



NCIS
CI & INSIDER THREAT
AWARENESS *AND* REPORTING BRIEF

VERSION 2

1.800.543.6289

NCIS.NAVY.MIL

TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)

CI & INSIDER THREAT
AWARENESS *AND* REPORTING BRIEF



INSIDER

| THREAT

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.

INSIDER

| *THREAT*

INSIDER THREAT: THE DEFINITION

INSIDER WHO USES HIS/HER ACCESS WITTINGLY OR UNWITTINGLY TO HARM NATIONAL SECURITY INTERESTS OR NATIONAL SECURITY THROUGH:

- ▶ unauthorized disclosure
 - ▶ data modification
 - ▶ espionage
 - ▶ terrorism
- ▶ kinetic actions resulting in loss or degradation of resources, to include:
 - ▶ personnel
 - ▶ facilities
 - ▶ information
 - ▶ equipment
 - ▶ networks or systems
 - ▶ capabilities

2

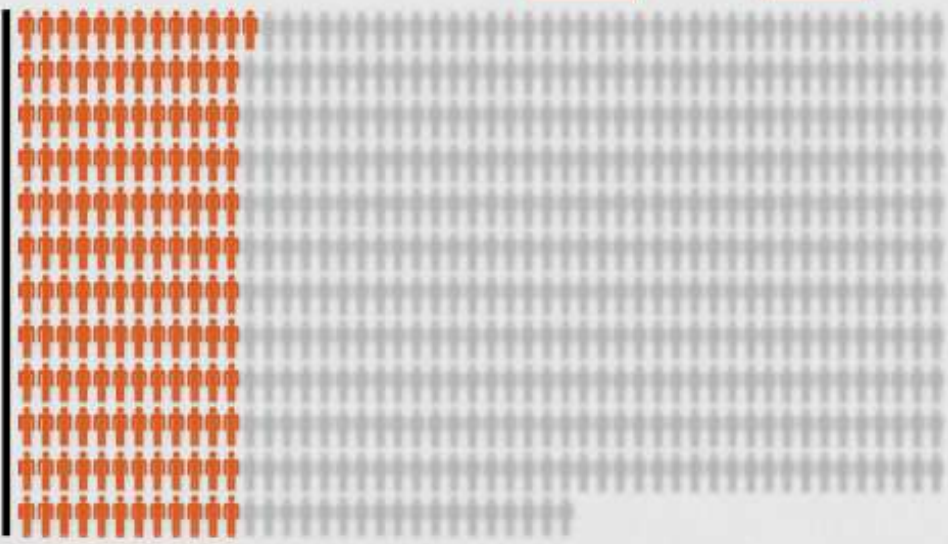
THE THREAT



2 THE THREAT

580 PEOPLE HAVE BEEN CHARGED WITH ESPIONAGE BETWEEN 1945 AND 2016.

NEARLY
1/4
SINCE 2008



TYPES OF THREATS

FACT:

ADVERSARIES
COLLECT SMALL PIECES
OF INFORMATION.

WHEN COMBINED,
THEY CAN REVEAL

THE WHOLE PICTURE

Source // Interagency OPSEC Support Staff,
Intelligence Threat Handbook



FOREIGN INTELLIGENCE ENTITY

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 and security services, international terrorist organizations, organized crime groups, and drug cartels.

BACK
TO MENU

TYPES OF THREATS

FACT :

MORE THAN 70%
of those convicted of
espionage were citizens
born in the United States.



Source // CI Centre: Citizenship of Individuals
Identified in Espionage Related Cases, 1949-2018



FILE: 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 nation.

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

TYPES OF THREATS

FACT:



MORE THAN 50%
of terrorist attack victims worldwide are **civilians**.

Source // 2010 FBI report



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

TYPES OF THREATS

FACT :

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



AND HAVE "ORDINARY"
LIVES, JOBS, AND LITTLE,
IF ANY, CRIMINAL HISTORY.

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



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.

Self-radicalization can lead to acts of terrorism and workplace violence.

TYPES OF THREATS

FACT:

AN INTERNET POSTING BY A TERRORIST GROUP IN 2009 DIRECTED THEIR FOLLOWERS TO COMB THROUGH



SOCIAL NETWORKING SITES

TO LOOK FOR DETAILS ABOUT SERVICE MEMBERS AND THEIR FAMILIES.

Source // Defense Personnel Security Research Center (PERSEREC), "Changes in Espionage by Americans: 1947-2007"



INADVERTENT

"Loose tweets sink fleets." One does not have to intend harm to create a threat. Lack of OPSEC in monitoring social media sites can lead to non-intentional disclosures.

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

TYPES OF THREATS

FACT:



Between 2011-2014,
1,756 PEOPLE WERE KILLED
in the U.S. as a result of
workplace violence.

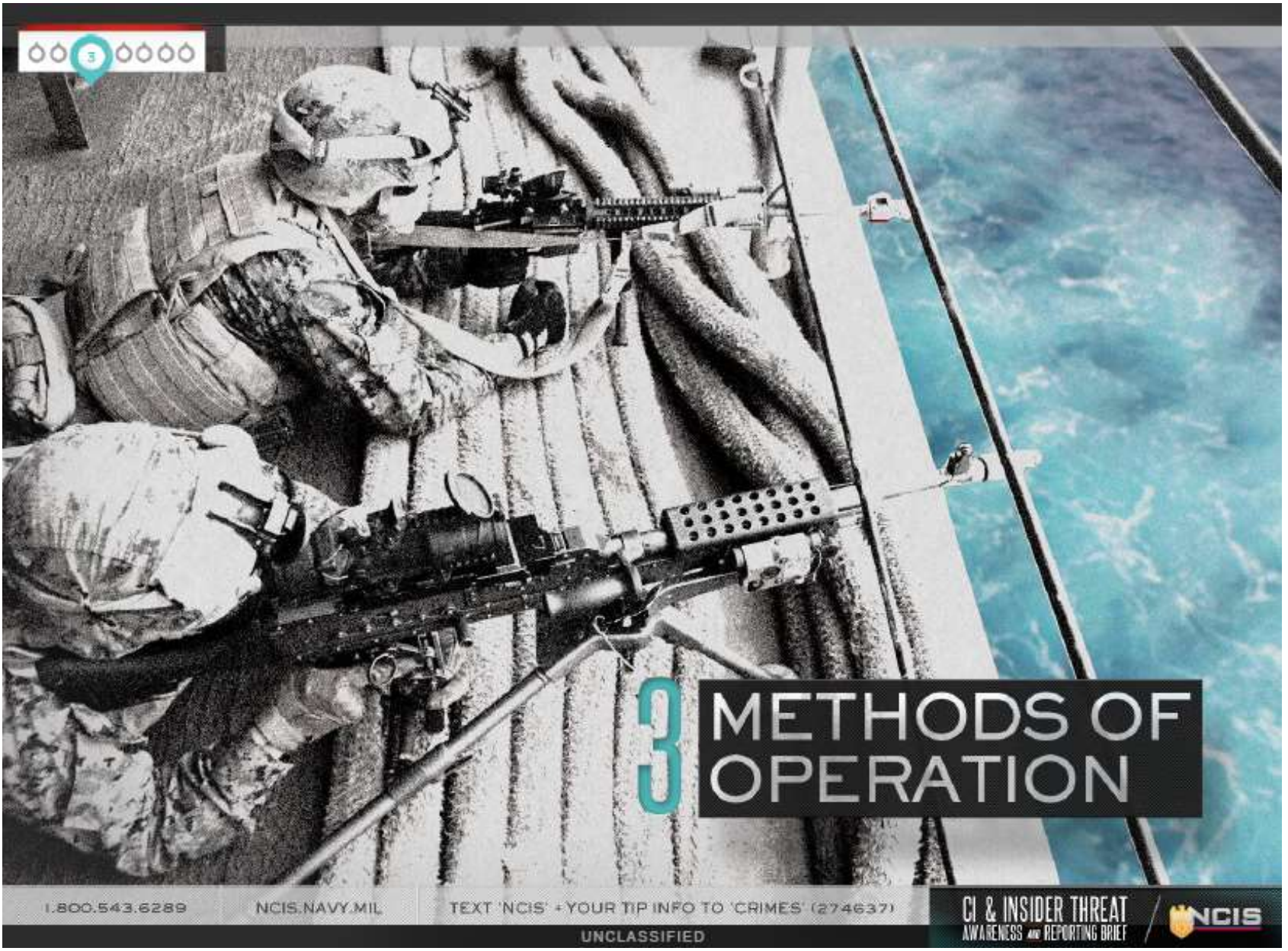
Source // Bureau of Labor Statistics (BLS),
"Workplace Homicides by Selected
Characteristics, 2011-2014"



WORKPLACE VIOLENCE

Motivations:

- Seeking revenge or justice
- Gain notoriety
- Bring attention to or solve a problem
- End pain or suffering
- Gain control
- Advance one's own belief system



3 METHODS OF OPERATION

3 METHODS OF OPERATION



“USING PUBLIC RESOURCES OPENLY & WITHOUT RESORTING TO ILLEGAL MEANS, IT IS POSSIBLE TO GATHER AT LEAST **80%** OF INFORMATION NEEDED ABOUT THE ENEMY.”

Source // Al Qaeda Handbook



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OPEN SOURCE

▶ HOW IT'S USED

▶ THE ADVERSARY'S GOAL

▶ PROTECT YOUR INFO

- Publicly available information from:
 - Newspapers and blogs
 - Media and photographs
 - Maps and Google searches
 - Social media and apps
- Captured via unsecure networks or in public places



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OPEN SOURCE

▶ HOW IT'S USED

▶ THE ADVERSARY'S GOAL

▶ PROTECT YOUR INFO

- Provide information about personal interests, preferences, 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



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OPEN SOURCE

- ▶ HOW IT'S USED
- ▶ THE ADVERSARY'S GOAL
- ▶ PROTECT YOUR INFO

Aggregated Information

- A customized picture used to:
 - Target you
 - Exploit your vulnerabilities
 - Recruit you
 - Gather intelligence





OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OPEN SOURCE

- ▶ HOW IT'S USED
- ▶ THE ADVERSARY'S GOAL
- ▶ PROTECT YOUR INFO

- Don't address private information on public networks
- Actively manage privacy settings and update policies and other software
- Be wary of people you meet online
- Respond to or open attachments from unknown senders
 - Unusual network behavior
- Limit the use of professional networks for personal business
 - Suspicious online interactions






OPEN SOURCES


ELICITATION


EAVESDROPPING


RECRUITMENT


TRADITIONAL METHODS

ELICITATION


- ▶ WHY IT WORKS
- ▶ THE ADVERSARY'S M.O.
- ▶ A SUBTLE DEFENSE

- GET you talking and KEEP you talking
- 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
- Operates under the guise of think tanks, exchange students, research organizations, foreign liaison officers, and official delegations






OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

- ▶ WHY IT WORKS
- ▶ THE ADVERSARY'S M.O.
- ▶ A SUBTLE DEFENSE

- Nonthreatening: Hard to recognize and easy to deny

- Easy to disguise: Seems like innocent conversation

- We're human: Exploits fundamental aspects of human nature. In general, we aspire to:
 - Be polite and helpful
 - Appear well-informed
 - Be appreciated
 - Trust others



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

▶ WHY IT WORKS

▶ THE ADVERSARY'S M.O.

▶ A SUBTLE DEFENSE

- Flattery/appeal to ego: Asks your opinion or values your insights
- Quid pro quo: Shares information with you in hopes you'll reciprocate
- Mutual interest: Focuses on details you have in common



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

▶ WHY IT WORKS

▶ THE ADVERSARY'S M.O.

▶ A SUBTLE DEFENSE

- 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



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

EAVESDROPPING, ELECTRONIC SURVEILLANCE

- Operative positioned within earshot of a conversation or within view of a computer screen
- Communications intercepted when devices are connected to public Wi-Fi, unsecured networks, or unencrypted email systems



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

RECRUITMENT

- Build personal relationship and gain trust, little by little
- Exploit personal weakness or circumstances
- Coerce or use inducements
- Start with small requests, then make bigger demands
- Praise and reward for accomplishments

4

WHAT MAKES YOU A TARGET?

WHAT MAKES YOU A TARGET?



ASK YOURSELF...

Circumstances

Do I have access to information or the means to acquire it?

Behaviors

Does my behavior make me stand out to adversaries?

Characteristics

Do I have personality characteristics that could be manipulated?

○○○ 4 ○○○

WHAT MAKES YOU A TARGET?



BULLSEYE!

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

CIRCUMSTANCES | *BEYOND YOUR CONTROL*



PLACEMENT

ACCESS

CULTURE

Where you're stationed or travel for work.



CIRCUMSTANCES | *BEYOND YOUR CONTROL*



PLACEMENT

ACCESS

CULTURE



The nature of the information you have access to.

CIRCUMSTANCES | *BEYOND YOUR CONTROL*



PLACEMENT

ACCESS

CULTURE

Your culture, ethnicity,
and background.



BEHAVIORS THAT ATTRACT

FIES, TERRORISTS, & OTHER ADVERSARIES



PERSONAL RELATIONSHIPS

Interactions with foreigners—especially close, ongoing relationships—can be viewed by an outsider as an opportunity.

BEHAVIORS THAT ATTRACT

FIES, TERRORISTS, & OTHER ADVERSARIES



PARTICULAR BEHAVIORS

Illegal, immoral, unethical, or embarrassing behavior may be seen as a willingness to participate in unlawful activities—and could open the door for blackmail.

BEHAVIORS

THAT ATTRACT

FIES, TERRORISTS, & OTHER ADVERSARIES



POLICY DISAGREEMENT

Open disapproval of U.S. policies could be a sign that you sympathize with anti-American sentiments or philosophies, or with the actions of foreign entities.

BEHAVIORS

THAT ATTRACT

FIES, TERRORISTS, & OTHER ADVERSARIES



GRIEVANCES WITH SUPERIORS

When you're openly disgruntled with your employer, you could be targeted by outsiders and encouraged to act against your organization.

BEHAVIORS THAT ATTRACT

FIES, TERRORISTS, & OTHER ADVERSARIES



SUBSTANCE ABUSE

If you're addicted to or abusing drugs or alcohol, your decision-making ability is impaired, making you more susceptible to recruitment.

CHARACTERISTICS

OF TARGETS



ANTISOCIAL

Has a propensity for violating commonly accepted rules and regulations, patterns of lying, misrepresentation, gross exaggeration.

Takes pleasure in beating the system and not getting caught.

CHARACTERISTICS OF TARGETS



NARCISSISTIC

Views the world from the perspective of
“How does this affect me?”

Treats others as objects to be manipulated
for personal benefit.

CHARACTERISTICS OF TARGETS



IMPULSIVE

Does whatever feels good or is thrilling at the moment without regard for short- and/or long-term consequences.



CHARACTERISTICS

OF TARGETS

PARANOID

Has a pervasive mistrust of others that could lead to viewing the government or an employer as the enemy.

CHARACTERISTICS OF TARGETS



ENTITLED

Believes oneself to inherently deserving of privileges or especially favorable treatment.

CHARACTERISTICS OF TARGETS



VINDICTIVE

Has a preoccupation with getting revenge for real or imagined wrongs.

WHAT INDICATORS SHOULD YOU LOOK FOR?

WHAT INDICATORS SHOULD YOU LOOK FOR?

1/3 

OF CONVICTED U.S. SPIES EXPERIENCED ONE OR MORE REPORTABLE LIFE EVENTS, POSITIVE OR NEGATIVE,  6-8 MONTHS BEFORE ATTEMPTING ESPIONAGE.

Source // Defense Personnel Security Research Center (PERSEREC), *Changes in Espionage by Americans: 1947-2007*

KEY INDICATORS OF ESPIONAGE



DISGRUNTLED

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

DIVIDED LOYALTIES

UNAUTHORIZED REMOVAL

UNAUTHORIZED DEVICES

KEY INDICATORS OF ESPIONAGE



DIVIDED LOYALTIES

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

UNAL WORKING ODD HOURS

UNAUTHORIZED DEVICES

SEEKING INFO

KEY INDICATORS OF ESPIONAGE



WORKING ODD HOURS

Shows up uncharacteristically early or stays unusually late

UNAL UNAUTHORIZED REMOVAL

NEED TO KNOW

SEEKING INFO

KEY INDICATORS OF ESPIONAGE



UNAUTHORIZED REMOVAL

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

UNAUTHORIZED DEVICES

SEEKING INFO

COPIING MATERIAL

KEY INDICATORS OF ESPIONAGE



UNAUTHORIZED DEVICES

“Mistakenly” brings items such as smartphones or USB drives into secure areas

NO NEED-TO-KNOW

SEEKING INFO

COPIING MATERIAL

KEY INDICATORS OF ESPIONAGE



NO NEED-TO-KNOW

Possesses or researches materials or information unrelated to their job, role, or duties

- UNN
- SEEKING INFO
- NEW WEALTH
- BRAGGING
- ...

KEY INDICATORS OF ESPIONAGE



SEEKING INFO

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

UNNECESSARY COPYING

DRAGGING

FORGETS/LEAVES

KEY INDICATORS OF ESPIONAGE



UNNECESSARY COPYING

Photocopies documents excessively or burns an inordinate number of files to CDs

UNEXPLAINED AFFLUENCE

FOREIGN TRAVEL

UNREPORTED CONTACTS

KEY INDICATORS OF ESPIONAGE



UNEXPLAINED AFFLUENCE

Makes purchases that appear to be “beyond their means”

BRAGGING

FOREIGN TRAVEL

KEY INDICATORS OF ESPIONAGE



BRAGGING

Talks excessively about work and what they know in mixed company

UNRI

FOREIGN TRAVEL

KEY INDICATORS OF ESPIONAGE



FOREIGN TRAVEL

UNREPORTED CONTACTS

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

KEY INDICATORS OF ESPIONAGE



UNREPORTED CONTACTS

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



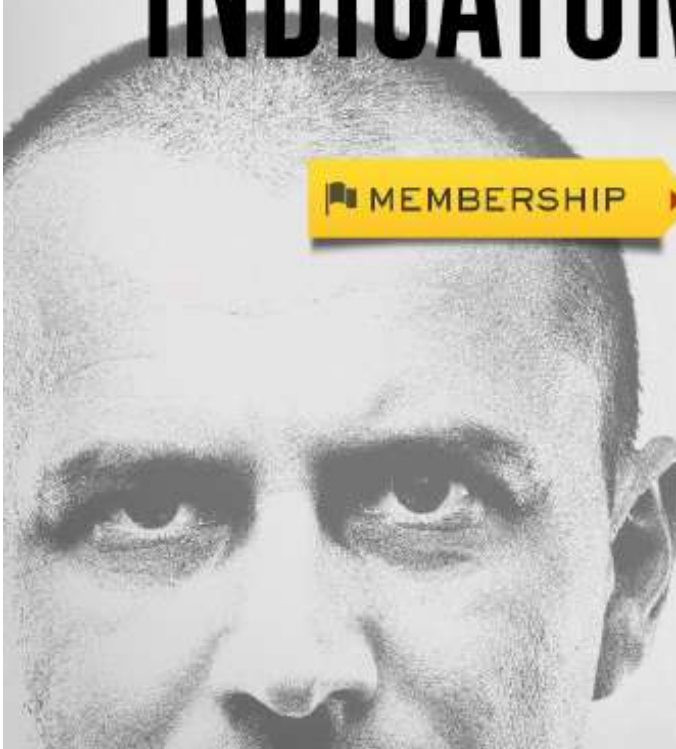
KEY

INDICATORS OF TERRORISM

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





KEY

INDICATORS OF TERRORISM

 STATEMENTS

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



KEY

INDICATORS OF TERRORISM



PUBLICATIONS

Possesses or distributes publications prepared by a person or group that advocates violence, foreign loyalties, or is known to be a front for a foreign interest



KEY

INDICATORS OF TERRORISM



INTERNET
ACTIVITIES

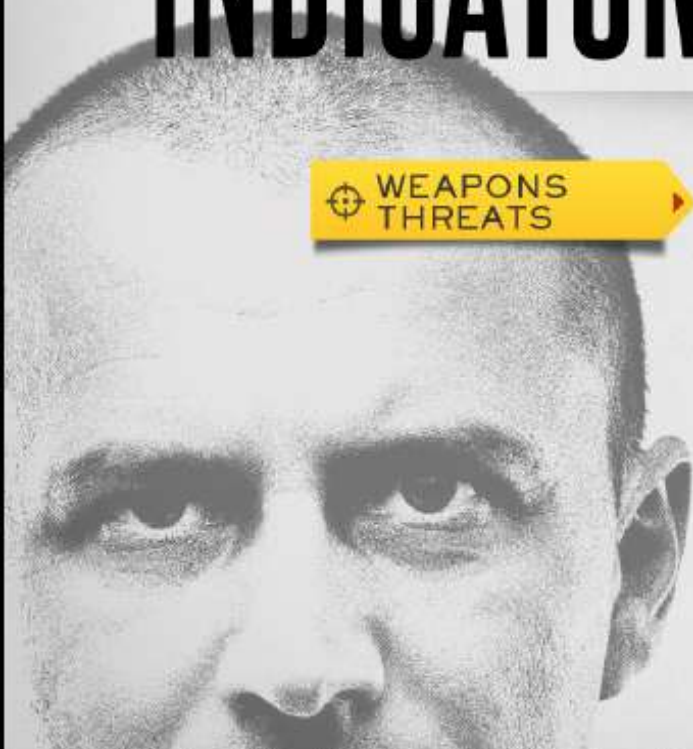
Frequently views websites that promote extremist or violent activities but access is not job-related



KEY INDICATORS OF TERRORISM

 WEAPONS THREATS

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





KEY

INDICATORS OF TERRORISM



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

KEY STRESSORS

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

KEY STRESSORS

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.



6

THE MOST IMPORTANT STEP: REPORTING

WHAT TO REPORT

While we've covered many of the reportable contacts, activities, indicators, and behaviors in this presentation, [DoDD 5240.06](#) lists all 53 mandated reporting requirements.

For an easy reference on reporting requirements, go to:

www.ncis.navy.mil "Counterintelligence"

PUNISHMENT

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.

REPORTING FOREIGN CONTACT & TRAVEL



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

REPORTING FOREIGN CONTACT & TRAVEL



ALL PERSONNEL

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

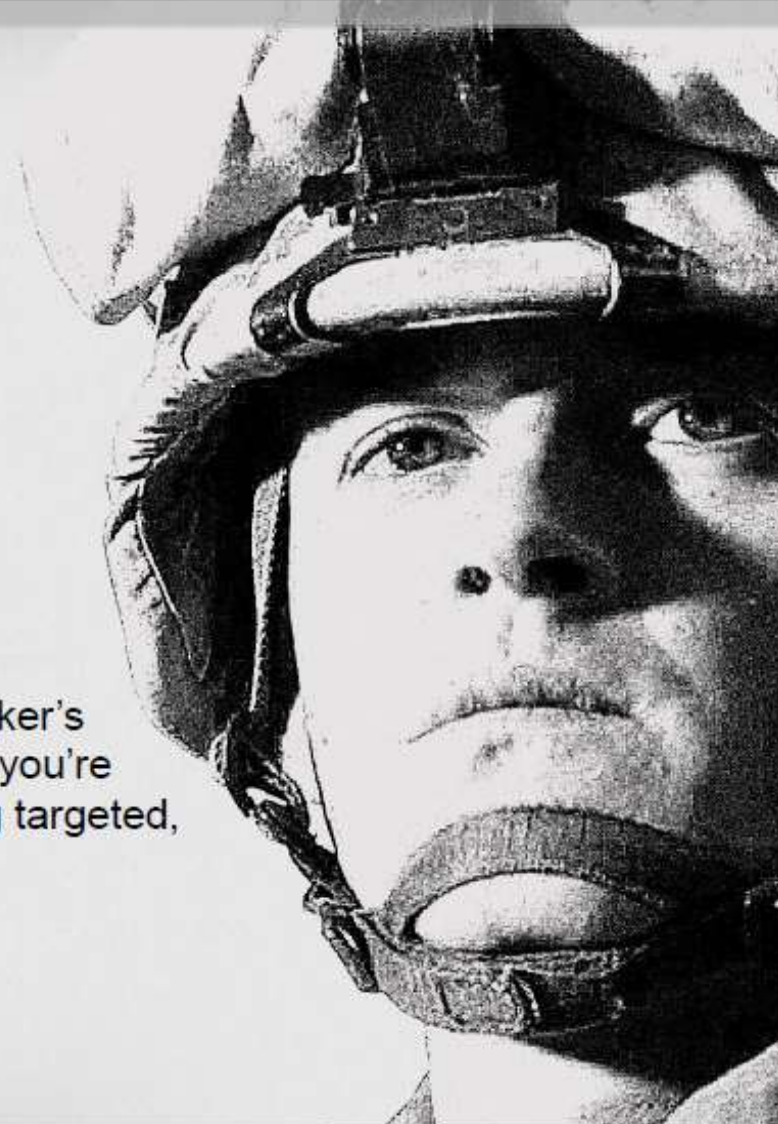
- Illegal or unauthorized access to classified or otherwise sensitive information is sought;
- You suspect you may be the target of exploitation by a foreign entity.

THE PROCESS OF REPORTING

THE INDICATOR

INDICATOR

You've noticed a coworker's reportable behavior, or you're concerned you're being targeted, exploited, or coerced.





REPORT FILED WITH NCIS


THE PROCESS OF REPORTING





Reporting is simple and methods are available 24/7:

-  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)

-  1.800.543.NAVY (6289)

Web, text, and 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.

NCIS may pay rewards up to \$5,000 for information leading to a felony arrest or the prevention of certain felony crimes.