime

October 28, Help Net Security – (International) **Facebook spammers trick users into sharing anti-CSRF tokens.** Symantec researchers have spotted a new Facebook spamming technique they expect to be used a lot in the near future. Scammers make the victim's account post messages by executing a Cross-site Request Forgery (CSFR) attack after the victim has been tricked into sharing her anti-CSRF token generated by Facebook. Once they have the anti-CSRF token, the crooks can generate a valid CSRF token, which allows them to

re-use an already authenticated session to the Web site to post the offending message unbeknownst to the user. The attack begins with a typical message inviting users to see an "amazing video" or similar content. A click on the link takes the user to a fake YouTube page, and when he wants to see the video, a window pops up telling him he must pass the "YouTube Security Verification". When he clicks on the Generate Code link, a request is sent to 0.facebook.com/ajax/dtsg(dot)php, which returns JavaScript code containing the session's anti-CSRF token in a separate window. After the user has copied and pasted the generated code into the empty field and pressed the "Confirm" button, he has sent the code to the attacker who extracts the anti-CSRF token, creates a CSRF token and inserts his own piece of code that executes the CSRF attack and posts the malicious message and link on the user's Facebook Wall.

Source: http://www.net-security.org/secworld.php?id=11857

October 27, IDG News Service – (International) **Researcher finds major flaw in Facebook.** A security penetration tester discovered a major flaw in Facebook that could allow a person to send anyone on the social-networking site malicious applications. A senior security penetration tester at technology consultancy CDW, discovered the vulnerability and publicly disclosed it October 27 on his blog. The flaw was reported to Facebook September 30, which acknowledged the issue October 26, he wrote. The security tester wrote Facebook does not normally allow a person to send an executable attachment using the "Message" tab. If you try to do that, it returns the message "Error Uploading: You cannot attach files of that type." He wrote an analysis of the browser's "POST" request sent to Facebook's servers showed a variable called "filename" is parsed to see if a file should be allowed. But by modifying the POST request with a space just after the file name, an executable could be attached to the message. A person would not have to be an approved friend of the sender, as Facebook allows people to send messages to anyone. The danger is a hacker could use social engineering techniques to coax someone to launch the attachment, which could infect their computer with malware.

Source: http://www.computerworld.com/s/article/9221251/Researcher_finds_major_flaw_in_Facebook

October 27, Associated Press – (International) **Phishing scam masked as email from StubHub lands in inboxes; company warns customers to avoid.** An e-mail scam masked as an order confirmation from StubHub landed in countless mailboxes October 27, the Associated Press reported. The San

Francisco-based online ticket broker was deluged with phone calls within a few hours, said a spokesman. The company placed a warning notice on its home page advising recipients not to click on any link in the e-mail. The e-mail looks like a receipt for an order for two tickets to a boxing match in Las Vegas November 12. It appears to be sent by StubHub, and the charge is $2,766.95. The spokesman said no accounts have been charged. The e-mail apparently went to StubHub users and individuals who have never purchased tickets from the site. The fake e-mail seeks to dupe recipients into clicking on the embedded links to obtain sensitive information like credit card account numbers, and passwords. StubHub does not display credit card details on its site, but the spokesman said it is possible to order tickets from an established account with stored payment data. The fake StubHub e-mail appears to have originated in Eastern Europe, the spokesman said.

Source: http://www.washingtonpost.com/business/technology/phishing-scam-masked-as-email-from-stubhub-lands-in-inboxes-company-warns-customers-to-avoid/2011/10/27/gIQACa69MM_story.html

NOVEMBER IN COUNTERINTELLIGENCE HISTORY

- November, 1939: The FBI and Royal Canadian Mounted Police began a regular exchange of counterintelligence information.
- November, 1940: The FBI began distribution of a Quarterly Intelligence Summary for use by the State Department, Military Intelligence Directorate and the Office of Naval Intelligence. Subsequently, a Monthly General Intelligence Survey of Activities in the United States was prepared and distributed to the White House, cabinet, and all intelligence agencies of the government.
- November 1st, 1996: FBI Agents arrested Vladimir Galkin at JFK International Airport, NY, while he was accompanying an official delegation. Russia protested, claiming the U.S. was violating the "usual practice" of allowing visas for former intelligence staff that had left the active intelligence service. They called his arrest a dirty trick. Unbeknownst to the Russians was the fact that a secret criminal complaint in Boston, unsealed by the DOJ on 11/5/96, charged Galkin with attempting to gather material on U.S. antiballistic missile technology, repeatedly trying to obtain reports about classified technology conferences on the proposed missile defense system known as Star Wars.
- November 6th, 1953: Attorney General Brownell reported President Truman had appointed Harry Dexter White as Director of the International

Monetary Fund, despite having received FBI reports suggesting White's ties to Soviet intelligence.

- November 7th, 1919: The Bureau of Intelligence, working with Immigration Department personnel arrested approximately 300 members of the Union of Russian Workers, a group advocating the overthrow of the U.S. Government. On 12/21/1919, 240 Aliens, including 199 Union of Russian Workers members were deported to Russia, shipped aboard the USS Buford.
- November 16th, 1996: CIA Branch Chief Harold J. Nicholsen was arrested at Dulles International Airport. He was en route to a shuttle flight to New York that would have taken him to Switzerland, where he was to meet with his Russian contacts and pass more classified information. His scheme, lasting at least two years, netted him an estimated $120,000.
- November 21st, 1985: Navy Analyst Jonathan J. Pollard was arrested for spying for Israel. His wife, Anne Henderson-Pollard, was arrested on 11/23/1985. Pollard plead guilty to conspiring to receive embezzled government property; his wife pled to being an accessory. A Federal Grand Jury indicted Israeli General Aviem Sella on charges of recruiting Pollard as a spy and receiving U.S. Defense secrets.
- November 23rd, 1985: Former CIA Analyst Larry Wu Tai Chin was arrested on charges of spying for the People's Republic of China. He committed suicide two weeks after being convicted on 2/7/1986.
- November 25th, 1985: former National security Agency employee William Pelton was charged with spying. He was sentenced to life on 12/16/1986 for selling military secrets to Russia.

PRESENTATIONS AND OUTREACH

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

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

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

The United States is a world's leader in innovation. Consider the breakthrough

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

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

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

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC. You may also be interested in scheduling a presentation of the FBI video "BETRAYED" followed by Q&A.

"Betrayed" represents a scenario where an FBI Intelligence Analyst is slowly but steadly compromised by a series of steps that ultimately fully compromise him into working on behalf of a foreign intelligence service. The video clearly demonstrates the traits and activities demonstrated by individuals who are involved in stealing classified information (or even proprietary information and

trade secrets). The video also shows the passivity of co-workers who have clearly seen demonstrations of suspicious activity by the Intelligence Analyst, and how their failure to report the suspicious activity exasperates the situation.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

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

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000