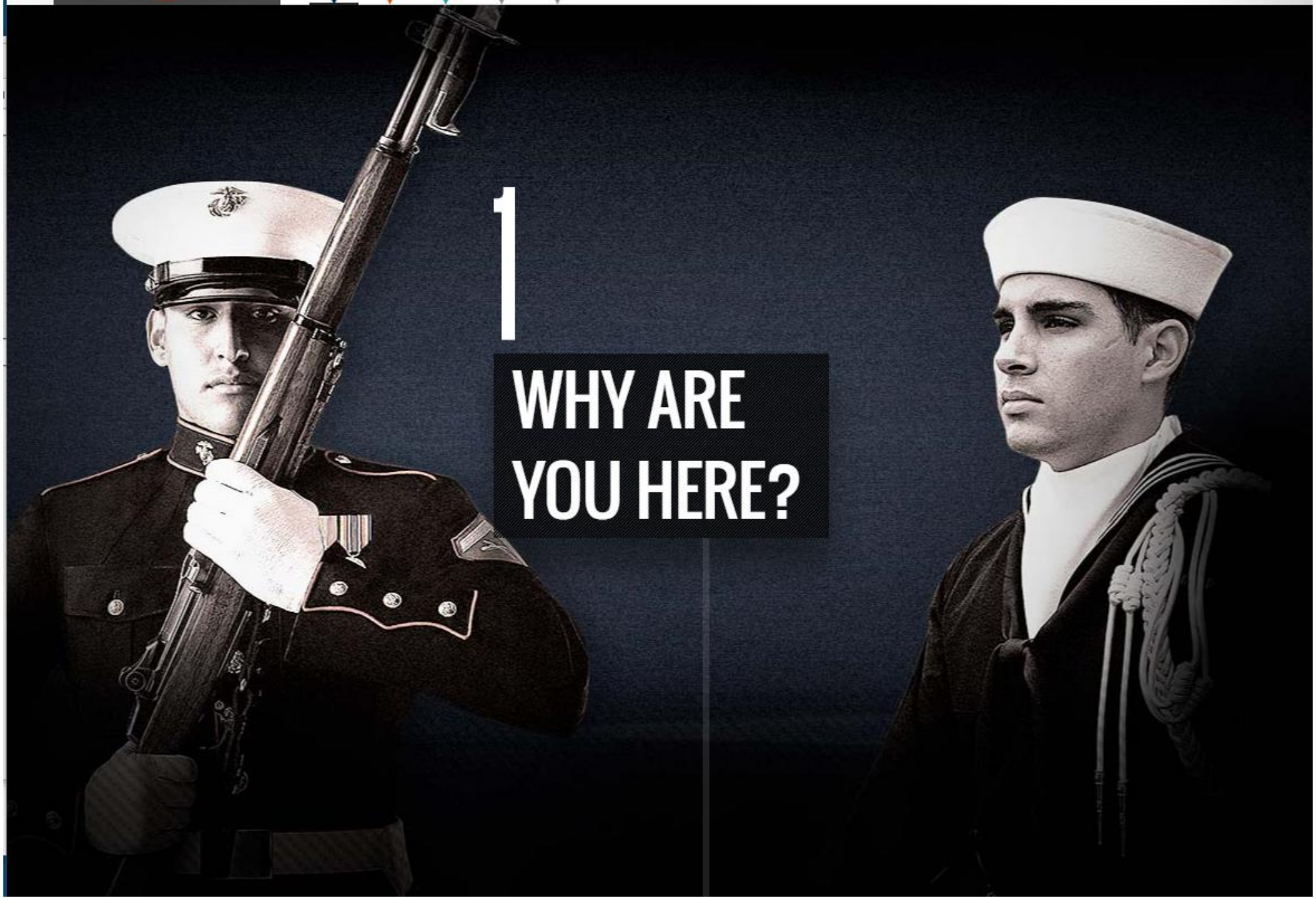

1
WHY ARE YOU HERE?

THE INSIDER THREAT LEAVES A LONG LINE OF VICTIMS

Loss of critical information and technology dramatically decreases the United States' ability to maintain battlefield superiority, strategic and tactical advantages, and our forces' ability to protect themselves.

THE THREAT IS REAL AND SOMETIMES IT EMANATES FROM THE INSIDE.

WHAT ARE THE TYPES OF DAMAGE?

THE DAMAGE TODAY'S INSIDER THREAT CAN INFLICT TAKES MANY FORMS.

Deaths
of military and civilian personnel

Loss
of military superiority

Countermeasures
to U.S. weapons and tactics

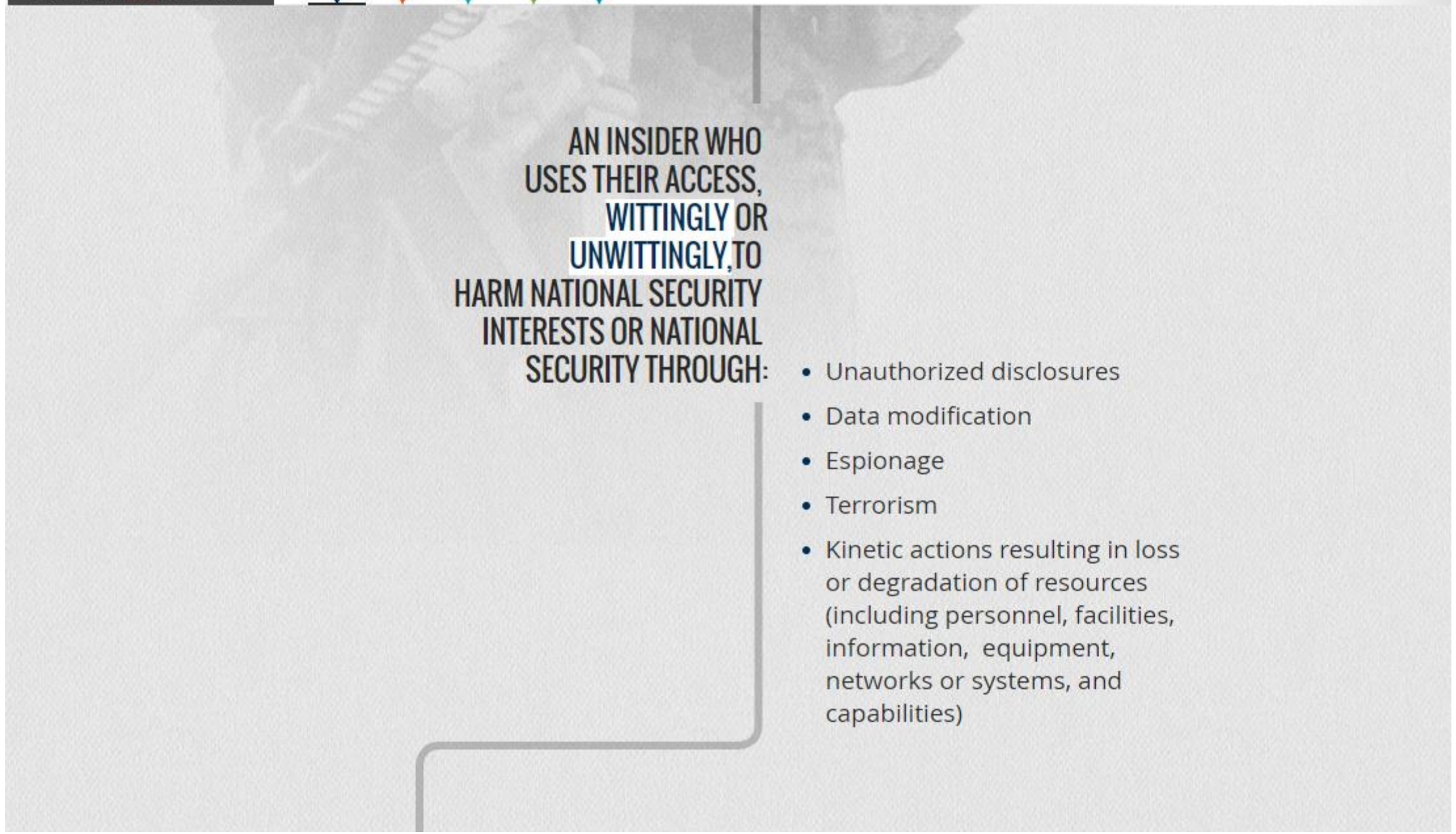
Waste
of billions of dollars and countless hours in research, development, and acquisition

Destruction
of families

WITH YOUR VIGILANCE AND HELP

we can stop the threat before damage is done.

WHAT IS AN INSIDER THREAT?



AN INSIDER WHO USES THEIR ACCESS, WITTINGLY OR UNWITTINGLY, TO HARM NATIONAL SECURITY INTERESTS OR NATIONAL SECURITY THROUGH:

- Unauthorized disclosures
- Data modification
- Espionage
- Terrorism
- Kinetic actions resulting in loss or degradation of resources (including personnel, facilities, information, equipment, networks or systems, and capabilities)

KNOWLEDGE CHECK

MODULE 1

Read each question and use the information you learned above to choose the best answer.

01

An insider threat may not realize that they are causing harm to national security.

✔ **a. True**

b. False

CORRECT!

The correct answer is **True**.

An insider threat is an insider who uses his/her access, wittingly (knowingly) or unwittingly, to harm national security interests or national security.

2

THE THREAT

THREATS

TAKE MANY FORMS

and they all have the potential to put our nation and the people who serve it in harm's way.

As a result, adversaries target U.S. civilian and military personnel to:

- Cause harm to the United States and its resources (including personnel)
- Gain a competitive edge
- Diminish the success of a particular United States program or operation
- Promote an ideology
- Compete with the United States for global or regional political and economic influence
  - Develop or obtain the most advanced military technology to defend themselves against a hostile neighbor
  - Influence U.S. policy towards themselves and a hostile neighbor
  - Rapidly acquire and develop new technologies to ensure their economic future


DID YOU KNOW?
ADVERSARIES
CAN INCLUDE "FRIENDLY"
OR "ALLIED" COUNTRIES.
WHAT ARE THE
TYPES
OF THREATS?

1 FOREIGN INTELLIGENCE ENTITY (FIE)

A foreign organization, person, or group that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, disrupt U.S. systems and programs, or gain a competitive edge.

Includes:

- Foreign intelligence
- Security services
- International terrorist organizations
- Organized crime groups
- Drug cartels

FACT:

Adversaries collect **small pieces** of information.

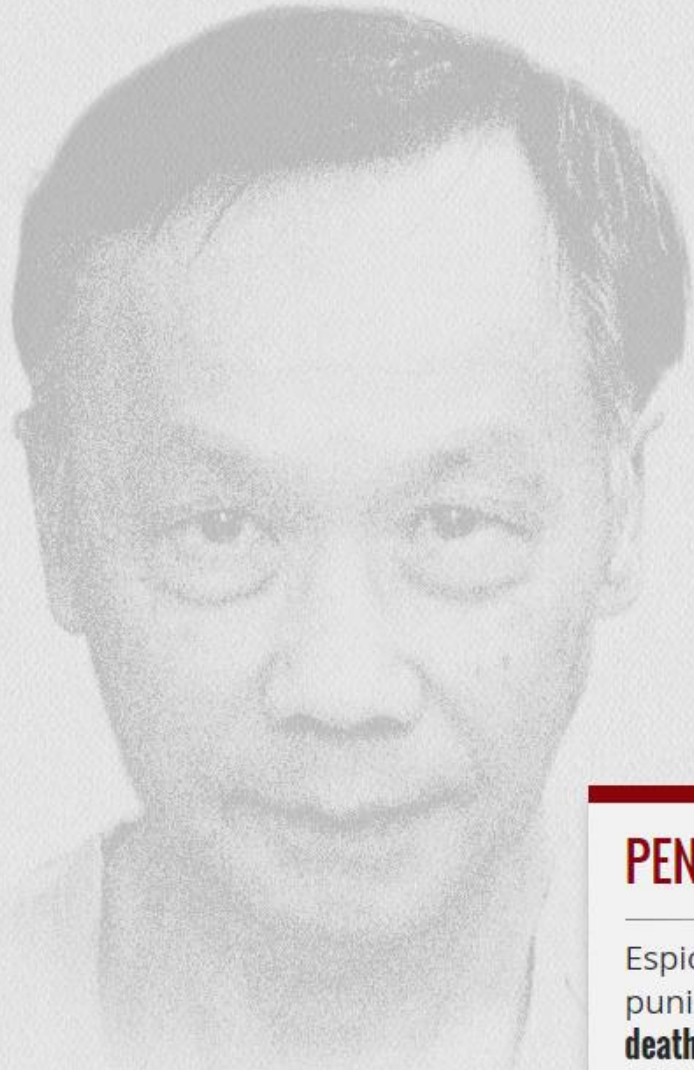
WHEN COMBINED, THEY CAN REVEAL THE WHOLE PICTURE.

Source // Interagency OPSEC Support Staff, "Intelligence Threat Handbook"

2 FIE - ESPIONAGE

The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of a foreign national.

Chi Mak, an electrical engineer on contract with the U.S. Navy, illegally exported sensitive defense technologies to China.



PENALTY

Espionage is punishable by **death** under the UCMJ & U.S. Code.

FACT:

MORE THAN 70%

of those convicted of espionage were citizens born in the United States.

Source // CI Centre: Citizenships of Individuals Identified in Espionage Related Cases, 1949-2016

EXAMPLES OF INFORMATION SOUGHT BY FIEs

- Project information on policies and intentions of the DoD worldwide
- Names, positions, phone numbers, email addresses, and PII
- Size or composition of an organization
- Scientific, military, and industrial technology
- Indications of reorganization or friction
- Missions, timetables, strengths, destinations, and readiness
- Security procedures
- Mission support
- Travel plans

3 TERRORISM

The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs.

Any support or advocacy of terrorism, or association with persons or organizations promoting or threatening violence, is a concern—even if the individual is not directly involved in planning a terrorist attack.

PENALTY

Terrorist acts that result in the loss of life are punishable by **death** under the UCMJ & U.S. Code.

FACT:

MORE THAN 50%

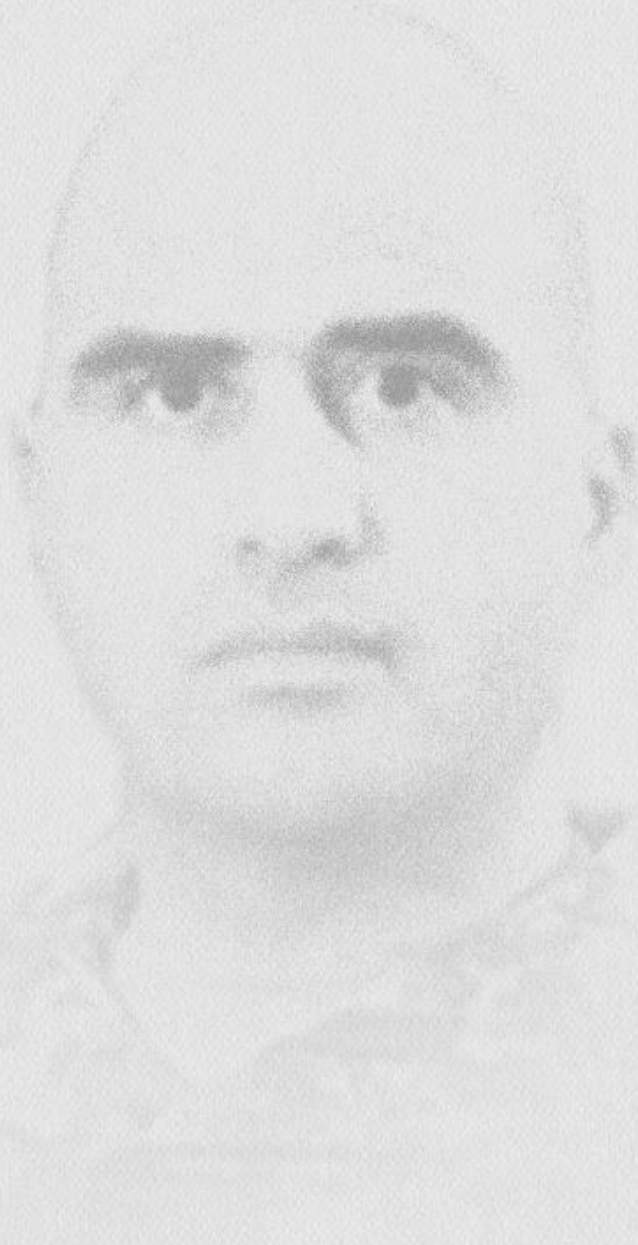
of terrorist attack victims worldwide are **civilians**.

Source // 2016 FBI Report

4 TERRORISM: SELF-RADICALIZATION

Individuals become terrorists without affiliation to or tasking by a radical group—although they may be influenced by its ideology or messages. Any ideology can be an influence, though self-radicalization is commonly associated with radical Islam.

Nadal Hasan, an Army psychiatrist at Fort Hood, killed 13 and wounded 32 at the Fort Hood Soldier Readiness Center.



SELF-RADICALIZATION CAN LEAD TO ACTS OF TERRORISM AND WORKPLACE VIOLENCE.

FACT:

SELF-RADICALIZED ISLAMIC EXTREMISTS TEND TO BE MALE, SECOND- OR THIRD-GENERATION IMMIGRANTS FROM MIDDLE-CLASS BACKGROUNDS

and have "ordinary" lives and jobs, and little, if any, criminal history.

Source // New York Police Department's phase model of self-radicalization

5 WORKPLACE VIOLENCE

An individual uses violence against an identified or symbolic target in a workplace as a response to a perceived conflict or problem.

The person will display observable "attack-related" behaviors that fall along a continuum from idea to action, including thinking, planning, and logistical preparation.

Aaron Alexis, a computer technician assigned to the Washington Navy Yard, killed 12 and wounded 8 at the Naval Sea Systems Command (NAVSEA) Headquarters.

Concerning behaviors associated with workplace violence include:

- physical altercations
- violent gestures/intimidation
- recurring suicidal and/or homicidal threats
- harassment
- stalking
- domestic violence
- sabotage
- substance use/abuse
- inappropriate weapon possession or use
- anger issues
- deteriorating physical appearance
- reckless sexual and financial conduct

WORKPLACE VIOLENCE IS THE CULMINATION OF MULTIPLE FACTORS

that typically involves conflicts, disputes, and failures. The potential perpetrator does not effectively cope with perceived stressful events, including a current situation and the target.

FACT:

Between 2011-2015,

2,173 PEOPLE WERE KILLED

in the U.S. as a result of workplace violence.

Source // Bureau of Labor Statistics (BLS), "Workplace Homicides by Selected Characteristics, 2011-2015"

MYTH VS. REALITY

MYTH:

Violent employees just "snap" without warning or clues.

MYTH:

Individuals are dangerous or not dangerous.

REALITY:

Violence is the final action in an often long and drawn out conflict.

Attacks are thought about and planned over time.

Potentially dangerous individuals present multiple observable behaviors to multiple people, including verbal statements and threats and aggressive behaviors.

REALITY:

Individuals fall along a continuum of violence risk that can increase and decrease over time and in response to certain stressful events.

KNOWLEDGE CHECK

MODULE 2

Read each question and use the information you learned above to choose the best answer.

01

Foreign adversaries target U.S. personnel in order to:

a. Cause harm to the United States and its resources, to include personnel

b. Gain a competitive edge

c. Diminish the success of a particular United States program or operation

✔ **d. All of the above**

CORRECT!

The correct answer is **d**.

These are just a few reasons why adversaries target U.S. civilian and military personnel. Adversaries can include "friendly" and "allied" countries; it might not be easy to spot the adversary.

02

What types of information do foreign intelligence entities (FIE) want?

a. Scientific, military, and industrial technology

b. Missions, strength, timetables, destinations, and readiness

c. Indications of reorganization or friction

✔ **d. All of the above**

CORRECT!

The correct answer is **d**.

FIEs want these types of information and more, including:

- Project information on policies and intentions of the DoD worldwide
- Mission support
- Security procedures
- Travel plans
- Anything that gives the size or composition of an organization
- Names, positions, phone numbers, email addresses, and PII

03

Violent employees just "snap" without warning or clues.

a. True

✔ **b. False**

CORRECT!

The correct answer is **False**.

Potentially dangerous individuals present multiple observable behaviors to multiple people, including verbal statements and threats and aggressive behaviors. Know the signs and report what you see and know.

3 METHODS OF OPERATION

FIE METHODS

OF OPERATION ARE ALL ABOUT SPOTTING AND ASSESSING A POTENTIAL TARGET.

A FIE's goal is to find out what a potential target knows or has access to, what makes him/her tick, what in his/her personality or life can be exploited, and what is so important to that person that it will motivate him/her to action.

Such as:

- Loyalties/obligations to a foreign country or foreign relatives
- Anger or bitterness toward employer
- Attraction to adventure and risk-taking
- Need for praise or ego recognition
- Circumstance that creates an urgent need for money

FACT:

target the United States, seeking information and technology.

Source // NSA Threat Briefing, 2008

WHAT ARE THE TRADITIONAL METHODS THAT FIEs USE?

AWARENESS WILL MAKE YOU MORE ALERT TO POSSIBLE THREATS.

1 OPEN SOURCE

FIEs prefer to use the least intrusive methods to gather information, using publicly available open sources, such as newspapers and blogs, media and photographs, maps and Google searches, social media, and apps—often captured via unsecure networks or in public places.

HOW IS THE INFORMATION USED?

- Provide information about personal interests, preferences, and motivations
- Reveal personal and professional activities
- Provide adversaries with additional targets
- Identify potential vulnerabilities
- Provide more details than should be shared
- FIEs use fake social media profiles to target DON members from whom they elicit sensitive information

WHAT IS THE ADVERSARY'S GOAL?

- Aggregated information
- A customized picture used to target you, exploit your vulnerabilities, recruit you, and gather intelligence

HOW CAN I PROTECT MY INFORMATION?

- Limit publicly available information
- Actively manage privacy settings and policies
- Use multiple and strong passwords
- Don't respond to or open attachments from unknown senders
- Limit the use of professional networks for personal business

2 ELICITATION

The goal of elicitation is to get you talking and keep you talking. Elicitation is a common, effective technique to subtly collect information through face-to-face or online interaction, often used during facility and ship tours, and at conventions and seminars where participants are eager to share information.

FIEs operate under THE GUISE OF:

- THINK TANKS
- EXCHANGE STUDENTS
- RESEARCH
- ORGANIZATIONS
- FOREIGN LIAISON OFFICERS
- OFFICIAL DELEGATIONS

WHY DOES IT WORK?

- It's hard to recognize and easy to deny
- It seems like innocent conversation
- It exploits human nature—in general, we aspire to be polite and helpful, appear well-informed, be appreciated, and trust others

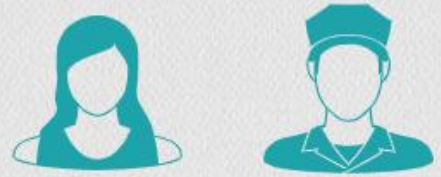
WHAT TECHNIQUES ARE USED?

FLATTERY/ APPEAL TO EGO

Asking your opinion or valuing your insights

What a great brief, you sound like you're a true expert on your program.

Your job sounds very exciting. I'd love to hear more about it.



QUID PRO QUO

Sharing information with you in hopes you'll reciprocate

Our ship's going to be ported in Italy in August. Where will your ship be in August?

I've just been cleared by my agency to work on that program. Is that the same one you're working on.

MUTUAL INTEREST

Focusing on details you have in common

HOW DO I PROTECT MYSELF?

- Don't allow others to control the conversation
- Listen more than you talk
- Deflect a question with a question
- Change the topic
- Be general and nonspecific
- Plead ignorance
- Don't answer

METHODS OF ELICITATION

FALSE FLAG

An agent can misrepresent him/herself as a citizen of a friendly country, nation, or organization in order to lessen suspicion and foster trust.

LEVERAGING OFFICIAL CHANNELS

Foreign liaison officers, foreign exchange officers, or other high-ranking foreign nationals can gain access to important information on official visits.

PHISHING & ONLINE SCAMS

An adversary may try to identify and recruit a target by soliciting information through deceiving emails. This technique may be used to check for gullibility and to test willingness.

3 EAVESDROPPING & ELECTRONIC SURVEILLANCE

AS SIMPLE AS IT SEEMS, FIEs CAN LEARN A LOT ABOUT A POTENTIAL TARGET OR ORGANIZATION BY STANDING BACK AND OBSERVING BEHAVIORS AND HABITS.

In doing so, FIEs can identify a target's personal interests and then disarm them by inserting themselves into seemingly "safe" environments, like fitness classes, church congregations, or local hangouts.

FIEs OPERATE AGGRESSIVELY

IN THEIR OWN COUNTRY

and often obtain information via:

- Surreptitiously entering hotel rooms to access laptop computers, briefcases, and suitcases
- Secret monitoring or recording of phone conversations that take place in hotel rooms, offices, meeting areas, and restaurants
- Intercepting phone, fax, and email communications
- Positioning themselves within earshot of a conversation or within view of a computer screen
- Intercepting communications when devices are connected to public Wi-Fi, unsecured networks, or unencrypted email systems

4 RECRUITMENT

Once a target is selected, FIEs will devise a strategy to entice or coerce the target into working for them.

HOW DO FIES RECRUIT?

- Collecting personal details about the target
- Building a personal relationship or befriending to gain trust
- Coercing or using incentives
- Exploiting vulnerabilities, personal weakness, or circumstances
- Starting with small requests, then making bigger demands
- Praising and rewarding for accomplishments
- Using brute force

DID YOU KNOW?

BRUTE FORCE

is an overt method in which FIEs use intimidation, coercion, or blackmail to get a target to cooperate and provide information.

THIS METHOD IS OFTEN USED WHEN A TARGET HAS RELATIVES LIVING IN A FOREIGN COUNTRY.

THE CYBER THREAT

THANKS TO THE INTERNET, our adversaries around the world no longer have to leave their offices to gather information:

They can access our information in seconds, without traveling for days and spending vast amounts of money and time to locate and exploit or recruit an insider who may or may not have the morsel of information they seek.

One way our adversaries use cyberspace is by a direct intrusion attack on our networks or by using our personnel to gain access to a network via a user's account. FIEs then use the victim's system as a launch platform for attacks on other sites or areas of the network.

Social networking sites, such as Facebook and Twitter, are great ways to connect with people, share information, and market products and services. However, these sites can also provide adversaries with the critical information needed to disrupt your missions and harm you, your co-workers, and even your family members.

REMEMBER, YOUR INFORMATION COULD BECOME PUBLIC AT ANY TIME THROUGH HACKING, CONFIGURATION ERRORS, SOCIAL ENGINEERING, OR THE BUSINESS PRACTICE OF SELLING OR SHARING USER DATA.

THINK BEFORE YOU POST.

IN FACT, OLD TECHNIQUES GET NEW LIFE USING TODAY'S TECHNOLOGY.

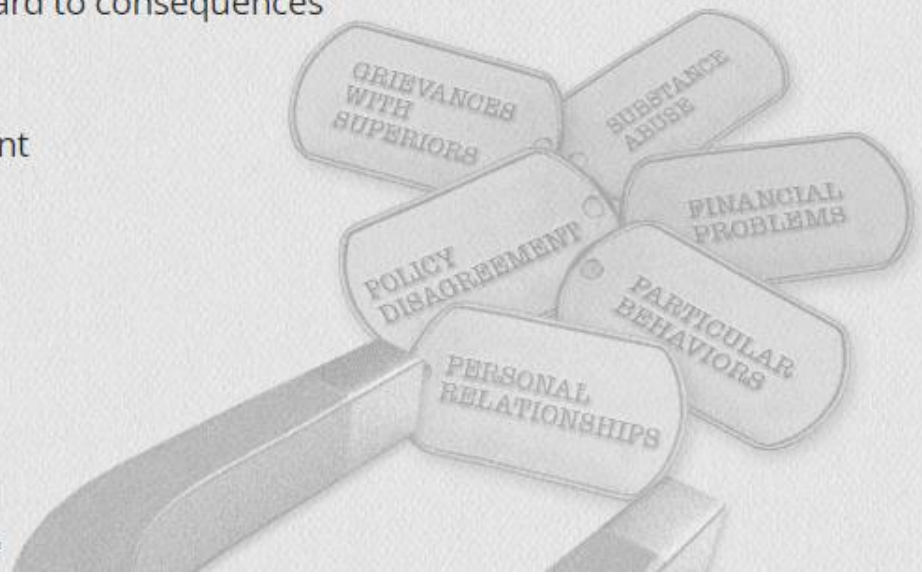
Elicitation, eavesdropping, recruitment, and open source research can be even easier online.

WHAT MAKES SOMEONE A TARGET?

NOT EVERYONE IS A VIABLE TARGET.

The adversary evaluates prospective targets based on placement, access, and exploitable behaviors and characteristics, such as:

- Access to information and the ability to collect the information
- Close and continuous foreign contacts
- Financial issues
- Substance abuse
- Tendency to overshare on social media
- Action without regard to consequences
- Impulsivity
- Sense of entitlement



YOU DON'T NEED TO BE THE MOST VALUABLE TARGET- JUST THE MOST AVAILABLE ONE.

KNOWLEDGE CHECK

MODULE 3

Read each question and use the information you learned above to choose the best answer.

01

Adversaries often exploit personnel's lack of OPSEC through social networking, elicitation, and eavesdropping.

✔ **a. True**

b. False

CORRECT!

The correct answer is **True**.

Lack of OPSEC practices can lead to unintentional disclosures.

02

Your behaviors can make you a target.

- [x] **a. True**
- [ ] b. False

CORRECT!

The correct answer is **True**.

Foreign Intelligence Entities (FIE) exploit a target's personality and life situation such as:

- Loyalties/obligations to a foreign country or foreign relatives
- Anger or bitterness toward employer
- Attraction to adventure and risk taking
- Need for praise or ego recognition
- Circumstance that creates an urgent need for money

03

How can you protect yourself online and mitigate what is available to the adversary?

- ✔ **a. Actively manage privacy settings and privacy policies**
- b. Delete all social media accounts
- c. Use an alias for all online interactions
- d. You can't, why bother

CORRECT!

The correct answer is **a**.

You don't have to go off the grid to protect your information, instead:

- Actively manage privacy settings and privacy policies
- Limit publicly available information
- Use multiple and strong passwords
- Don't respond to or open attachments from unknown senders
- Limit the use of professional networks for personal business

04

Foreign Intelligence Entities (FIEs) can get information from you by:

a. Get you talking and keep you talking

b. Eavesdropping

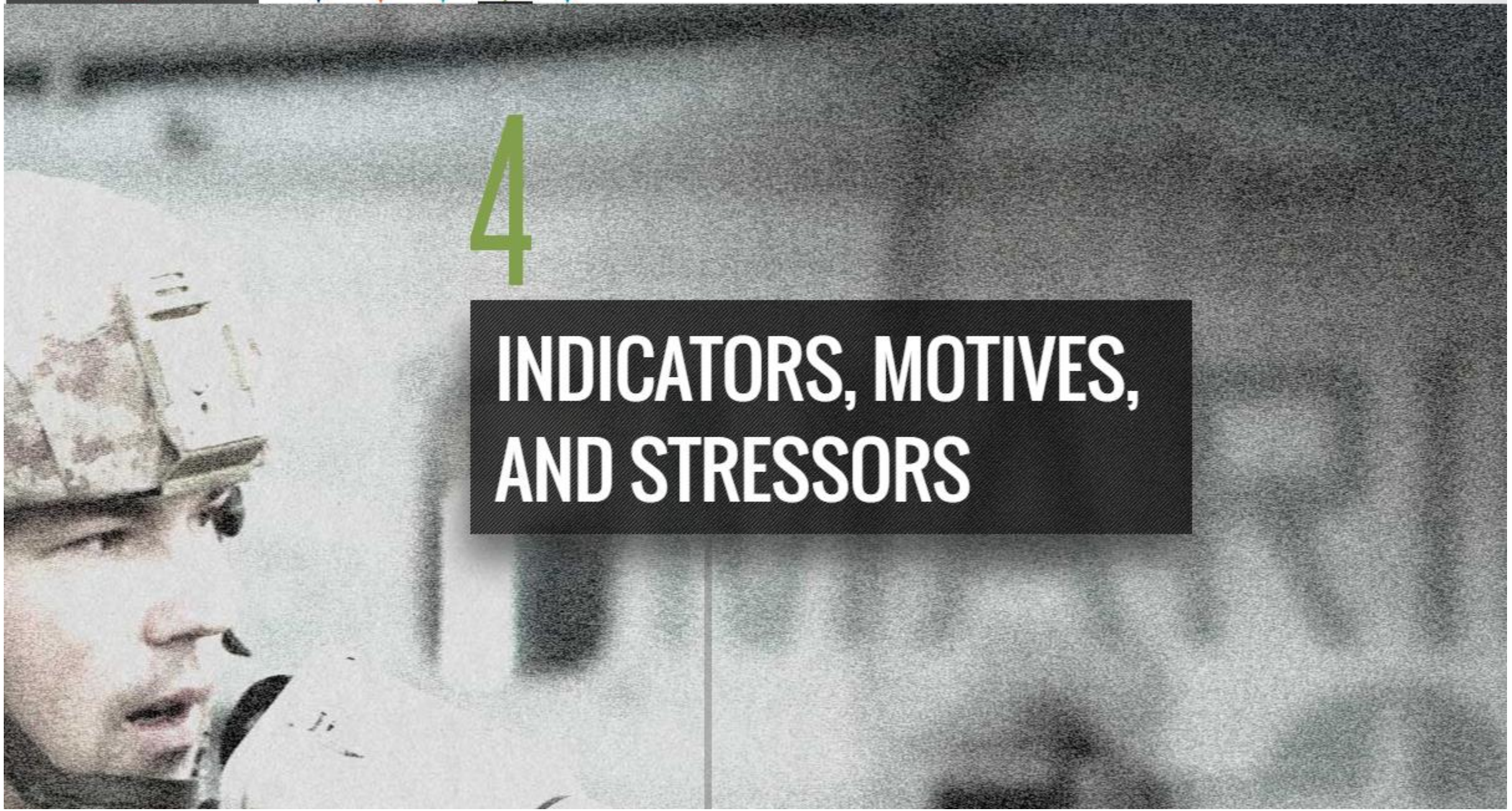
c. Sending deceiving emails

✔ **d. All of the above**

CORRECT!

The correct answer is **d**.

FIEs have numerous methods in which to extract information. Be careful not to overshare, don't talk shop in public, and be wary of unsolicited email.



4 INDICATORS, MOTIVES, AND STRESSORS

ESPIONAGE

THE KEY TO IDENTIFYING A POTENTIAL INSIDER THREAT IS PAYING ATTENTION TO A PERSON'S BEHAVIOR, INCLUDING VERBAL CUES.

Behavior will provide the most relevant information that a potential threat is evolving.

WHAT ARE THE KEY INDICATORS OF ESPIONAGE?

THERE ARE CERTAIN ACTIONS AND BEHAVIORS THAT MAY INDICATE SOMEONE IS CONSIDERING OR HAS ALREADY COMMITTED ESPIONAGE.

NOTE:

These are potential indicators. No single indicator necessarily constitutes evidence of espionage, terrorism, or any other unauthorized use of classified or protected information. **Each indicator has several possible explanations.** Therefore, single indicators often have limited significance.

REMEMBER:

Reporting indicators alert authorities that further inquiry **may be** appropriate to clarify the situation and determine if other concerns are present.

1 DISGRUNTLED

Displays signs of increased dissatisfaction with job, boss, or employer.

2 DIVIDED LOYALTIES

Personal or religious beliefs that conflict with assigned duties; this sometimes includes a desire to help the "underdog" or a particular cause.

THESE ARE ALL LOYALTIES THAT DO NOT BECOME A PROBLEM UNTIL THEY BECOME DIVIDED/CONFLICTING LOYALTIES.

Individuals may have multiple loyalties, including loyalty to:

- United States
- country of origin
- gangs
- people they grew up with
- religion
- political ideologies

3 UNAUTHORIZED REMOVAL

Takes classified documents, files, or folders from secured areas without permission.

4 SEEKING INFO

Makes inquiries to co-workers in other departments about sensitive or classified information unrelated to their current duties.

5 FOREIGN TRAVEL

Takes unscheduled, unexpected, unexplained, or unreported trips to foreign countries.

6 UNREPORTED CONTACTS

Has contact with a representative of a foreign government or an unreported close and continuing relationship with a foreign national.

PAST ESPIONAGE CASES

SHOW THAT CO-WORKERS AND SUPERVISORS OFTEN IGNORED OR FAILED TO REPORT INDICATORS.

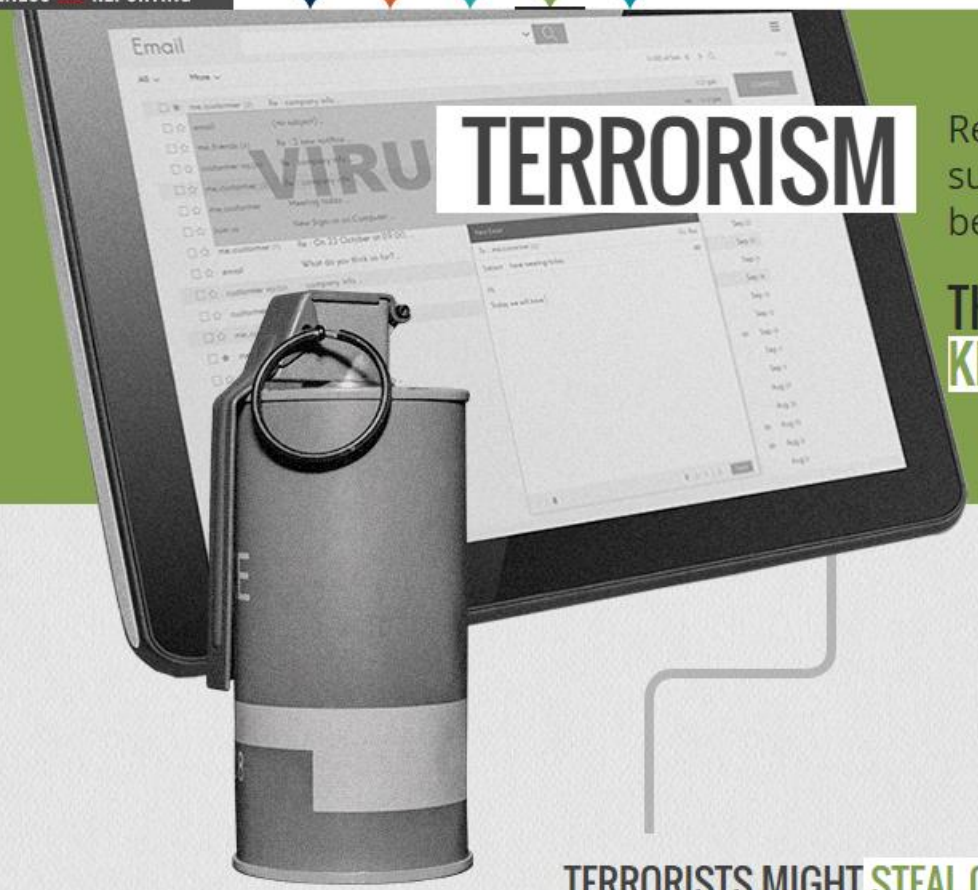
REPORTING

COULD HAVE PERMITTED EARLIER DETECTION AND MITIGATION OF THE INSIDER THREAT.

DID YOU KNOW?

WHAT ARE SOME OBSERVABLE BEHAVIORS OF SPIES?

- There is usually some personal contact with a foreign intelligence operative who recruits the insider or to whom the insider volunteers his/her service
- The insider must obtain information, which could include information to which the insider doesn't have normal or regular access. This information usually needs to be copied or emailed for removal from the office
- The insider must then communicate the information to the FIE. This often requires keeping or preparing materials at home and traveling to signal sites or secret meetings at unusual times and places
- The insider may receive large sums of money, which may then be deposited, spent, or hidden
- Periods of high stress sometimes affect the insider's behavior



TERRORISM

Research has shown that perpetrators and supporters of terrorism display common behaviors leading up to an attack.

THESE ARE CONSIDERED THE KEY INDICATORS OF TERRORISM.

TERRORISTS MIGHT STEAL OR COLLECT INFORMATION, SIMILAR TO A SPY.

This includes collecting or seeking information inconsistent with the person's hobbies or job requirements such as:

- Building, installation, or ship plans
- High-powered weapons
- Fraudulent identification documents

TERRORISTS ALSO ENGAGE IN SURVEILLANCE

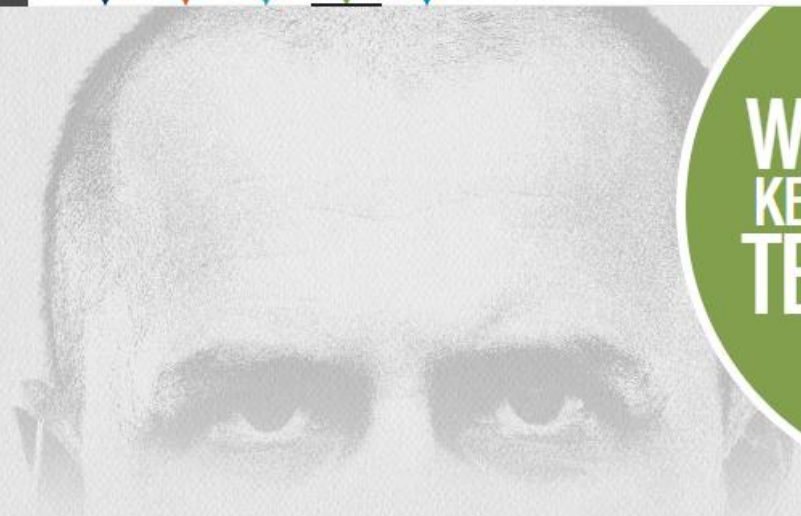
photography, videotaping, or note-taking on patterns of activities of potential targets, such as:

- High-value personnel
- Symbolic buildings and locations
- Large public gatherings

DID YOU KNOW?

INDIVIDUALS INVOLVED IN TERRORISM OR SUBVERSION ALSO ENGAGE IN OTHER OBSERVABLE BEHAVIORS

—planning, preparing, supporting, or executing some violent action.



WHAT ARE THE KEY INDICATORS OF TERRORISM?

1 MEMBERSHIP

Known membership in, or attempts to conceal membership in, any group that advocates force or violence to achieve political goals; has been identified as a front group for foreign interests; or advocates loyalty to a foreign interest instead of loyalty to the United States.

2 STATEMENTS

Makes statements in conversations, email, chat rooms, blogs, etc. in support of terrorism.

Verbal behaviors are just as important as physical ones and should be taken seriously and reported.

EXAMPLES OF TERRORIST STATEMENTS

- Intent to commit, or threaten to commit, a terrorist act, whether serious or supposedly as a "joke," and regardless of whether or not you think the person intends to carry out the action
- Support for suicide bombers even though they kill innocent bystanders
- Belief that the U.S. government is engaged in a crusade against Islam
- Talking knowingly about a future terrorist event, as though the person has inside information about what is going to happen
- Support for the militant jihadist ideology of holy war against the West
- Support for violence against U.S. military forces either at home or deployed abroad

KNOWLEDGEABLE EMPLOYEES WHO RECOGNIZE AND REPORT THESE BEHAVIORS/ACTIONS

play a significant role in helping to protect themselves and others against attacks and other subversive activities.

REMEMBER:

Although we often focus on radical Islam when discussing terrorism, terrorism and its indicators are about violence or the threat of violence as a means of intimidation and can be done on behalf of any ideology or cause—political, religious, etc.

3 INTERNET ACTIVITIES

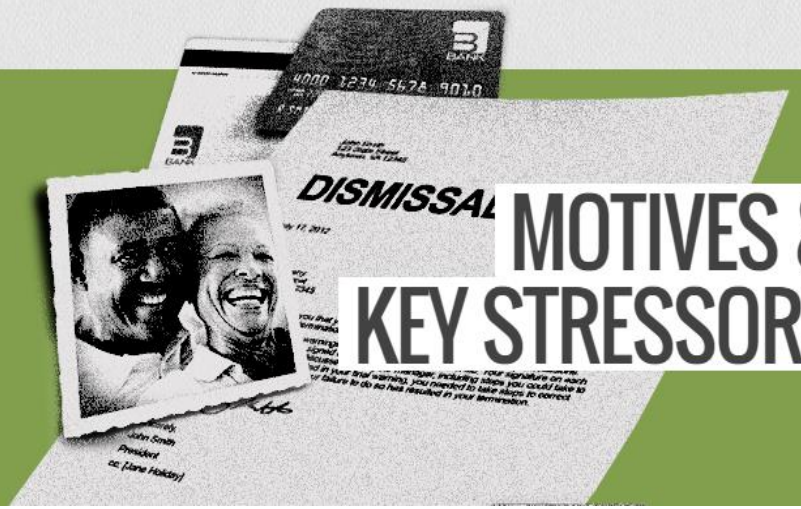
Frequently views websites that promote extremist or violent activities but access is not job-related.

4 WEAPONS THREATS

Makes statements about having or getting weapons or materials (including bombs), or about learning how to make such devices.

5 SEDITION

Advises, counsels, urges, or in any manner attempts to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the U.S. Armed Forces.



MOTIVES & KEY STRESSORS

STRESSORS, SITUATIONS OR CHARACTERISTICS MAY LEAD PEOPLE TO COMMIT ESPIONAGE OR ACTS OF VIOLENCE.

WHAT ARE SOME COMMON MOTIVES?

- **DIVIDED LOYALTIES:** Allegiance to another person or to a country besides the United States
- **DISGRUNTLED:** Obsessively angry at one's organization or co-workers/supervisors stemming from a perceived lack of recognition, dissatisfaction with the job, a pending layoff/disciplinary action
- **MONEY:** A belief that money can fix the problem (excessive debt or overwhelming expenses)
- **THRILLS:** Want to add excitement to their lives or are intrigued by clandestine activity
- **EGO:** An "above the rules" attitude, or desire to repair wounds and self-esteem
- **IDEOLOGY:** A desire to help the "underdog" or a particular cause

WHAT ARE THE KEY STRESSORS?

Crises could be positive or negative. Oftentimes, these events by themselves do not precipitate a crime. Rather, multiple events occurring all at once or in succession, along with opportunity, a motive, and personality characteristics, can lead individuals to engage in behaviors they might not otherwise consider.

STUDIES BASED ON INTERVIEWS WITH OFFENDERS SUGGEST A PATTERN IN WHICH PERSONAL DISRUPTIONS OR CRISES (STRESSORS) PRECEDE, OR "TRIGGER," AN INDIVIDUAL'S DECISION TO COMMIT ESPIONAGE OR ACTS OF VIOLENCE.

Regardless of mental health, anyone can be affected by emotionally charged events such as:

- Divorce/breakup
- Death of a loved one
- Money problems
- Relocation
- Medical problems
- Work problems

EMPLOYEE ASSISTANCE PROGRAMS

Recognizing a personal stressor that may seem too overwhelming to handle isn't easy. Knowing the available resources and using them when needed is courageous and shows your commitment to the service, your family, and yourself.

EMPLOYEE ASSISTANCE PROGRAMS ARE FREE AND CONFIDENTIAL. THEY CAN HELP YOU SOLVE PROBLEMS, ON AND OFF THE JOB.

Many offer 24/7 assistance with work, family, health, substance abuse, legal, and financial issues.

More information on EAP Programs can be found under the resource tab.

KNOWLEDGE CHECK

MODULE 4

Read each question and use the information you learned above to choose the best answer.

01

Not everyone is a viable target. The adversary evaluates prospective targets based on placement, access, and exploitable behaviors and characteristics.

✔ **a. True**

b. False

CORRECT!

The correct answer is **True**.

The adversary wants someone who:

- has access to information and the ability to collect the information
- can be exploited such as having close and continuous foreign contacts, financial issues, substance abuse, or overshares on social media
- commonly violates rules, acts without regard to consequences, are impulsive, or feels entitled.

5 THE MOST IMPORTANT STEP: REPORTING

WE'VE COVERED MANY OF THE REPORTABLE

CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS IN THIS TRAINING. DOD DIRECTIVE 5240.06 LISTS ALL 53 MANDATED REPORTING REQUIREMENTS.

IT IS YOUR RESPONSIBILITY

to read and understand all the items. A pamphlet is available on the NCIS website and the resource tab.

IF YOU WITNESS SOMETHING THAT DOESN'T SEEM RIGHT OR MAKES YOU UNCOMFORTABLE,

REPORT IT.

PENALTY

If you fail to report the information as directed by **DoDD 5240.06**, you may be subject to punitive action under **UCMJ Article 92**, which carries a maximum sentence of two years, or similar penalties according to civilian law.

WHEN SHOULD I REPORT FOREIGN CONTACTS & TRAVEL?

ALL PERSONNEL

You must report to NCIS any contact with a person, regardless of nationality, whether within or outside of the scope of your official activities, in which:

- Illegal or unauthorized access to classified or otherwise sensitive information is sought
- You suspect you may be the target of exploitation by a foreign entity

LET YOUR SECURITY MANAGER KNOW BEFORE YOU GO AND INFORM THEM OF ANY NEW FOREIGN FRIENDS AND ASSOCIATES.

PERSONNEL WITH A SECURITY CLEARANCE

If you have a security clearance, (Confidential, Secret, or Top Secret), you must report the following to your security manager:

- Any foreign connections, including those in your immediate family, a cohabitant, or other persons to whom you are bound by affection or obligation, who are not U.S. citizens
- Any financial interest in a foreign country
- All personal foreign travel as part of your required periodic reinvestigation

PERSONNEL WITH ADDITIONAL ACCESS

CONTACT YOUR SSO FOR YOUR SPECIAL ACCESS PROGRAM'S SPECIFIC REPORTING REQUIREMENTS.

If you have special access, such as CPI, SCI, and SAP, the additional reporting responsibilities include:

- Reporting all planned official and unofficial foreign travel
- Reporting all foreign contacts that are close and continuing

HOW DO I FILE A REPORT WITH NCIS?

Reporting is simple and methods are available 24/7:

- Contact your local NCIS Office
- www.ncis.navy.mil
- Text "NCIS" + your tip info to CRIMES (274637)
- "Tip Submit" Android and iPhone App (select NCIS as the Agency)
- Call 1.800.543.NAVY (6289)

WEB, TEXT, & SMARTPHONE REPORTING IS ANONYMOUS.

IF YOU CANNOT REPORT TO NCIS, NOTIFY YOUR SECURITY OFFICER, SUPERVISOR, OR COMMAND. PER DODD 5240.06, THEY ARE REQUIRED TO NOTIFY NCIS WITHIN 72 HOURS.

DID YOU KNOW?

NCIS MAY PAY REWARDS

UP TO $5,000 FOR INFORMATION

leading to a felony arrest or the
prevention of certain felony crimes.

IT'S UP TO YOU

YOU ARE THE FIRST
LINE OF DEFENSE

KNOWLEDGE CHECK

MODULE 5

Read each question and use the information you learned above to choose the best answer.

01

You can identify a potential insider threat by paying attention to a person's behavior and verbal cues.

- ✔ a. True
- b. False

CORRECT!

The correct answer is **True**.

Behavior will provide the most relevant information that a potential threat is evolving. Know the signs.

02

Many individuals who exhibited violent behavior or participated in espionage had experienced a key stressor within a few months of the act.

- ✔ a. True
- b. False

CORRECT!

The correct answer is **True**.

Studies based on interviews with offenders suggest a pattern in which personal disruptions or crises (stressors) precede, or "trigger," an individual's decision to commit espionage or acts of violence.

Employee Assistance Programs can help solve problems on and off the job. Many offer 24/7 assistance with work, family, health, substance abuse, legal, and financial issues.

CONGRATULATIONS!

YOU HAVE COMPLETED THE DEPARTMENT OF THE NAVY'S

COUNTERINTELLIGENCE AND INSIDER THREAT AWARENESS AND REPORTING TRAINING.