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.*

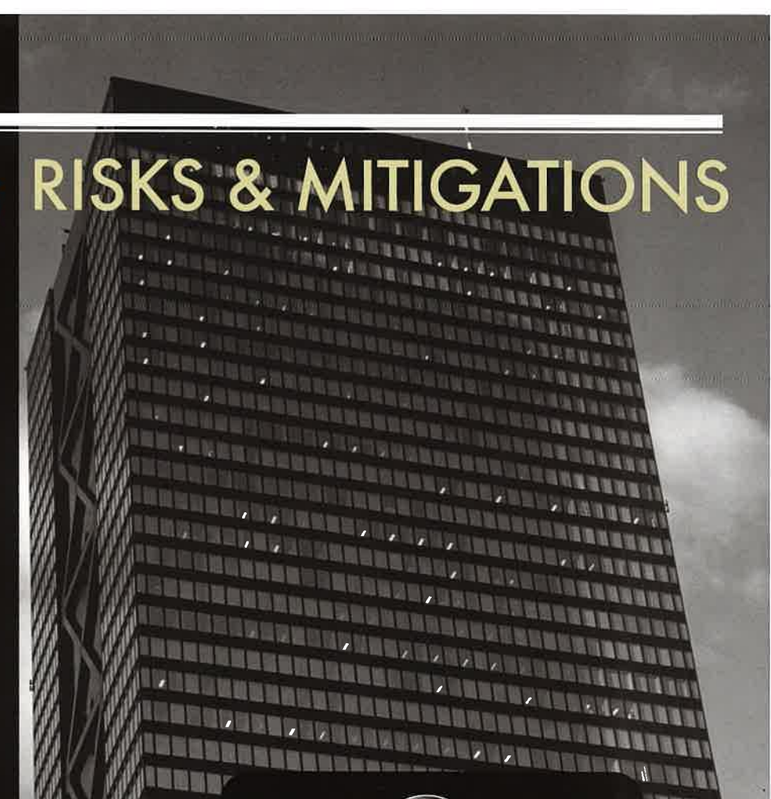
***Proprietary Information** = information that is not available to the public, has been developed by the holder, and is viewed as the property of the holder, but does not rise to the level of a trade secret.*

***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

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.

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
- 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