Van Nuys
Los Angeles World Airports

AIRPORT ADVISORY NOTICE

Notice #2016-27

Dear VNY Stakeholders,

Thank you for attending the VNY Safety & Security Stand-Down session held on February 29, 2016. At the request of those who attended, and for the benefit of those who did not, please find attached a summary of information that was presented by Jeff Price of Leading Edge Strategies whose specialty is safety and security of airports. Also enclosed are the following four brochures on security from the U.S. Department of Justice:

Potential Indicators of Terrorist Activities Related to General Aviation Airports

Visitors: Risks & Mitigations

Elicitation

The Insider Threat

Please know that we are ready to assist you with any information you need on VNY's MVOP, ASMP, and VSAFE programs which were also part of the Stand-Down presentation.

Remember, "bottom line DO NOT cross the RED line". Please use the following link http://www.lawa.org/welcome_VNY.aspx?id=13386 to access the Van Nuys Red-Line Safety video that can be used to educate your employees and visitors on the importance of remaining behind the red lines of your leasehold boundaries.

We thank you for making safety and security the #1 priority at Van Nuys Airport.

The Van Nuys Airport Operations Team

VNY Airport Safety and Security Stand Down

Runway Incursion Prevention

Runway incursion is defined as "any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle or person on the protected area of the surface designated for the landing and takeoff of aircraft"

Surface incident is defined as "the unauthorized or unapproved movement within the designated movement area, or an occurrence in that same area associated with the operation of an aircraft that affects or could affect the safety of flight"

Vehicle or Pedestrian Deviation (V/PD) – is defined as any entry or movement on the airport movement area or safety area by a vehicle operator or pedestrian that has not been authorized by air traffic control (includes surface incidents involving aircraft operated by non-pilots, such as anyone).

What do you get when you have a safe operating environment?

Runway safety is everybody's problem. Everyone has something to lose if the problem isn't solved including: loss of life, loss of property, client lawsuits, insurance premium hikes, loss of federal funding, loss of clients (through bad publicity), and loss of community support. **What do you have to lose?**

Everyone has something to gain by problem solving. Both the airports and tenants get: protection of life, protection of millions in assets, lower insurance premiums, federal grant money, lower legal costs, attract more clients and community support and publicity.

"Let's be careful out there."

Realize that this is an ongoing issue that must be managed.
Instill a culture of safety
Be a part of any airport or FAA initiatives to improve runway safety.
Send decision makers, not note takers, to airport safety and security meetings.

Van Nuys Airport Safety and Security Stand Down

Principles and Practices in Business Aircraft and Facility Security

Are you doing what you should be doing?

- NBAA Security Guidance Flight School security guidance and regulations TSA's General Aviation Airport Security Guidance Security plan for your facility
- Encourage AOPA Watch, signs and training for personnel

Facility Protection

- Security force (unarmed or personal protection)
- Window security and structural reinforcement
- Escort vehicles on and off the ramp
- Conduct security training and have a security information program
- Post emergency numbers around facility, conduct drills
- Fencing, lighting, CCTV cameras
- Security champion
- Facility Security Plan
- Suspicious awareness training for personnel
- Security patrol training for personnel
- Access control and credentialing for ramp
- Vehicle and personnel escorts ramp-side
- Secure all doors including hangar doors, and gates
- Accompany all visitors, challenge those are out of place
- Pilot sign in / sign our procedures
- Confirm identity of passengers / personnel on the ramp
- Secure all key storage areas (fuel, chemicals)

8 Signs of Terrorism

1. Surveillance
2. Elicitation
3. Tests of Security
1. Funding
2. Supplies
3. Impersonation
4. Rehearsal
5. Deployment

http://dhsem.state.co.us/prevention-security/citizen-resources/eight-signs-terrorism

Ultimately, it's about building a Culture of Security

Conduct your own security risk assessment at your facility, identify and mitigate hazards

- Engage Airport Management in your solutions; create a safety and a security plan
- Identify a security champion / manager within your organization; he or she should have something to say at every staff meeting, is responsible for coordinating with sub lessees, or clients, and sign's off on routine and special activities
- Ensure all upcoming unusual activities (construction, VIP visits, events) are communicated to Airport Operations
- Low tolerance for violations as the behavior you tolerate is what you will get
- Blogs, email signature lines, posters, and internal publicity campaigns that focus on security awareness and prevention of criminal activities
- Continual "coffee shop" and bi-annual formalized contingency plan training
- Reward system for identifying and reporting or preventing security situations

Bureau of Justice Assistance
U.S. Department of Justice

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to General Aviation Airports

What Should I Consider Suspicious?

- Individuals who are taking flying lessons or ask about lessons and are uninterested in learning all that is necessary to pilot an aircraft safely.
- Attempts to obtain flying lessons or rent or charter a plane without proper identification.
- Inquiries about renting or chartering an aircraft for questionable or vague reasons.
- Requests to be flown through restricted airspace.
- Requests to be flown over specific potentially sensitive locations (e.g., schools, dams, bridges) for unsubstantiated reasons.
- Individuals on chartered flights who take pictures or videos of potentially sensitive locations.
- Individuals who appear more interested in photographing/documenting airport security procedures and safeguards than airplanes.
- Inquiries about buying aviation fuel in containers as opposed to dispensing it into an airplane.
- Attempts to load fuel or propane into a passenger compartment of an aircraft.
- Evidence of attempted breaches of airport perimeter security (e.g., holes in fences).
- Individuals whose actions/behaviors are outside the norm and raise your suspicions based on your experience.
- Vehicles parked near an airport perimeter fence, especially for extended periods.
- Attempts to leave or enter airport buildings through emergency exits, employee doors, or other outlets not designed for public access.
- Airport employees who are found in areas that are not permitted by their airport credentials.
- Requests for information about airport security procedures, staffing, or equipment.
- Persons requesting ramp security access codes.
- Individuals who ask about crop dusting planes and are unable to provide a satisfactory reason for the inquiry.
- Non-U.S. citizens applying for flight training with an expired M-1 vocational visa or without the required M-1 vocational visa.

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different, it does not mean that he or she is suspicious.

What Should I Do?

Be part of the solution.

- If something seems wrong, notify law enforcement authorities.
- Report suspicious activity to the General Aviation Hotline (866) GA-SECURE or (866) 427-3287.
- Establish a contact (e.g., airport manager) at the airport for easy reporting of suspicious activities.
- Restrict entry to specific airport facilities.
- Ensure that all flight school employees complete required Flight School Security Awareness (FSSA) training every year.
- Educate airport personnel about indicators of terrorist activities.
- Work with local law enforcement to ensure that the airport perimeter is patrolled.
- Install security cameras at all entrances and exits to airport buildings.
- Make note of suspicious statements, people, and/or vehicles.

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.

This project was supported by Grant No. 2008-DD-BX-0393 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

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. www.fbi.gov

***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.*

U.S. Department of Justice
Federal Bureau of Investigation

VISITORS: RISKS & MITIGATIONS

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.

- Educate employees extensively on the scope of the project and how to report security concerns

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.

- 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

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.

- 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

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

- 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

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.

- 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

Opposition / Feigned Incredulity: *Indicate disbelief or opposition in order to prompt a person to offer information in defense of their position.* "There's no way you could design and produce this that fast!" "That's good in theory, but…"

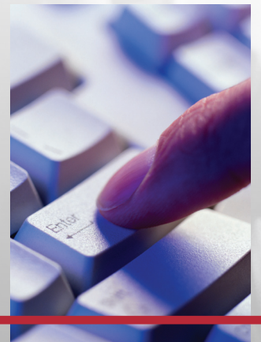
Provocative Statement: *Entice the person to direct a question toward you, in order to set up the rest of the conversation.* "I could kick myself for not taking that job offer." *Response*: "Why didn't you?" Since the other person is asking the question, it makes your part in the subsequent conversation more innocuous.

Questionnaires and Surveys: *State a benign purpose for the survey. Surround a few questions you want answered with other logical questions. Or use a survey merely to get people to agree to talk with you.*

Quote Reported Facts: *Reference real or false information so the person believes that bit of information is in the public domain.* "Will you comment on reports that your company is laying off employees?" "Did you read how analysts predict…"

Ruse Interviews: *Someone pretending to be a headhunter calls and asks about your experience, qualifications, and recent projects.*

Target the Outsider: *Ask about an organization that the person does not belong to.* Often friends, family, vendors, subsidiaries, or competitors know information but may not be sensitized about what not to share.



COLLECTING INFORMATION

Volunteering Information / Quid Pro Quo: *Give information in hopes that the person will reciprocate.* "Our company's infrared sensors are only accurate 80% of the time at that distance. Are yours any better?"

Word Repetition: *Repeat core words or concepts to encourage a person to expand on what he/she already said.* "3,000 meter range, huh? Interesting."

DEFLECTING ELICITATION ATTEMPTS

Know what information should not be shared, and be suspicious of people who seek such information. Do not tell people any information they are not authorized to know, to include personal information about you, your family, or your colleagues.

You can politely discourage conversation topics and deflect possible elicitations by:

- Referring them to public sources (websites, press releases)
- Ignoring any question or statement you think is improper and changing the topic
- Deflecting a question with one of your own
- Responding with "Why do you ask?"
- Giving a nondescript answer
- Stating that you do not know
- Stating that you would have to clear such discussions with your security office
- Stating that you cannot discuss the matter

If you believe someone has tried to elicit information from you, especially about your work, report it to your security officer.

For additional information or training, contact the FBI. www.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation

This brochure is an introduction to elicitation and elicitation techniques. Understanding the techniques and the threat may help you detect and deflect elicitation attempts.

ELICITATION

Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, or in writing.

Conducted by a skilled collector, elicitation will appear to be normal social or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information.

Many competitive business intelligence collectors and foreign intelligence officers are trained in elicitation tactics. Their job is to obtain non-public information. A business competitor may want information in order to out-compete your company, or a foreign intelligence officer may want insider information or details on US defense technologies.

ELICITATION DEFINED

The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated.

Elicitation attempts can be simple, and sometimes are obvious. If they are obvious, it is easier to detect and deflect. On the other hand, elicitation may be imaginative, persistent, involve extensive planning, and may employ a co-conspirator. Elicitors may use a cover story to account for the conversation topic and why they ask certain questions.

Elicitors may collect information about you or your colleagues that could facilitate future targeting attempts.

Elicitation can occur anywhere— at social gatherings, at conferences, over the phone, on the street, on the Internet, or in someone's home.

ELICITATION IS NOT RARE

It is not uncommon for people to discover information about a person without letting on the purpose. For example, have you ever planned a surprise party for someone and needed to know their schedule, wish list, food likes and dislikes or other information without that person finding out you were collecting the information or for what purpose? The problem comes when a skilled elicitor is able to obtain valuable information from you, which you did not intend to share, because you did not recognize and divert the elicitation.

STRATEGIC CONVERSATION

WHY ELICITATION WORKS

A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit those. Natural tendencies an elicitor may try to exploit include:

- A desire to be polite and helpful, even to strangers or new acquaintances
- A desire to appear well informed, especially about our profession
- A desire to feel appreciated and believe we are contributing to something important
- A tendency to expand on a topic when given praise or encouragement; to show off
- A tendency to gossip
- A tendency to correct others
- A tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used
- A tendency to believe others are honest; a disinclination to be suspicious of others
- A tendency to answer truthfully when asked an "honest" question
- A desire to convert someone to our opinion

For example, you meet someone at a public function and the natural getting-to-know-you questions eventually turn to your work. You never mention the name of your organization. The new person asks questions about job satisfaction at your company, perhaps while complaining about his job. You may think, "He has no idea where I work or what I really do. He's just making idle chat. There's no harm in answering." However, he may know exactly what you do but he relies on his anonymity, your desire to be honest and appear knowledgeable, and your disinclination to be suspicious to get the information he wants. He may be hunting for a disgruntled employee who he can entice to give him insider information.

TECHNIQUES

There are many elicitation techniques, and multiple techniques may be used in an elicitation attempt. The following are descriptions of some of those techniques.

Assumed Knowledge: *Pretend to have knowledge or associations in common with a person.* "According to the computer network guys I used to work with…"

Bracketing: *Provide a high and low estimate in order to entice a more specific number.* "I assume rates will have to go up soon. I'd guess between five and 15 dollars." *Response:* "Probably around seven dollars."

Can you top this? *Tell an extreme story in hopes the person will want to top it.* "I heard Company M is developing an amazing new product that is capable of …"

Confidential Bait: *Pretend to divulge confidential information in hopes of receiving confidential information in return.* "Just between you and me…" "Off the record…"

Criticism: *Criticize an individual or organization in which the person has an interest in hopes the person will disclose information during a defense.* "How did your company get that contract? Everybody knows Company B has better engineers for that type of work."

Deliberate False Statements / Denial of the Obvious: *Say something wrong in the hopes that the person will correct your statement with true information.* "Everybody knows that process won't work—it's just a DARPA dream project that will never get off the ground."

TARGETING KNOWLEDGE

Feigned Ignorance: *Pretend to be ignorant of a topic in order to exploit the person's tendency to educate.* "I'm new to this field and could use all the help I can get." "How does this thing work?"

Flattery: *Use praise to coax a person into providing information.* "I bet you were the key person in designing this new product."

Good Listener: *Exploit the instinct to complain or brag, by listening patiently and validating the person's feelings (whether positive or negative).* If a person feels they have someone to confide in, he/she may share more information.

The Leading Question: *Ask a question to which the answer is "yes" or "no," but which contains at least one presumption.* "Did you work with integrated systems testing before you left that company?" (As opposed to: "What were your responsibilities at your prior job?")

Macro to Micro: *Start a conversation on the macro level, and then gradually guide the person toward the topic of actual interest.* Start talking about the economy, then government spending, then potential defense budget cuts, then "what will happen to your X program if there are budget cuts?" A good elicitor will then reverse the process taking the conversation back to macro topics.

Mutual Interest: *Suggest you are similar to a person based on shared interests, hobbies, or experiences, as a way to obtain information or build a rapport before soliciting information.* "Your brother served in the Iraq war? So did mine. Which unit was your brother with?"

Oblique Reference: *Discuss one topic that may provide insight into a different topic.* A question about the catering of a work party may actually be an attempt to understand the type of access outside vendors have to the facility.

RECENT INSIDER THEFT CASES

Wen Chyu Liu, a retired research scientist, was sentenced in January 2012 to 60 months in prison, two years supervised release, a $25,000 fine and was ordered to forfeit $600,000. Liu was convicted in February 2011 of stealing trade secrets from his former employer and selling them to companies in China. Liu conspired with at least four current and former employees, traveled throughout China to market the stolen information, paid current and former employees for material and information, and bribed a then-employee with $50,000 in cash to provide a process manual and other information.

Kexue Huang was employed by two different US companies. He admitted that from 2007 to 2010 he delivered stolen trade secrets from both companies to individuals in Germany and China. The stolen materials were used to conduct unauthorized research to benefit Chinese universities. Huang also pursued steps to develop and produce the trade secrets in China. The aggregated loss from both companies was between $7 and $20 million. Huang pleaded guilty to charges of economic espionage and theft of trade secrets, and was sentenced in December 2011 to 87 months in prison and three years supervised release.

Yuan Li, a former research chemist with a global pharmaceutical company, pleaded guilty in January 2012 to stealing her employer's trade secrets and making them available for sale through Abby Pharmatech, Inc. Li was a 50% partner in Abby. Between October 2008 and June 2011 Li accessed her employer's internal databases, downloaded information to her personal home computer, and made them for sale through Abby. She was sentenced to 18 months in prison.

Elliot Doxer sent an e-mail to the Israeli Consulate stating that he was willing to provide information from his employer that might help Israel. An undercover FBI agent posing as an Israeli intelligence officer spoke to Doxer and established a "dead drop" where the two could exchange information. For the next 18 months, Doxer visited the dead drop at least 62 times. Doxer provided customer and employee lists, contract information, and other trade secrets. He pleaded guilty to one count of foreign economic espionage and was sentenced in December 2011 to six months in prison, six months home confinement, and fined $25,000.

Sergey Aleynikov worked as a computer programmer for a Wall Street company. During his last few days at that company, he transferred 32 megabytes of proprietary computer codes -- a theft that could have cost his employer millions of dollars. He attempted to hide his activities but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets.

Michael Mitchell became disgruntled and was fired from his job due to poor performance. He kept numerous computer files with his employer's trade secrets; he entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets. In March 2010, he was sentenced to 18 months in prison and ordered to pay his former employer over $187,000.

Shalin Jhaveri gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and confirmed that the information he had taken from his employer was everything he needed to start the business. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $5,000 fine, and a $100 Special Assessment.

Hanjuan Jin took a leave of absence from her US employer in 2006. While on leave, Jin worked for a similar company in China. A year later, Jin returned to the United States. Within a week of her return, she bought a one-way ticket back to China, and advised her US employer that she was ready to end her leave. Jin returned to work on February 26, 2007 and for the next two days downloaded hundreds of technical documents. On February 28, 2007, during a routine check at the airport, more than 1,000 electronic and paper documents proprietary to her US employer were found in Jin's luggage. In 2012, Jin was sentenced to four years in prison and fined $20,000.

Greg Chung spied for China from 1979-2006. Chung stole trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He stole hundreds of thousands of documents from his employer. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents. He also used Mak (below) to transfer information back to China. In February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for over 20 years. He passed information on quiet electric propulsion systems for US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Mak was convicted of conspiracy, failing to register as an agent of a foreign government, and other violations. He was sentenced to over 24 years in prison.

Report theft of trade secrets to your local FBI office or submit a tip online: tips.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider–the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a "spy"–someone who is stealing company information or products in order to *benefit another organization or country.*

THE INSIDER THREAT

An introduction to detecting and deterring an insider spy

- Disgruntled
- Working odd hours
- Unexplained affluence
- Unreported foreign travel

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

PROTECT YOUR INTELLECTUAL PROPERTY

Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

PERSONAL FACTORS

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification: A desire to help the "underdog" or a particular cause.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/ Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

ORGANIZATIONAL FACTORS

Organizational situations may increase the ease for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.

Proprietary or classified information is not labeled as such, or is incorrectly labeled.

The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials.

Undefined policies regarding working from home on projects of a sensitive or proprietary nature.

The perception that security is lax and the consequences for theft are minimal or non-existent.

Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.

Employees are not trained on how to properly protect proprietary information.

BEHAVIORAL INDICATORS

Some behaviors may be a clue that an employee is spying and/ or methodically stealing from the organization:

Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.

Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.

Unnecessarily copies material, especially if it is proprietary or classified.

Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Short trips to foreign countries for unexplained or strange reasons.

Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Overwhelmed by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company's intellectual property, its reputation, its financial well-being, and its future. They are protecting their own jobs. Remind them that if they see something, to say something.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts–such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.