9LINE★LLC

INSIDER THREAT PROGRAM (ITP) 2024

Cleared and Uncleared Employee Training

Agenda

- Fundamentals of the Insider Threat Program (ITP)
- Establishing an ITP
- ITP Definitions
- Insider Threat Impact on Industry
- ITP Training Requirement

Insider Threat Program Fundamentals What to implement immediately

- Implement a ITP plan.
- Establish an insider threat program that will identify and report suspicious activities or threats
- Designate a senior contractor official
- Train ITP designated and all cleared employees
- Implement classified networks monitoring
- Maintain ITP records

Establishing an Insider Threat Program Senior Official

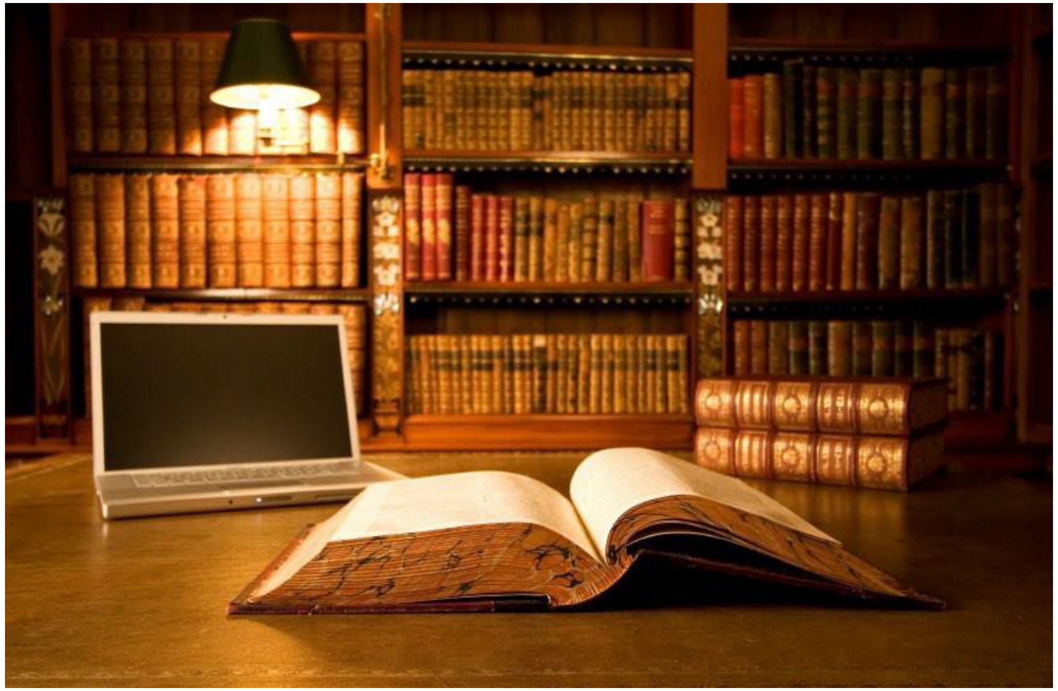
Cleared defense contractors must integrate an insider threat program. The first step is to designate a “Senior Official” to *establish and execute* the insider threat program

- U.S. citizen
- Employee
- Senior official
- Security Clearance at the same level as the facility clearance to establish and execute an insider threat program
- If FSO is not the designated official, the FSO is an integral member of the program

Establishing an Insider Threat Program
Insider Threat Program Requirements

Insider Threat Program-Develop awareness of and respond to information indicative of potential or actual insiders threats. ITP Goals:

- Gather information
- Integrate gathered information
- Report relevant and available information per:
  - Executive Order (EO) 13587 - directs the heads of agencies that operate or access classified computer networks
  - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
  - And the catchall; as required by the appropriate CSA (DSS)



Establishing an Insider Threat Program
ITP Training Requirements

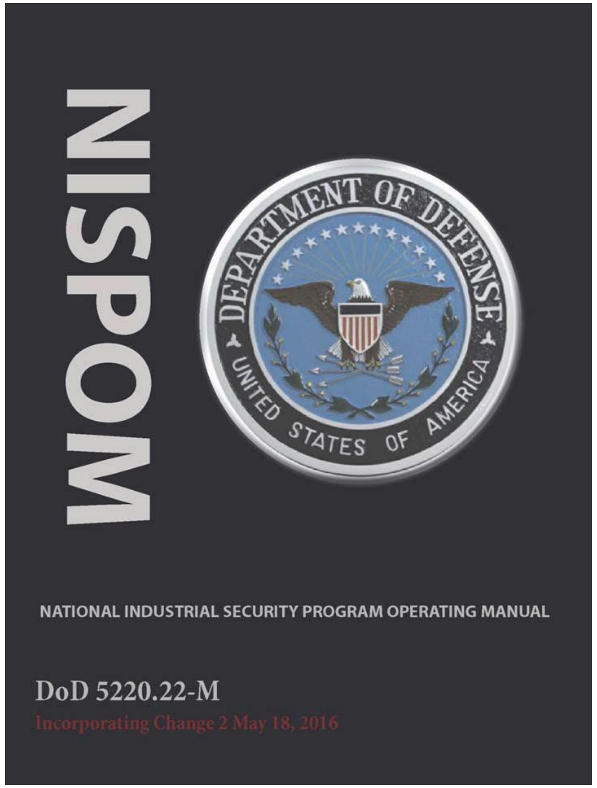
Insider threat program should execute the following:

- Training:
    - cleared employees (initial security briefing and follow-up briefings)
    - cleared employees assigned insider threat program responsibilities
    - 9Line also trains all un-cleared employees

Establishing an Insider Threat Program
What a Successful ITP Looks Like

The NISPOM has identified the following requirements to establish an Insider Threat Program:

- Designate an Insider Threat senior official
- Establish an Insider Threat Program / Self-certify the Implementation Plan in writing to DSS.
- Establish an Insider Threat Program group
- Provide Insider Threat training
- Monitor classified network activity
- Gather, integrate, and report relevant and credible information; detect insiders posing risk to classified information; and mitigate insider threat risk
- Conduct self-inspections of Insider Threat Programs


NISPOM

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL

DoD 5220.22-M

Incorporating Change 2 May 18, 2016

ITP Definitions

Insider - Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

- Authorized
- Security clearance
- Need to Know

ITP Definitions

Insider Threat - The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States.

Because of the authorized access to classified information an insider can cause accidental and malicious damage to national security that may not otherwise be easily detected.

The ITP should be designed to deny, detect, deter and report insider threat information

Insider threats may include:

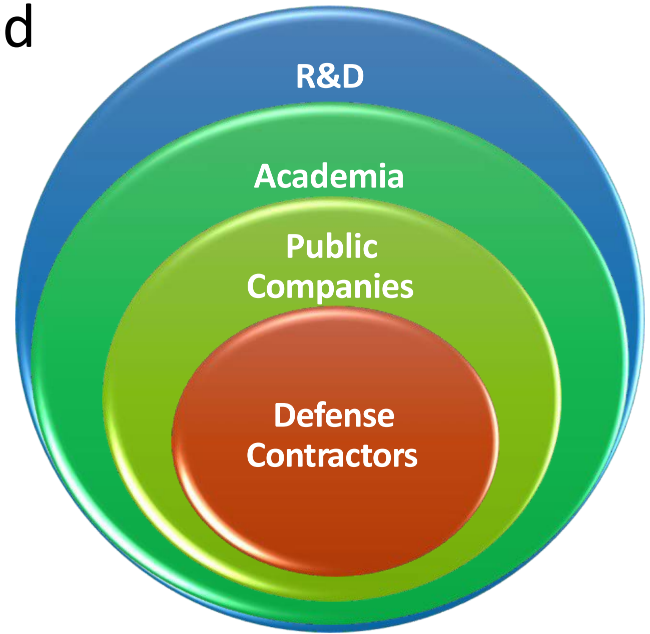
- Harm to contractor
- Harm to program information
- Insider threats impact the contractor or agency's obligations to protect classified national security information

For the purposes of this briefing the Insider threat focuses on threat to national security

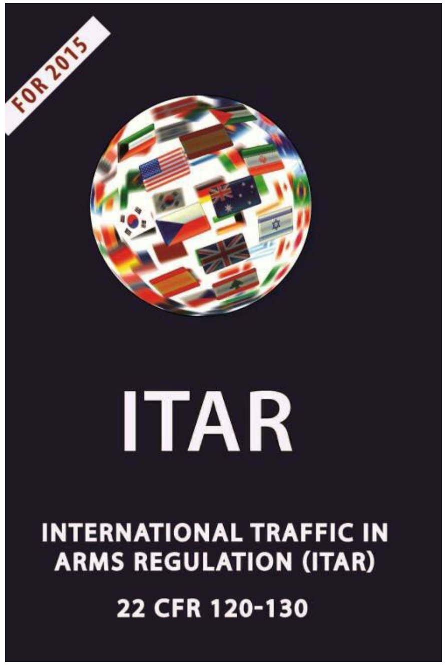
Insider Threat Action
Impact on Industry

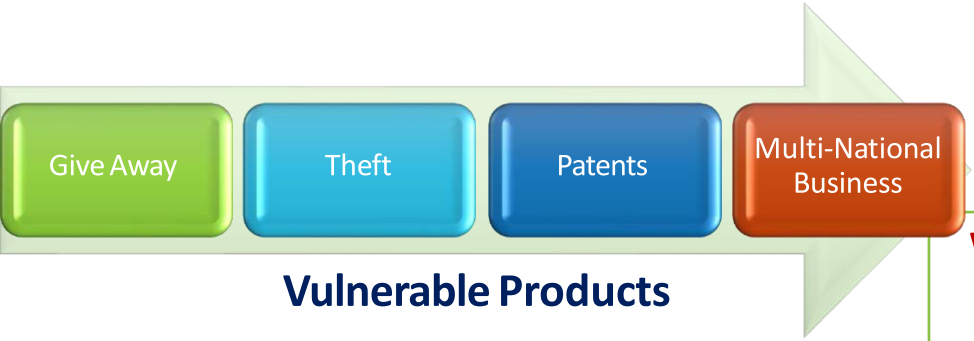
An insider can have a negative impact on national security and industry resulting in:

- Loss or compromise of classified, export-controlled, or proprietary information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Loss of life



Vulnerable Industries





Vulnerable Products

When foreign governments counter or copy U.S. technology they could erode enhanced military capability

Insider Threat Training Requirement

According to NISPOM 3-107, Insider threat reporting is a new training requirement for cleared employees PRIOR to gaining access to classified information.

- A threat awareness security briefing, including insider threat awareness in accordance with paragraph 3-103b of this Man
- A counterintelligence awareness briefing.
- An overview of the security classification system.
- Employee reporting obligations and requirements, *including insider threat*.
- Initial and annual refresher cybersecurity awareness training for all authorized IS users (see chapter 8, paragraph 8-101c, this Manual).
- Security procedures and duties applicable to the employee's job.

Insider Threat Training Requirement Employees with Insider Threat Program Duties

Employees with Insider Threat Program Duties must be trained in:

- Counterintelligence and security fundamentals
- Procedures for conducting insider threat response actions
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable legal, civil liberties, and privacy policies.

Insider Threat Training Requirement
Training for All Cleared Employees

Requirements PRIOR to the recent changes to NISPOM:

- The FSO provided initial security training and annual refresher training
- The holder of classified information validated an employee’s access (clearance level) and need to know

<u>ADDITIONAL</u> Requirements <u>AFTER</u> the NISPOM updates:

- The FSO demonstrates that cleared employees have completed ITP awareness training before being granted access to classified information, and annually thereafter

ITP training can be conducted in concert with existing training or stand alone

The remainder of this presentation addresses the IPT “all cleared employee” training requirement

Insider Threat Training Requirement
Cleared Employees

Required Training Topics.

This insider threat training will address current and potential threats in the work and personal environment and includes:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee
- Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs
- Indicators of insider threat behavior, and procedures to report such behavior
- Counterintelligence and security reporting requirements, as applicable

Required Topics
Detecting Suspected Activity

Protecting classified information has always required reporting suspicious activity.

This requirement now specifies potential threats to national security from trusted employees.

Be alert to cleared employee behavior that could jeopardize classified information under their care.

Required Topics

Methodologies of Adversaries to Recruit Trusted Insiders

Methodologies to collect classified information, in particular within information systems

- Elicitation
- Eavesdropping
  - Electronic-Computers, directional microphone, bugging, etc.
  - Visual-reading lips, reading over shoulder, binoculars, etc.
  - Personal-overhearing conversations, listening outside of meetings, attending meetings under false pretences

Required Topics

Methodologies of Adversaries to Recruit Trusted Insiders

Methodologies to collect classified information, within information systems

- Surveillance-observation, studying work habits, developing target behaviors, developing plan
- Theft-stealing, hacking, robbing
- Interception-hacking, posing as authorized recipient

Methodologies of Adversaries to Recruit Trusted Insiders Technology Based

Adversaries Target technology and focus on stealing or sabotaging technology

- Don’t have to expend Research and Development resources
  - Let someone else pay for research and development
  - Possible military application
- Prevent US advanced capability efforts
  - If adversary can’t develop technology, they can prevent US capability advancement through sabotage

Methodologies of Adversaries to Recruit Trusted Insiders

Why Our Technology?

- Research and development is an expensive endeavor. It is much cheaper to acquire technology through reverse engineering, requests for information or theft

- While it is illegal to provide any export to some countries; adversaries may try to circumvent laws with implementing creative methods of obtaining what they need.

- Some products seem to have commercial application, but they may appeal to a dual use possibilities

Methodologies of Adversaries to Recruit Trusted Insiders

Potential Non-Classified Information Targets

- vendor prices
- personnel ratings
- medical records
- corporate financial investments and resources
- trade secret information
- corporate/government relations
- corporate security vulnerabilities
- financial forecasts and budget information

Intellectual property, Proprietary information, FOUO, ITAR controlled, etc.

Methodologies of Adversaries to Recruit Trusted Insiders Classified Information

Classified Information:

- TOP SECRET
- SECRET
- CONFIDENTIAL

Methodologies of Adversaries to Recruit Trusted Insiders
Protect All Sensitive Classified and Non-Classified Information

Classified Information

- GSA approved container
- Vault
- SCIF

UNCLASSIFIED

- Restrict emailing or faxing
- Develop a destruction policy
- Everyone has a right to privacy, respect that right
- Protect your business to the fullest

Enforce Need to Know

Review Information Before Releasing It
What to Review

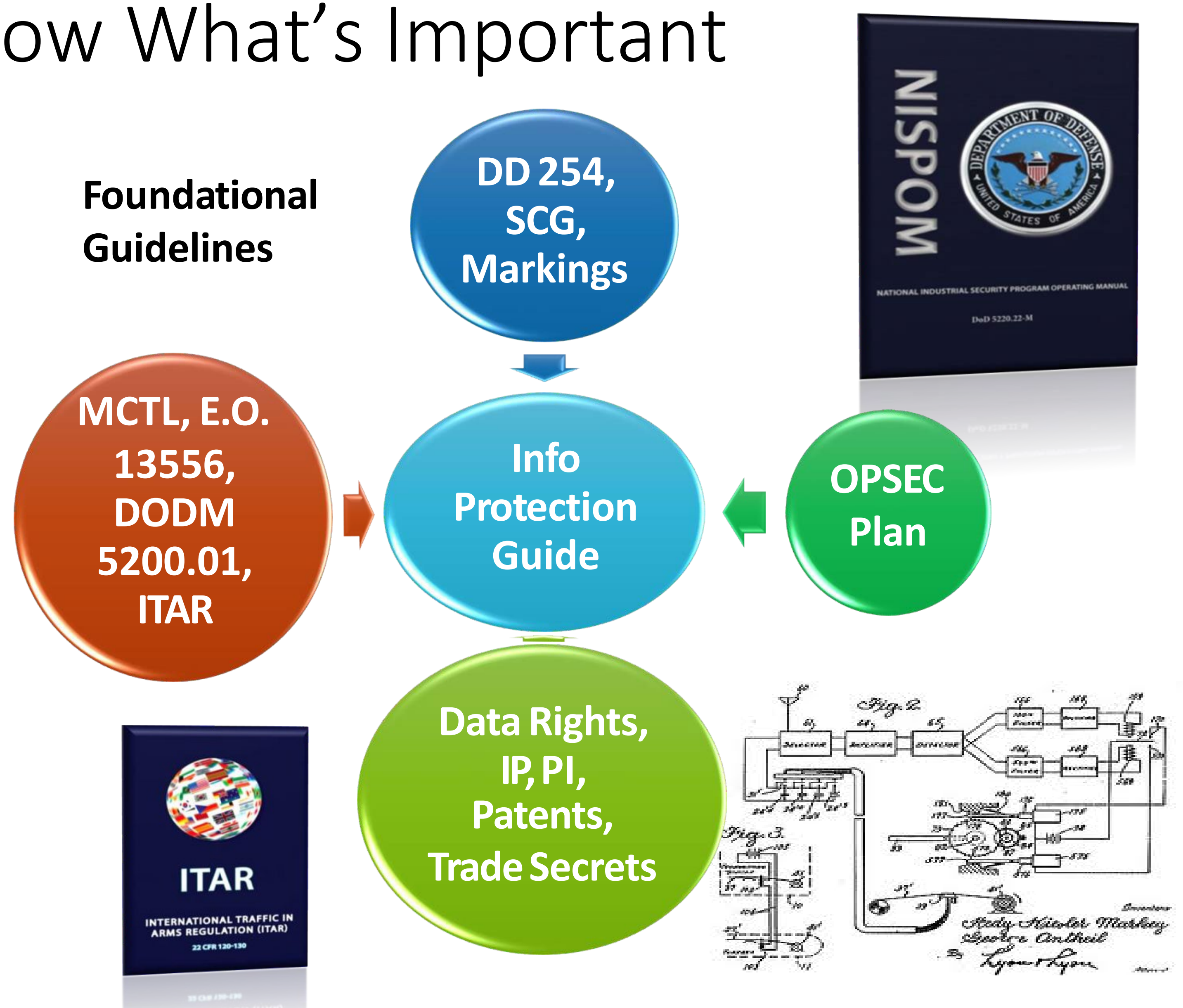
- Provides a frame of reference for:
  - OPSEC Reviews
  - Press Releases
  - Patents
  - Brochures and Presentations
  - Email Filters

Identify any controlled information in produced raw data (reports, brochures, test result, etc.)

Before you release it….Review it.

What to Protect-Classified and Unclassified Information Review Information-Know What’s Important

Who Reviews	What To Review
Techie	IP, classified, OPSEC, ITAR
PM	IP, classified, OPSEC, ITAR
OPSEC	OPSEC indicators
FSO	Classified, ITAR,
Legal	ITAR, PI, Trade Secret



Foundational Guidelines

DD 254, SCG, Markings

MCTL, E.O. 13556, DODM 5200.01, ITAR

Info Protection Guide

OPSEC Plan

Data Rights, IP, PI, Patents, Trade Secrets

Methodologies of Adversaries to Recruit Trusted Insiders Requests over Information Systems

- Adversaries can gain access to trusted employees (scientists, subject matter experts, support staff) through various means
- Fax
- Snail Mail
- E-mail
- Telephone
- Personal Contact

Contact may seem innocent enough, but….

- Legitimate business requests will come through appropriate channels
- Personal Contact: Asks about project specifics, whether or not classified or proprietary details
- Email address originated in a foreign country

Social Media Can Provide A Threat Opportunity

Be aware of contacts, friends, and requests

9 LINE ★ LLC

Methodologies To Thwart Recruiting Efforts

Protect Information Systems

Company Computer Security Safeguards

- Use computers for authorized business
- Establish and protect passwords
- Visit only authorized websites
- Use caution when downloading attachments
- Save all work
- Use classified systems for classified processing

Indicators Of Insider Threat Behavior / Procedures To Report Such Behavior

Suspicious Activities

- Requests for information outside of need to know
- Unauthorized reproduction of materials
- Unauthorized removal/destruction of materials
- Unexplained affluence
- Regular, unexplained foreign travel
- Maintains long hours despite job dissatisfaction

Report To FSO

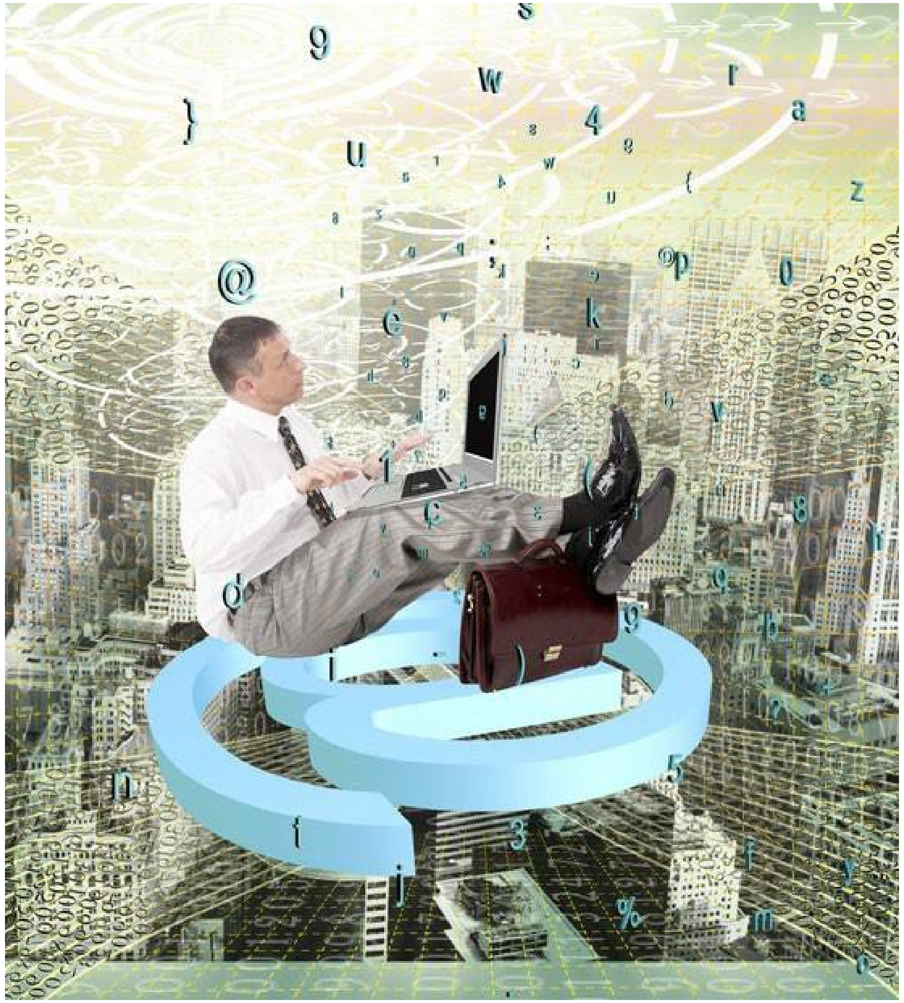
NISPOM Requires employees to report efforts by any individual to obtain illegal or unauthorized access to classified or sensitive information

Review

Indicators Of Insider Threat Behavior

Suspicious activity includes some of the following:

- Attempting to gain access to classified information without need to know
- Transmitting classified information without approval
- Attempting to bypass security procedures
- Losing classified information under their control
- Refusing to protect classifying information as required
- Repeated security violations



Indicators Of Insider Threat Behavior / Procedures To Report Such Behavior

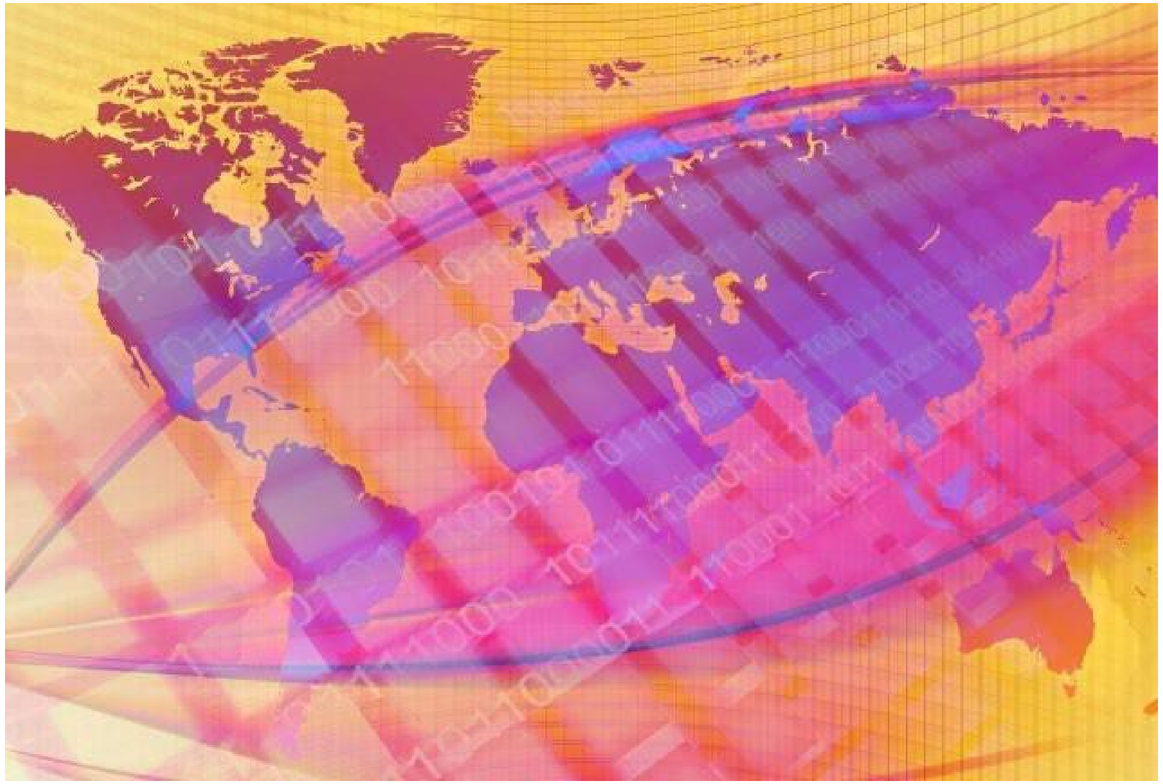
What to do if approached to commit espionage

- Remain non-committal and report as many details as possible.
  - If you agree, you may find yourself under investigation.
  - If you say “no”, the suspicious person may go to another target.

How Adversaries Recruit Trusted Employees Espionage 101

The following characteristics and situations could make you a target:

- Your access to intelligence information
- Visits to overseas locations where foreign intelligence operates
- Location in the U.S. where foreign nationals can gain access to you
- Ethnic, racial, or religious background that may attract the attention of a foreign intelligence operative



Review
Why You Could Be Targeted And Reducing Risk

Get approval for any technical presentations that involve proprietary, FOUO, ITAR controlled, or classified information

- What business will you be conducting?
- Is it approved?
- Make sure to stay on target

For example, suppose you have approval to present a business opportunity for a teaming effort on your company's refractor lenses for a foreign government's telescope. The foreign entity brings the discussion to focus light beam intensity. Same product, different capabilities.

- Your present situation may cause you to look vulnerable, but it doesn't mean you will be targeted.
- You can't control whether or not you are targeted
- You can control your actions and how you react to assessment and recruiting efforts.

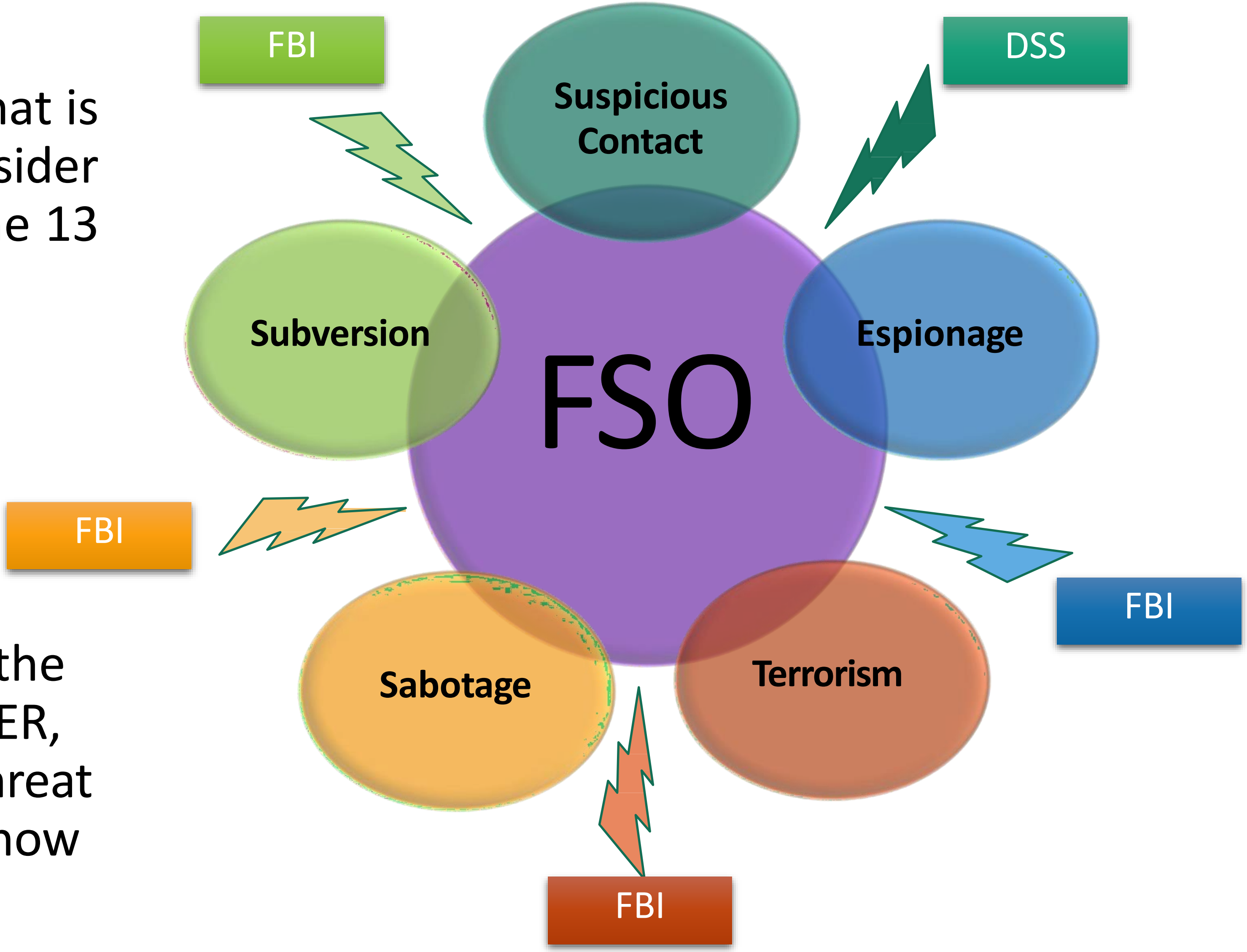
Incorporate a communications strategy and stick to it.

Reporting Requirements

Procedures to report such behavior that is indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines

- Suspicious contact-CSA (DSS)
- Espionage, sabotage, terrorism or subversion - FBI

The above agencies are referenced as the ultimate report destination. HOWEVER, your first stop is the FSO or insider threat program designee. Does everyone know who that is?



Summary

Cleared defense contractors are required to establish Insider Threat Programs (ITP) to protect classified information.

- An established ITP begins with required training for all cleared employees as a pre-requisite for access to classified information
- This training meets the NISPOM requirement by addressing:
  - The importance of detecting potential insider threats by cleared employees and reporting suspected activity
  - Methodologies of adversaries to recruit trusted insiders and collect classified information, within ISs
  - Indicators of insider threat behavior, and procedures to report such behavior
  - Counterintelligence and security reporting requirements

Acknowledgement

I certify that I have read and understand 9line’s 2024 Insider Threat Program Requirements:

__________________ __________________

Printed Name Signature

Date:__________________

Scott Heintz – FSO/ITPSO sheintz@9linellc.com

David Heintz – AFSO david.Heintz@9linellc.com