Welcome

Welcome to the DoD Counterintelligence Awareness and Reporting Briefing. This briefing is unclassified.

To navigate through this briefing, click on the next arrow at the bottom of the screen.
On September 11th, 2001, American Airlines Flight 77 left Washington Dulles International Airport at 8:20 a.m. en-route to Los Angeles with a six-person crew and 58 passengers. Five of those passengers were actually terrorists, who hijacked the plane and intentionally crashed it into the Pentagon at 9:37 a.m. The attack on the Pentagon killed 184 people. The Department of Defense is the target of both Foreign Intelligence threats and potential terrorist attacks. On any given day, a foreign intelligence agent or terrorist may be assessing a DoD employee for recruitment to commit espionage or acts of terrorism. We must remain vigilant in recognizing and reporting signs of espionage and terrorism.
Objectives

- Identify the threats and methods of Foreign Intelligence Entities (FIE)
- Recognize the Foreign Intelligence Entities use of Cyber attacks
- Describe the Insider Threat
- Identify intelligence and security anomalies
- Understand Counterintelligence Awareness and Reporting requirements

Objectives

At the conclusion of this briefing, you will be able to:

- Identify the threats and methods of Foreign Intelligence Entities (FIE)
- Recognize the Foreign Intelligence Entities use of Cyber attacks
- Describe the Insider Threat
- Identify intelligence and security anomalies
- Understand Counterintelligence Awareness and Reporting requirements
What is Counterintelligence?

Counterintelligence is: “information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.”

Executive Order 12333 was signed by President Ronald Reagan on December 4, 1981.

What is Counterintelligence?

Counterintelligence, or CI, as defined by Executive Order 12333, as amended, is “information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons or their agents, or international terrorist organizations or activities.”

The National Counterintelligence Strategy of the U.S. states that “CI includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st century.”
What does that mean?

- Identifying, understanding, prioritizing, and counteracting foreign intelligence threats.

- Core concerns
  - Intelligence entities of foreign states
  - Terrorist organizations
  - Trusted insider

In addition to collecting and processing intelligence about our enemies, the Intelligence Community is also faced with the problem of identifying, understanding, prioritizing, and counteracting the foreign intelligence threats that are encountered by the United States. This activity is known as counterintelligence.

The core concerns of CI are the intelligence entities of foreign states and similar organizations of non-state actors, such as terrorist organizations and the trusted insider.
“You Are The Target”

- YOU are the first line of defense!
- Remember, CI involves understanding and neutralizing intelligence operations of foreign nations or international terrorist activities.
“You Are The Target”

- As a DoD employee, you can be the target of a Foreign Intelligence Entity anytime, anywhere:
  - Because of what you have access to;
  - Because of who you have access to; or
  - Because of what you know

- Remember: family, friends and co-workers may be viewed as a means to gain information about you

- REPORT SUSPICIOUS BEHAVIOR!
"You Are The Target"

- Common sense and basic CI awareness can protect you against Foreign Intelligence Entity attempts to collect classified, unclassified, or sensitive information.
What are the Adversaries Goals?

To defeat our objectives and advance their interests, foreign entities:
- Collect our information to advance their interests
- Manipulate the intelligence we gather
- Counter our national security operations
- Acquire our technology
- Learn our methods of operation

Foreign entities are actively engaged in efforts to gain information from the U.S. and its allies. To defeat our objectives and advance their interests, they attempt to collect information about our plans, technologies, activities, and operations.

In an attempt to manipulate and distort the facts of intelligence we gather, they may conduct covert influence operations.

They seek to detect, disrupt, and counter our national security operations. In addition, they wish to acquire technology that will enhance their capabilities or economic well-being.

If they can learn our methods of operation, they will be in a better position to carry out their plans.
In late 1980’s, a senior KGB Intelligence Officer commented that for the Soviets to win the Cold War, only three U.S. Generals needed to defect:

- General Electric
- General Motors
- General Dynamics

Just as it was in the 80’s, our Defense Industrial Base is still the target of Foreign Intelligence Entities, who feel they can win the War on Economy through Industrial Espionage. Since the Defense Department relies on the cleared defense contractors developing our nations’ classified or most critical technologies, that puts DoD in the same cross hairs. Our adversaries are highly sophisticated, constant, and pervasive.

Source: A former Cuban Intelligence Officer who was in charge of the Directorate of Intelligence’s M-6, which targeted foreign technology and research.
Collection Methods

- Elicitation
- Unsolicited requests for information
- Visits to DoD Installations
- International conventions, seminars, and exhibits
- Solicitation and marketing of services
- Foreign Intelligence
Elicitation

- Elicitation is a form of Social Engineering.
- The process of subtly drawing forth and collecting information from people, through a seemingly innocent conversation.
- FIE use Elicitation to extract information from people who have access to classified or sensitive information.
Anna Chapman

Introduction

Anna Chapman, born Anna Vyacheslava
Kushchenko, is the daughter of a Russian
intelligence general within the SIS
(Blažko
Vlasovský Razoulík). She practised
counterintelligence trade craft such as
Steganography & counter
surveillance. She was a
deep cover Russian intelligence officer targeting
U.S. policy, economics, and personnel with
potential access.

She would use Facebook to social engineer her
targets and later used Steganography to hide
encrypted her emails back to Russia.

Click the timeline below or click on the next

Anna Chapman

London

Anna moved to London when her father was stationed there. She later married a Brit,
picking up the name Chapman.

Anna Chapman

New York

She left New York, where she
established her own business, helping folks find affordable
living arrangements.

Anna Chapman

June 28, 2010

On June 28, 2010 - she was one of ten
Russians arrested on charges of conspiring to
act as an unregistered agent of a foreign
government.

After it was announced that she was arrested
for espionage against the U.S., hundreds of
her Face Book friends quickly dropped her.
Anna Chapman

July 8, 2010

On July 8, 2010 - she pled guilty and was part of a spy exchange which returned her to Russia in exchange for 4 U.S. sources.

In Oct 2010 - Chapman received highest honors from the Kremlin for her work as an undercover Russian agent working within the United States.
Unsolicited Requests

- From foreign companies, individuals, government officials, and organizations
- Originate via e-mail, telephone, facsimile, or mail
- Increased cases involving suspicious Internet activity

An unsolicited request for information is any request that was not sought or encouraged by DoD for information from a known or unknown company, or from another country. They may originate via email, telephone, facsimile or mail.

The explosive growth of the Internet and abundance of free e-mail accounts has resulted in increased cases involving suspicious Internet activity.
Visits to DoD or Contractor Facilities

- Hidden agendas NOT associated with the stated purpose of the visit
- Visitors or students requesting information and becoming irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed

Foreign visitors include one-time visitors, long-term visitors (exchange employees, official government representatives, students) and frequent visitors (foreign sales representatives). A suspicious contact can occur before, during, or after a visit. Some indicators of suspicious conduct are:
- Last-minute and unannounced persons added to the visiting party
- Wandering visitors who act offended when confronted
- A foreign entity attempts a commercial visit or uses a U.S.-based third party to arrange a visit after an original foreign visit request is denied
- Visitors claim business-related interest but lack experience researching and developing technology
- Visitors ask to meet personnel from their own countries and attempt to establish continuing contact with
Requirements for Visits to DoD

- Contact Security or CI immediately upon learning of a foreign visit.
- CI specialists will provide the host facility with foreign threat and awareness briefings and provide possible countermeasures pertinent to the visit.
- Protect work environment and any classified or sensitive information.

Reporting foreign visitors in advance, as required, is of paramount importance to efforts undertaken to protect the Department of Defense and its protected information.

- The names of all foreign visitors to your unit facility or installation must be pre-approved by security officials prior to the visit.
- It is important to note that not all foreign visitors are intelligence officers; however, some are here to collect more information than they are legally allowed.
- Contact your servicing CI or security official immediately upon learning that you will be the host of a foreign visit to any government facility or installation.

- CI specialists will provide the host facility with foreign threat and awareness briefings and provide possible countermeasures pertinent to the visit.

Protect your work environment and any classified or sensitive information you may be working on when foreign visitors are in your work space.
International Conventions, Seminars and Exhibits

- You can be a target of telephone monitoring and hotel room intrusions (mainly when overseas)
- Technical experts may receive invitations to share their knowledge in international forums
- Experts can be “pressed” for restricted, proprietary, and classified information.

Although the monitoring of telephones and hotel room intrusions are not as likely to take place within the continental United States, this does not preclude a hostile entity from developing and exploiting a relationship with hotel employees. Technical experts may receive invitations to share their knowledge in international forums or could be “pressed” for restricted, proprietary, and classified information.
International Conventions, Seminars and Exhibits

- Collection Indicators:
  - Excessive or suspicious photography, filming of technology and products
  - Casual conversations during and after event hinting at future contacts or relations
  - Foreign attendees’ business cards do not match stated affiliations

Some indicators of this collection practice are:
- Conversations involving classified, sensitive, or export-controlled technologies or products
- The foreign country or organization hosting the event unsuccessfully attempted to visit U.S. government installations or facilities in the past
- You receive an all-expense-paid invitation to lecture in a foreign nation
- Entities want a summary of the requested presentation or brief several months prior to the lecture date
- Excessive or suspicious photography and filming of technology and products
- Casual conversations during and after the event hinting at future contacts or relations, and
- Foreign attendees’ business cards do not match stated affiliations
Noshir Gowadia

Introduction

Noshir Gowadia, an Indian national, was the principal designer of the stealth bomber as a contractor from 1968 to 1986. As one of the principal designers, he conceived and conceptually designed the B-2 Bomber's entire propulsion system (enables B-2 stealth bombers to fly virtually undetected by heat-seeking missiles) and also developed stealth cruise missiles. He referred to himself as the “father of stealth technology.”

He became a naturalized citizen in 1970.

Click the timeline below or click on the

In 1993, Gowadia taught a course to foreigners in an unspecified country, including secret information that he had access to while working as a contractor.
In 1999, he established his own consulting firm, N.S. Gowadia, Inc. He traveled to Chengdu, China which is the epicenter for Research and Development of military technology. Chengdu is also home to the Chengdu Aircraft Design Institute, where the new Chinese state-of-the-art fighter, the J-10 jet is being built. Gowadia provided detailed information on "low observable technology." According to the Department of Justice, Gowadia was paid $2 million for his expertise on the cruise missile and the B-2 Spirit stealth bomber. His engineering expert business N.S. Gowadia, Inc. received $759,000 in economic benefit.
In 2002, he faxed a proposal to develop infrared suppression technology on military aircraft to a representative in an unspecified foreign country. He was accused of passing information to the PRC, the Swiss government and businesses in Israel.
In 2005, as a visiting professor at several universities, Gowadia used classified information during his lectures. He was arrested on charges of marketing and disclosing classified B-2 stealth technology.
Noshir Gowadia

August 9, 2010

On August 9, 2010 he was found guilty on charges that he designed a cruise missile component for China and pocketed at least $100,000.
On January 25, 2011, Gowadia was sentenced to 32 years in prison.
Solicitation and Marketing of Services

- Invitations for cultural exchanges, individual-to-individual exchanges, or ambassador programs
- Offers to act as sales or purchasing agent in foreign countries
- Internships sponsored by foreign government or foreign business
- Purchases of foreign-made equipment
Foreign Intelligence Threats

- NON-TRADITIONAL ACTIVITY
  - Foreign government-sponsored commercial enterprises
  - International trafficking organizations
  - Terrorist organizations

Regardless of the method or activity, Foreign Intelligence Entities seek one thing: to learn more about the Department of Defense plans to exploit its information and impede its mission.

TRADITIONAL ACTIVITY
- Foreign Intelligence Entities operating out of:
  - Embassies
  - Consulates
  - Universities
  - Trade Missions
- Internal Spies (Insider Threat)

NON-TRADITIONAL ACTIVITY
- Foreign government-sponsored commercial enterprises
- International trafficking organizations
- Terrorist organizations
Dongfan Chung

**Introduction**

Dongfan “Greg” Chung was born in China and lived in Taiwan before moving to the United States in 1962. Chung became a naturalized U.S. citizen and spent 40 years working for Boeing and related companies.

Click the timeline below or click on the next button in the top right corner to navigate through this interaction.

1979
1985-2003
2006-2009

**1985-2003**

From 1985 to 2003, Chung made multiple trips to China to deliver lectures on technology involving the space shuttle and other programs, never reporting his travel. During those trips, Chung met with government officials, including agents affiliated with the PRC’s People’s Liberation Army.

**1996**

In 1996, Chung divulged secrets for the B-1 Bomber that came from research years before.

**1979**

In 1979, individuals in the Chinese Aviation Industry began sending “tasking” letters to Chung.
In 2000, Chung was charged with providing proprietary information to China. He supplied trade secrets relating to the Space Shuttle, C-17, B-1 Bomber and the Delta IV rocket. He was tasked by Chinese agents to supply documents and to give lectures in China on space technology and military systems. Gu Weihao of China’s Ministry of Aviation told Chung that passing information through Chi Mak would be “faster and safer” and added: “It is your honor and China’s fortune that you are able to realize your wish of dedicating yourself to the service of your country. Mak was

In 2003, Chung sent three sets of flight manuals on “flight stress analysis” illegally to the PRC. In various letters to his handlers in PRC he mishandled documents and sent engineering manuals relating to the B-1 bomber that was prohibited from disclosure outside the company.

In September 2006, FBI and NASA searched Chung’s house and found more than 250,000 pages of documents from Boeing, Rockwell and other defense contractors that included decades’ worth of stress analysis reports, test results and design information for the space shuttle.

Chung was convicted in July 2009. He was sentenced to nearly 16 years in prison.
What Do They Want?

Defense Information

- classified and unclassified
- personnel information
- personnel weaknesses
- security weaknesses
- locations

What do they want?
Defense Information. This includes classified and unclassified information, personnel information, locations of sensitive information and technology, security weaknesses at cleared facilities and personnel weaknesses that may be exploited.
Intelligence Collection Tradecraft

- Intercepts of cell phones, other wireless signals – “technical eavesdropping”
- Intercepts of open telephone lines
- Intercepts in hotels while TDY
- Looking through the trash - “dumpster diving”
- Simple conversations, online (chat rooms) or in person
- Hacking into unclassified or classified systems
Cyber Threat to DoD Systems

- **External**
  - Input of falsified, corrupted data
  - Malicious code (e.g., virus, logic, Trojan horse)
  - Hacking, also achieved via wireless or Bluetooth
  - Chat rooms - elicitation, relation building
  - Phishing

*See the glossary for a definition of Phishing*

Technological advances have made simple mistakes costly to information systems. The malicious insider (disgruntled employee, saboteur or co-opted employee) has the capability to disrupt interconnected DoD information systems. Other inadvertent actions such as using easy passwords, practicing poor computer security, and emailing or placing personal files on your computer can provide Foreign Intelligence entities an avenue of penetration into DoD systems. Aided by a team of highly sophisticated and well-resourced outsiders, the severity of insider malicious activity may be significantly amplified by:
  - Inputting falsified, corrupted data
  - Malicious code (e.g., virus, logic, Trojan horse)
  - Hacking, also achieved via wireless or Bluetooth
  - Chat rooms - elicitation, relation building
  - Phishing

All of these actions can potentially reduce or compromise our effectiveness and place in jeopardy the lives of our men and women.
In March 2011, theft of an unencrypted NASA notebook resulted in the loss of the algorithms used to command and control the International Space Station. Hackers with IP addresses in China gained "full system access" to change or delete sensitive files and user accounts for "mission-critical" systems at the Jet Propulsion Laboratory. Between April 2009 and April 2011, forty-eight agency mobile computing devices were reported lost or stolen. NASA reported that it was the target of 47 sophisticated cyber attacks in 2011, referred to as "advanced persistent threats". Thirteen of those attacks successfully compromised NASA computers. "The individuals or nations behind these attacks are typically well organized and well-funded and often target high-profile organizations like NASA.”

In the 2010-2011 timeframe, the space agency reported 5,408 incidents "that resulted in the installation of malicious software on or unauthorized access to its systems.” "These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit, to intrusions that may have been sponsored by foreign intelligence services seeking to further their countries' objectives.”

NASA has conducted 16 investigations over the last five years that led to the arrests of foreign nationals from China, Great Britain, Italy, Nigeria, Portugal, Romania, Turkey and Estonia. These intrusions "have affected thousands of NASA computers, caused significant disruption to mission operations, and resulted in the theft of export-controlled and otherwise sensitive data, with an estimated cost to NASA of more than $7 million.”

The most dangerous cyber threats the FBI faces today are posed by the state-sponsored computer experts of hostile foreign nations seeking to steal corporate trade secrets and classified U.S. government documents, and potentially wreak havoc on the nation's most vital infrastructure.

"State-sponsored hackers are patient and calculating, have the time, the money, and the resources to burrow in and to wait.”
Insider Threat to DoD Systems

* WikiLeaks has become a catalyst for DoD action to address insider threat
* DoD has multiple tools for detecting insider threat
* Follow Security Regulations
* Report Security Infractions, Violations or Suspicious Activity

* See the Glossary for definitions of WikiLeaks, insider and insider threat

WikiLeaks has become a catalyst for DoD-wide action to address Insider Threat. Insider misuse is hard to detect because it can operate at a higher semantic level than penetration by an outsider or an outsider attempting to masquerade as an insider. Cyber outsiders can quickly attain many characteristics of an insider, making it difficult to detect. DoD has multiple tools in place to identify and mitigate insider threats. Not only must we reduce the risk of insider threat, we must prevent current malevolent insiders from hampering or subverting this process. It is therefore imperative that you and your co-workers follow security rules and regulations and report all security infractions, violations or suspicious activity to your supervisor and the Office of Security. Imagine what kind of damage could result from a hostile enemy gaining access to JWICS or SIPRNET systems?
Introduction

In July 2010, Army private Bradley Manning was charged with storing classified material on his home computer and transferring national defense information to WikiLeaks, a website dedicated to making secret information public. Manning is at the center of the largest leak of classified material in United States history. He is alleged to have leaked more than 250,000 embassy cables to WikiLeaks, which in turn, made them available to a
Potential Espionage Indicators

Private Manning demonstrated several behaviors that indicated he was a potential security risk. While at the Army Intelligence School, he was reprimanded for posting messages to YouTube that revealed sensitive information.

Manning also displayed anti-social behavior. At Fort Drum, Manning had trouble with his roommates, screamed at superior officers, and was referred to an Army counselor.

Who Reported the Incidents?

Manning was arrested after Adrian Lamo, a self-professed computer hacker, reported to the FBI that Manning had told him during online chats that he had downloaded material from SIPRNet and passed it to WikiLeaks. Lamo said his decision to go to the authorities had not been easy, but he believed lives were in danger. On May 25, 2010, shortly after his first chat with Manning, Lamo met with FBI and Army CID officers, where he showed them the chat.

Timeline

It is alleged that Manning first contacted WikiLeaks in November 2009, days after it posted 570,000 pager messages from the September 11th, 2001 attacks.


Damage/Impact

In the wake of this unprecedented document dump, the administration ordered agencies to ensure that unauthorized employees do not gain access to sensitive or classified information. The DoD Insider Threat Program, a Department of Defense Directive, was drafted which will require all agencies to establish a program to help identify and mitigate the insider threat vulnerability.
The Charges

Manning was arrested on May 26, 2010. On July 5, 2010, under the Uniformed Code of Military Justice (UCMJ), he was charged with violations of Articles 92 and 134 for leaking hundreds of thousands of classified and sensitive U.S. government documents. Other charges against him include:

- aiding the enemy,
- wrongfully causing intelligence to be published on the internet knowing
Economic Espionage Annual Loss

The FBI estimates that they are aware of at least $200 Billion dollars worth of information stolen each year.
Recruitment Process

Spotting and Assessment Phase

In the Spotting and Assessment Phase, the foreign intelligence officer begins with identifying the target. They may meet at trade shows, on line, or at social events.

The intelligence officer may begin by accessing the corporate web page to identify candidates to target via emails or social engineering. As the potential source is being assessed, the intelligence officer will look for exploitable weaknesses such as; alcohol, drugs, extramarital affairs, gambling or other financial problems.

Development, Recruitment and Handling Phase

A close relationship is established and once the source gains trust, the intelligence officer makes the offer to help him through his problems. If he takes the bait, the source is recruited and they move into a more clandestine relationship.

The source handler instructs the individual on specific information needed and begins paying him for his efforts. He is now hooked and on his way to espionage.
Indicators of FIE Targeting

- Invited to lecture/attend conference in foreign country
- Singled out for socializing or special attention
- Meets foreign national becomes romantically involved
- Personally involved with known/suspected foreign intelligence officer or foreign intelligence entities
Potential Espionage Indicators

- Unreported contact with foreign nationals
- Attempting to gain access, without need-to-know
- Unexplained absences
- Foreign travel of short duration
- Avoiding polygraph
- Terminating employment
- Illegal downloads

Potential espionage indicators (PEIs) are activities, behaviors, or circumstances that “may be indicative” of potential espionage activities by an individual who may have volunteered or been recruited by a foreign entity as a willing espionage agent.

Many of these methods result in detectable behavior and activities that could indicate an act of espionage. Some potential indicators are:

- Unexplained affluence
- Concealing foreign travel
- Unusual interest in information outside the scope of assigned duties
- Unusual work hours
- Taking classified material home
- Disgruntled
- Copying files
- Unreported contact with foreign nationals
- Attempting to gain access, without need-to-know
- Unexplained absences
- Foreign travel of short duration
- Avoiding polygraph

These indicators are not limited to those with access to classified information.
What is a Security Anomaly?

- Examples of anomalies include:
  - An adversary conducts activities with precision that indicates prior knowledge.
  - An adversary uses technical countermeasures to block a previously undisclosed or classified U.S. intercept technology.
  - Foreign officials reveal details they should not have known.
  - An adversary is able to anticipate DoD plans and activities.
  - Media is waiting where a sensitive DoD program will be tested.

“Foreign power activity or knowledge which is inconsistent with the expected norm that suggests that foreign powers have knowledge of U.S. national security”

Examples of anomalies include:
- An adversary conducts activities with precision that indicates prior knowledge.
- An adversary uses technical countermeasures to block a previously undisclosed or classified U.S. intercept technology.
- Foreign officials reveal details they should not have known.
- An adversary is able to anticipate DoD plans and activities.
- Media is waiting where a sensitive DoD program will be tested.
Detection and Identification

- Detecting an anomaly requires a degree of suspicion
- Don’t simply believe that the unexpected activity was coincidental
- Anything that doesn’t fit the pattern could be an indicator of espionage
- When in doubt, report it!
What Should You Do?

- If you feel you are being solicited for information:
  - Prepare in advance
  - Never answer uncomfortable questions
  - Change any conversation
  - Be observant
  - Do not probe for information
  - Be wary of personal questions
  - Provide non-descript answers

- Reporting Covers You!

If you feel you are being solicited for information:
- Prepare in advance - practice responses to possible questions concerning your duties
- Never answer questions which make you feel uncomfortable
- Without indicating that you are uncomfortable, change any conversation that might be too probing with respect to your duties, private life, and coworkers
- Be observant - Note as much as possible about the person asking questions
- Do not probe for information - Nonchalantly ask questions about them
- Be especially wary of questions about your personal information or colleagues’
- Provide non-descript answers; leave the talking to someone else

Remember, reporting covers you!
Your Responsibilities

- Practice good Operations Security!
  - Do not leave sensitive documents or equipment unattended in cars, hotel rooms, or hotel safes
    - Store in appropriate secure facilities:
      - U.S. Military or government site
      - U.S. Embassy,
      - U.S. Federal law enforcement office, or
      - A cleared contractor facility
  - Keep unwanted material secured until it can be disposed of
  - Burn or shred paper and discs or other media

Do not leave sensitive documents or equipment unattended in cars, hotel rooms, or hotel safes. Store the information in appropriate secure facilities like U.S. Military or government site, a U.S. Embassy, U.S. Federal law enforcement office, or a cleared contractor facility.

Keep unwanted material secured until it can be disposed of.

Burn or shred paper and discs or other media.
Your Responsibilities

- Practice good Communications Security!
  - Do not use personal/commercial computers, telephones, or fax for sensitive or classified matters
  - Use secure communications equipment at appropriate U.S. Government establishments
  - Take battery out of cell phones before holding sensitive discussions
  - Beware of being overheard in public

Do not use personal/commercial computers, telephones, or faxes for sensitive or classified matters, especially at a foreign establishment. Take the time to use secure communications equipment at appropriate U.S. Government establishments such as an Embassy, U.S. Federal law enforcement office, or a cleared contractor facility. Take the battery out of cell phones before holding sensitive discussions, and beware of being overheard in public.
Need to Know/Need to Share

- **Rule of Thumb:**
  - Does anyone need to know the information?
  - Is there a need to share the information?

- Balance need-to-know with necessity of sharing classified information

- Significant number of past spies had access to and later passed information that they had no need-to-know

---

We need to continue working toward establishing and maintaining dissemination and control procedures that balance need-to-know with necessity of sharing classified information. A significant number of individuals convicted of espionage and other national security crimes had access to and later passed information that they had no need-to-know.
Penalties for Espionage

The penalties for Espionage include:
- Fines
- Up to life imprisonment, and
- Death

The penalties for Espionage include:
- Fines
- Up to life imprisonment, and
- Death
Theft of Trade Secrets for Foreign Government

- Penalty for a individual
  - $500,000 fine, and/or
  - not more than 15 years in Federal prison

- Penalty for a organization
  - a fine of not more than $10,000,000

According to the Economic Espionage Act of 1996, the penalties for economic espionage can be stiff. Those using stolen trade secrets to benefit a foreign government face a fine of up to $500,000 and/or up to 15 years in Federal prison, while companies can be fined up to $10 million for stealing trade secrets for another government.
Theft of Trade Secrets for Personal Gain

- Penalty for an individual
  - may be fined, and/or
  - imprisonment up to 10 years

- Penalty for an organization
  - a fine of not more than $5,000,000

Those who steal trade secrets for their own gain may be fined and/or put in prison for up to ten years. Companies can be fined up to $5 million for using stolen secrets for their own gain.
Reportable Contacts

Introduction

It is important to report any suspicious foreign intelligence, international terrorist and cyberspace contacts, activities, indicators or behaviors.

According to DoD Directive 5240.06, a Foreign Intelligence Entity is “any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.”

Click through this interaction using the next button at the top right of the page to learn about each of these activities and how to report them.

For the answer to each question, click the green arrow at the bottom right of the page.

Reportable Contacts

What are reportable foreign intelligence contacts?

According to DoD 5240.06 Reportable Foreign Intelligence Contacts, Activities, Indicators and Behaviors include:

- Espionage, sabotage, subversion, or other intelligence activities directed against the U.S.
- Contact with Known or Suspected Foreign Intelligence
- Illegal activity
- Discussing classified in inappropriate locations
- Attempts to obtain information without need to know
- Request to witness destruction certificates
- Unauthorized electronic/recording devices
- Unauthorized storage of classified information
- Unauthorized access to information systems
- Listening or surveillance devices in restricted areas
- Unsecured/unauthorized transmission of classified
- Removing of classification markings
- Discussing classified over non-secure lines
- Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material

Reportable Contacts

What are reportable international terrorism contacts?

Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors include:

- Advocating violence on behalf of terrorist organization
- Advocating support for terrorist organizations or objectives
- Providing financial support to terrorist organizations
- Contact or association with known or suspected terrorists
- Repeated browsing of international terrorist websites
- Expressing an obligation to engage in violence in support
- Familial ties to known or suspected terrorists or supporters
- Attempt to recruit on behalf of terrorist organizations
- Collecting intelligence on behalf of terrorists

Reportable Contacts

What are reportable cyberspace contacts?

Reportable Cyberspace, Activities, Indicators, and Behaviors include:

- Actual or attempted unauthorized access into classified systems
- Unauthorized network access
- Suspicious internet activity (downloads, uploads, etc)
- Unauthorized use of removable media
- Unauthorized e-mail traffic to foreign destinations
- Hacking or cracking activities
- Social engineering, electronic elicitation, spoofing, phishing
- Password cracking, key logging, steganography
- Internet browsing beyond normal duties/responsibilities
- Denial of service attacks or suspicious network failures
- Malicious codes, viruses, worms, trojans, malware, spyware
- Tampering with information systems
Reportable Contacts

What do I do if I believe I have witnessed suspicious activities?

If you believe that a foreign entity has attempted to contact or recruit you, or if you suspect a co-worker of suspicious activities; contact your Counterintelligence Office immediately.

Supervisors must report questionable intelligence Activities to the appropriate CI office within 72 hours.

Personnel failing to report CI concerns are subject to appropriate disciplinary action under regulations governing military or civilian employees.

Notify your Security Office:
- If you have any questions pertaining to foreign travel (personal or official), whether or not you have Sensitive Compartmented Information (SCI) access, and
- Within 30 days of foreign travel for official business or leisure, if you have SCI access.
Course Summary

“There is but one evil I dread, and that is their spies.

I could wish therefore, the most attentive watch be kept.”

~ George Washington

Now that you have completed this briefing, you should be able to:

- Identify the threats and methods of Foreign Intelligence Entities
- Recognize the Foreign Intelligence Entities use of Cyber attacks
- Describe the Insider Threat
- Identify Intelligence and security anomalies
- Understand Counterintelligence Awareness and Reporting requirements

For questions pertaining to this briefing, contact your supporting counterintelligence or security office.
In order to receive course credit you must complete the following quiz.
Quiz

Potential espionage indicators (PEIs) are activities, behaviors, or circumstances that "may be indicative" of potential espionage activities by an individual who may have volunteered or been recruited by a foreign entity as a witting espionage agent. Examples of PEI include:

- Unexplained affluence, Concealing foreign travel, Unusual work hours, Avoiding polygraph
- Taking classified material home, Illegal downloads, Unreported contact with foreign nationals
- Disgruntled employee, Attempting to gain access without need-to-know, Taking short trips
- Copying files, Unexplained absences, Terminating employment
- All of the above
If you feel you are being solicited for information which of the following should you do?

- Do not probe for information - Nonchalantly ask questions about them
- Without indicating that you are uncomfortable, change any conversation that might be too probing with respect to your duties, private life, and coworkers
- Never answer questions which make you feel uncomfortable
- Be observant - Note as much as possible about person asking questions
- All of the Above
Collection methods of operation frequently used by Foreign Intelligence Entities to collect information from DoD on the critical technology being produced within the cleared defense contractor facilities we support include:

- International conventions, seminars, and exhibits
- Cyber Attacks
- Unsolicited requests for information
- Solicitation and marketing of services
- All the above
Foreign Intelligence Entities seldom use the Internet or other communications including social networking services as a collection method.

- [ ] True
- [ ] False
Under DoDD 5240.06 Reportable Foreign Intelligence Contacts, Activities, Indicators and Behaviors; which of the following is not reportable?

- Contact with Known or Suspected Foreign Intelligence
- Removing of classification markings
- Unexplained or undue affluence
- Frequent questionable foreign travel
- None of the above
DoD personnel who suspect a coworker of possible espionage should:

- Start recording their conversations to gather evidence
- Discuss situation with others to get second opinion
- Call the FBI Hot Line
- Report directly to your CI or Security Office
Counterintelligence, as defined by Executive Order 12333, as amended, is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities."

- True
- False
Personnel who fail to report CI Activities of concern as outlined in Enclosure 4 of DoD Directive 5240.06 are subject to appropriate disciplinary action under regulations.

☐ True
☐ False
Cyber Vulnerabilities to DoD Systems may include:

- Disgruntled or Co-opted employee
- Weak passwords
- Viruses
- Illegal downloads
- All of the above
Which of the following is **NOT** an example of an anomaly?

- An adversary conducts activities with precision that indicates prior knowledge.
- An adversary uses technical countermeasures to block a previously undisclosed or classified U.S. intercept technology.
- Foreign diplomat attempts to defect.
- Foreign officials reveal details they should not have known.
Foreign Intelligence Entities seldom use elicitation to extract information from people who have access to classified or sensitive information.

- True
- False
Result:

Congratulations! Your test score qualifies you to receive a Certification of Successful Course Completion. Click Next to continue.