Be aware when asked to share.

❹ *Communicate Issues of Concern*

Be diligent in reporting to your facility security officer or your Domain Coordinator (see below) any contact information or circumstances that could pose a threat to your company's research and technology. This could include classified national security information, sensitive information, trade secrets, or intellectual property.

Here are examples of contacts that should be reported immediately:

- Requests by anyone, regardless of nationality, for unauthorized access to classified information, proprietary data, or other controlled information.
- Contact with an individual, regardless of nationality, under circumstances that suggest your personnel may be the target of an attempted exploitation by foreign intelligence collectors or international terrorist organizations.
- Contact with anyone receiving information of planned, attempted, actual, or suspected international terrorism, espionage, sabotage, subversion, or other intelligence activities against the Department of Defense or other U.S. facilities, U.S. organizations, or U.S. citizens.
- Actual or attempted unauthorized access into U.S. automated information systems and/or unauthorized transmissions of classified or controlled unclassified information over online computer services and telephones.
- Requests from people who appear to be exploiting the business relationship to the detriment of you or your firm.
- Requests for export-controlled technologies, components, or information.

For further information on items of concern, please request access to the Research and Technology Protection Infragard Special Interest Group at www.infragard.net.

How to Report:

- Report contacts, such as those listed above, to your local facility security officer.
- If you do not have a facility security officer, contact your local Domain Coordinator.

Your Domain Coordinator is: ____

Phone Number: ____

By working together, government agencies, private industry, government contractors, and academia can protect the U.S. economy and critical technology, while, at the same time, protecting our national security. Please join us in keeping the U.S. domain safe and secure; we're looking forward to your partnership.

Partnering to Protect Tomorrow's Technology Today

Globalization has brought opportunities—but also risk.

Is your technology and information safe?

PREVENT ✦ PROTECT ✦ PARTNER ✦ PROSPER
FBI CI DOMAIN PROGRAM

In today's global marketplace, more spies—not just traditional adversaries but also allies, hackers, and terrorists—are trying to steal more of our secrets from more places than ever before.

What Do They Want?

They want our country's most sensitive information—from military plans to national security vulnerabilities to our own intelligence activities to economic interests. These economic interests include our country's trade secrets—from big innovations that give us a leg up in the global marketplace to common or seemingly harmless technologies that could actually assist in developing or improving weapons.

Other countries know that this information and technology will help them modernize their militaries and build their economies. But what U.S. firms often do not realize is how companies in other countries also target your innovations to increase their market share at your expense.

> *"There are more funds expended on R&D by the U.S. Government and industry than any other country in the world."*

There are more funds expended on R&D by the U.S. Government and industry than any other country in the world, making U.S. contractors a prime target for collection of both classified and commercial/proprietary technology by other countries. In fact, the U.S. Intelligence Community (USIC) estimates that every year billions of U.S. dollars are lost to competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies. Adversaries also cull intelligence out of shelved technologies by exploiting open source information and the classified or proprietary material found in trade secrets.

What Is Being Done?

To prevent this unauthorized transfer of technology and sensitive information to foreign governments, organizations, or businesses, the Federal Bureau of Investigation (FBI) and our U.S. Government partners have collaborated to protect key technologies in the U.S. "domain." The FBI's preventative program in this area has been coined the **Counterintelligence Domain Program**. Counterintelligence is the business of identifying, detecting, and mitigating threats posed by Foreign Intelligence Services (FIS) that seek to disadvantage our national security and economic objectives. The Counterintelligence Domain Program is a national, multi-agency initiative focused on sharing information with private industry and academia to safeguard our nation's critical research and technology. Current participants in this program include the FBI, Defense Security Service (DSS), Army Counterintelligence, Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), Counterintelligence Field Activity (CIFA), and the Department of Commerce (Project Guardian).

We cannot do it alone. A partnership with U.S. businesses, universities, and research facilities is the solution to ensure the United States maintains its technological and competitive edge. Whether your domain involves inventing, developing, manufacturing, testing, or maintaining U.S. technology, your partnership with us is critical to protecting your economic interests—and the backbone of our country's vital technologies and national security.

How Can You Protect Your Domain?

1 Protect Your Equities

The first step is to identify your most sensitive research, technologies, and information that FIS, including foreign competitors, may illegally try to acquire. Remember, what they seek is not necessarily classified. Unclassified or sensitive information is often just as critical as classified or proprietary information, especially that which is sought to further foreign economic interests.

Then, once your equities have been identified, we recommend that you develop, implement, and monitor a protection program that includes network security. Make sure to educate your employees about this program and what to do if they suspect your organization has become a target of an FIS. We suggest fully utilizing the Counterintelligence Domain Program services (see 3 for more details).

2 Realize You May Be a Target

Next, realize when you or your firm may be a target of a foreign country's efforts to obtain technology outside of authorized channels. One authorized way for a foreign country to obtain restricted U.S. technology is through an export license. However, it is much easier to simply ask for information.

If you experience the following solicitations, be aware that your company's technology and information are potentially at risk:

- Suspicious requests for information, such as e-mails, phone calls, or personal requests for technology, information, manuals, or parts.
- Extravagant gifts or compliments; this technique is known as *quid pro quo*—creating a friendship to elicit information.
- Invitations to submit papers, attend conferences, or speak at symposia; in advance of the event, ensure that you determine what you are authorized to share.
- Visitors to a facility asking probing or intrusive questions or found in areas outside the scope of the visit's purpose; for example, a visitor wandering off from a group who is later found in a restricted area of the building.

Ultimately, be aware when asked to share.

3 Utilize the Counterintelligence Domain Program Services

To succeed, the Counterintelligence Domain Program needs you as a partner, and the program offers several services to assist you in security, education, training, and awareness. Contact your Domain Coordinator to request the following services:

> *"Unclassified information is often just as critical as classified information."*

- If you are traveling outside of the United States, you can receive a travel briefing prior to your departure to learn about a country's criminal and intelligence threats.
- You can be provided with technology- and program-specific threat information.
- You can take the Counterintelligence Vulnerability Assessment (CIVA). This self-administered assessment survey, designed specifically to assist industry in building a proactive protection capacity, will help focus on areas and issues where your proprietary equities and interests may be most at risk.

In addition, you can visit the Research and Technology Protection Infragard Website, the USIC's common communications portal for counterintelligence information in this arena. This is a secure website that provides actionable and relevant information to private industry, cleared defense contractors, and academia on how to protect your research and technology. Please visit www.infragard.net for a membership application.

Think you are or have been a target?
Flip over for more tips.