SUSPICIOUS CONTACT REPORTING
FOR CLEARED EMPLOYEES
PURPOSE

To become familiar with National Industrial Security Program (NISPOM) reporting requirements regarding Reporting Suspicious Contacts

Identify threats, technology targets, and collection methods to classified and unclassified government assets.

The only thing between our adversaries and classified/proprietary information is you and the diligent performance of YOUR SECURITY responsibilities.
PERSONNEL

Know your UA security officer:

Keith A. Corson
University of Arizona
Facility Security Officer
(520) 626-5865
kcorson@email.arizona.edu

Your sponsor’s cleared facility will also have a local security officer with information specific to that location
REPORTING REQUIREMENTS
Reporting Requirements (NISPOM Section 3) – 1-302 b: Suspicious Contacts:

“Cleared employees are required to report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. All contacts by cleared employees with known or suspected intelligence officers from any country or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country must be reported.”*

*DoD 5220.22-M, National Industrial Security Program Operating Manual (“NISPOM”)
• As a cleared employee, you are responsible to report incidents of Suspicious Contacts to the FSO of the University of Arizona.
• You are also required to follow the rules regarding suspicious contacts reports of your host site.
INTERNATIONAL TRAVEL

–International travel, either for business or pleasure, should be reported to the Facility Security Officer prior to making the trip. You will be provided with a foreign travel briefing as necessary.

–Upon your return, you must report any suspicious contacts that may have occurred during your travel. Suspicious contacts are discussed in the next section.
SUSPICIOUS CONTACTS
Examples of Suspicious Contacts:

• Efforts by an individual, regardless of nationality, to obtain unauthorized access to classified, proprietary, or export controlled information.

• Efforts by an individual to compromise a cleared employee.

• Any contact which suggests an attempted exploitation by the intelligence services of another country.

• Suspected or actual incidents of espionage, sabotage, or subversive activities against the University of Arizona or the United States.
More examples of Suspicious Contacts:

- Requests for protected information under the guise of a price quote, purchase request, or other pretense (this could come from both US citizens and foreign nationals).

- Foreign entities targeting cleared employees traveling overseas via detentions or intrusive screenings.

- Indications that hotel rooms, luggage, rental cars, etc. were searched.

- Attempts to entice cleared employees into situations that could lead to blackmail or extortion.

- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file.

- Attempts to place cleared personnel under obligation through special treatment, favors, gifts or money.
A suspicious contact may also occur if you are contacted by an unknown entity or individual with a request to:

- Lecture Overseas
- Host a foreign national visit
- Collaborate
- Provide information related to an export controlled or classified project.
IMPORTANCE OF REPORTING
Maintaining a compliant security program is vital to the University of Arizona. No one plays a greater role in security than each of you. The success of our program is based on the everyday security actions taken by cleared employees.

The partnership between cleared defense contractors and the Defense Security Service (DSS) has contributed to significant strides in the understanding of the collection threat directed against industry. The value of the Suspicious Contact Reports from Industry to DSS is of a very high level as they assist the DoD in understanding methods and targets of collectors. These reports are used to educate both Government and Industry on which DoD Technologies are targets of the foreign intelligence services.
TECHNOLOGY TARGETS
TOP 10 TECHNOLOGY TARGETS

- Electronics
- Command, Control, Communication, and Computers (C4) Systems
- Aeronautics
- Software
- Marine Systems
- Armament and Survivability
- Optics
- Materials: Raw and Processed
- Radars
- Energy Systems
Indicators of Being a Target

• **Be wary of:**
  - Technology request for classified or export controlled information
  - Request for information from foreign government or foreign government program
  - Requests disguised as ‘marketing surveys’
  - Inappropriate conduct during foreign visits
  - Strangers making intensive effort at forming friendships

• **Do not respond to a suspicious request**
  - Inform sponsor facility security office or Keith Corson, UA FSO (520) 626-5865, kcorson@email.arizona.edu
METHODS USED TO OBTAIN CLASSIFIED INFORMATION
COLLECTION METHODS IDENTIFIED BY DSS

• Requests for scientific and technological information
  This is the most frequently used method of collection. It includes any request not sought or encouraged by an organization, received from a known or unknown source, and concerns requests for classified, sensitive, export controlled or proprietary information.

• Solicitation and marketing of foreign services
  This method consists of foreign companies and research facilities offering their technical and business services to U.S. companies, research facilities and academic institutions. These foreign companies may also ask to represent the newly-developed products in their respective countries.

• Exploitation of visits to U.S. companies
  This method involves visits by non-U.S. persons or competitors to U.S. technology/research facilities and includes one-time visits, long-term visitors, government representative visits and student visits. Suspicious contact/conduct includes actions before, during and after the visits. The technique most often used is an attempt to discuss information outside the scope of the approved visit.
COLLECTION METHODS IDENTIFIED BY DSS (cont’d)

• **Targeting at conventions**
  Conventions and seminars are “target rich” environments for collection. Individuals attending these activities have the opportunity to study, compare and photograph actual products or research in one location.

• **Internet activity**
  This method deals with attempts to illegally obtain access to an organization’s network and subsequently its information.

• **Exploitation of joint venture/research projects, including international programs and cooperative agreements**
  • Activities include the foreign person attempting to access research areas and information outside the purview of the research agreement.
  • This could also include enticing U.S. researchers to provide large quantities of technical data as part of the bidding process.

• **Foreign targeting of U.S. travelers overseas**
  This method mainly targets defense contractors traveling abroad. Targeting activities are conducted on trains, planes and in airports. Information is collected using electronic surveillance equipment and entrapment ploys such as inducement of the target into a compromising situation which can lead to blackmail.
Academic Solicitation is the Single Most Common Form of Stealing U.S. Technology

“Seeking employment and academic solicitation remain at the top of methods of technical data collection, as foreign entities continue attempts to gain employment, internships, and research positions at cleared facilities, institutions associated with classified research, or institutions known for excellence in targeted technologies”*

COLLECTION METHODS: ACADEMIC SOLICITATION

Reasons academic solicitation is important to foreign entities:

• This is a shortcut to reduce investment in the necessary resources (time, money, effort) required to support development of emerging technologies.

• This can leverage the placement of smaller numbers of espionage agents (possibly students) to more quickly gain knowledge that allows foreign countries to advance R&D cycles by integrating basic capabilities into advanced military research projects.
EXAMPLE OF COLLECTION METHODS

Co-opting Former Employees/Colleagues

There have been several reports that highlight situations in which formerly cleared U.S. employees get hired by a foreign company or institute, and their work involves projects or technologies similar to those with their former U.S. employer.

The formerly cleared employees then collect classified technical information from unsuspecting former coworkers by inquiring about technological advances made since they left.

U.S. citizens working for foreign companies or institutes may also wittingly or unwittingly take advantage of their former U.S. coworkers by incorrectly convincing them that "unclassified" technical discussions are appropriate or authorized.
SUSPICIOUS EMAILS
Suspicious emails may appear to come from one foreign country but are actually originating from a different country. For example, the email may appear to be sent from Germany, when in fact, it was actually sent from China.

Suspicious emails may even come from a “front” company located in the United States.
Examples

An email comes directly from the foreign country or person that is soliciting the information, but is altered in order to disguise the actual end use or end user. The sender hopes the email will appear legitimate and the U.S. researcher will overlook the suspicious elements and reply to the email with the requested information.

Cleared UA employee/researcher receives an email request from an individual in a country such as China or Iran to study under or work with UA researcher. Researcher may also receive numerous requests from the same country or foreign institution which raises suspicions.
REPORTING: WHAT TO INCLUDE

When reporting a suspicious contact, include the following:

• A short paragraph describing why you think the contact is suspicious and include the nature of the information requested. For example, is this information export-controlled (ITAR/EAR), classified, or related to a classified program?

• Forward the entire suspicious email to the Facility Security Officer. The email will then be reported to DSS.

• If reporting an email, note whether an attachment or link was opened.
  • Did anyone else receive the same email?
  • Was the email forwarded within your organization or to someone else?

• Include the entire expanded headers. If you’re not sure how to acquire the expanded header from an email, save the email and contact your security representative.

  Remember, there are no wrong answers to the questions of what to include.
REPORTING: TO WHOM

Suspicious contact reports should be sent to:

Keith A. Corson
University of Arizona
Facility Security Officer
(520) 626-5865
kcorson@email.arizona.edu

or

The FSO or Security Office of your sponsor’s cleared facility
REPORTING: ALTERNATIVES

Defense Hotline

While contractor personnel are encouraged to furnish information through established company channels, the Defense Hotline is provided as an unconstrained avenue to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. This alternate means of reporting is provided for your use when you consider it prudent or necessary.

– The Pentagon
– Washington, DC 20301-1900
– (800) 424-9098

Reports Submitted to the FBI

A cleared employee must promptly report any information coming to his or her attention concerning actual, probable or possible espionage, sabotage, or subversive activities. Reports of this nature will be immediately forwarded to the Federal Bureau of Investigation (FBI). You may report this information directly to the FBI if you so choose.
DEFENSE AGAINST ESPIONAGE
DEFENSIVE ACTIONS

Your main defense against espionage is awareness and reporting all suspicious contacts. By alerting your FSO or host facility security contact it is more likely that previously unknown foreign intelligence operatives and espionage activities will be discovered.

If you do find yourself in contact with a suspicious person no need to panic but remember to use caution. Cleared personnel are much more likely to be charmed by a friend than blackmailed by an enemy.
If the contact goes so far that you are asked to provide information, perhaps as a consultant, you should:

• Listen carefully
• Be observant
• Remember as many details as possible
• Keep all options open by neither agreeing or refusing to cooperate
• Remain calm
• Be non-committal
• Ask for time, and
• Report immediately to your Security office/FSO.
Additional information and training can be found at the following Defense Security Services websites:


- [http://www.cdse.edu/catalog/counterintelligence.html](http://www.cdse.edu/catalog/counterintelligence.html)
QUESTIONS

Contact List

The FSO or Security Office of your sponsor’s cleared facility

or

Keith A. Corson
University of Arizona
Facility Security Officer
(520) 626-5865