



International Operations

# INSIDER THREAT TRAINING

## Insider Threat – Espionage – Subversion – Sedition



PFC Manning

Compromised classified documents to WikiLeaks

- UNEXPLAINED AFFLUENCE OR WEALTH
- DISREGARD FOR SECURITY PRACTICES
- FOREIGN INFLUENCE OR CONNECTIONS



SPC Anderson

Attempted selling info on defeating M1 Abrams

- UNUSUAL WORK BEHAVIOR

- ADVOCATING VIOLENCE, THE THREAT OF VIOLENCE, OR THE USE OF FORCE AGAINST U.S.

**What is Insider Threat?**

**Why is the Insider Threat significant?**

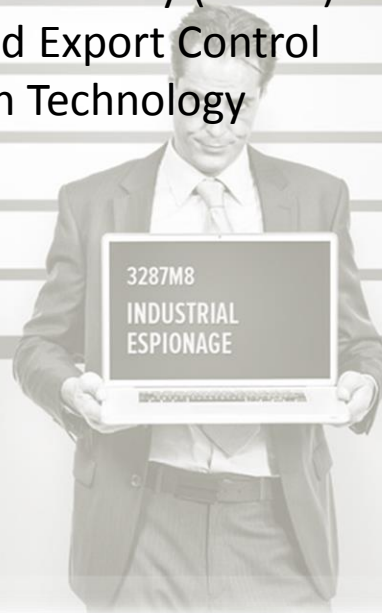
**How do you recognize the Insider Threat?**

**How can you help defeat the Insider Threat?**

**From a Counter Intelligence perspective, the Insider Threat is an employee with access to a classified or controlled environment who has the opportunity, capability, and intent to purposefully compromise sensitive information and/or materials for distribution to entities who pose a risk to the security interests of the United States.**

# Specifically what types of information are at risk due to Insider Threats?

- Classified and Proprietary information
- Intellectual Property
- Personally Identifiable Information (PII)
- Sensitive Information
- Classified Information
- Classified PII
- Sensitive but Unclassified
- Export Control
- For Official Use Only (FOUO)
- PII Classified Export Control
- Information Technology
- Weapons





# Presidential Documents Executive Order 13587 of October 7, 2011. The Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

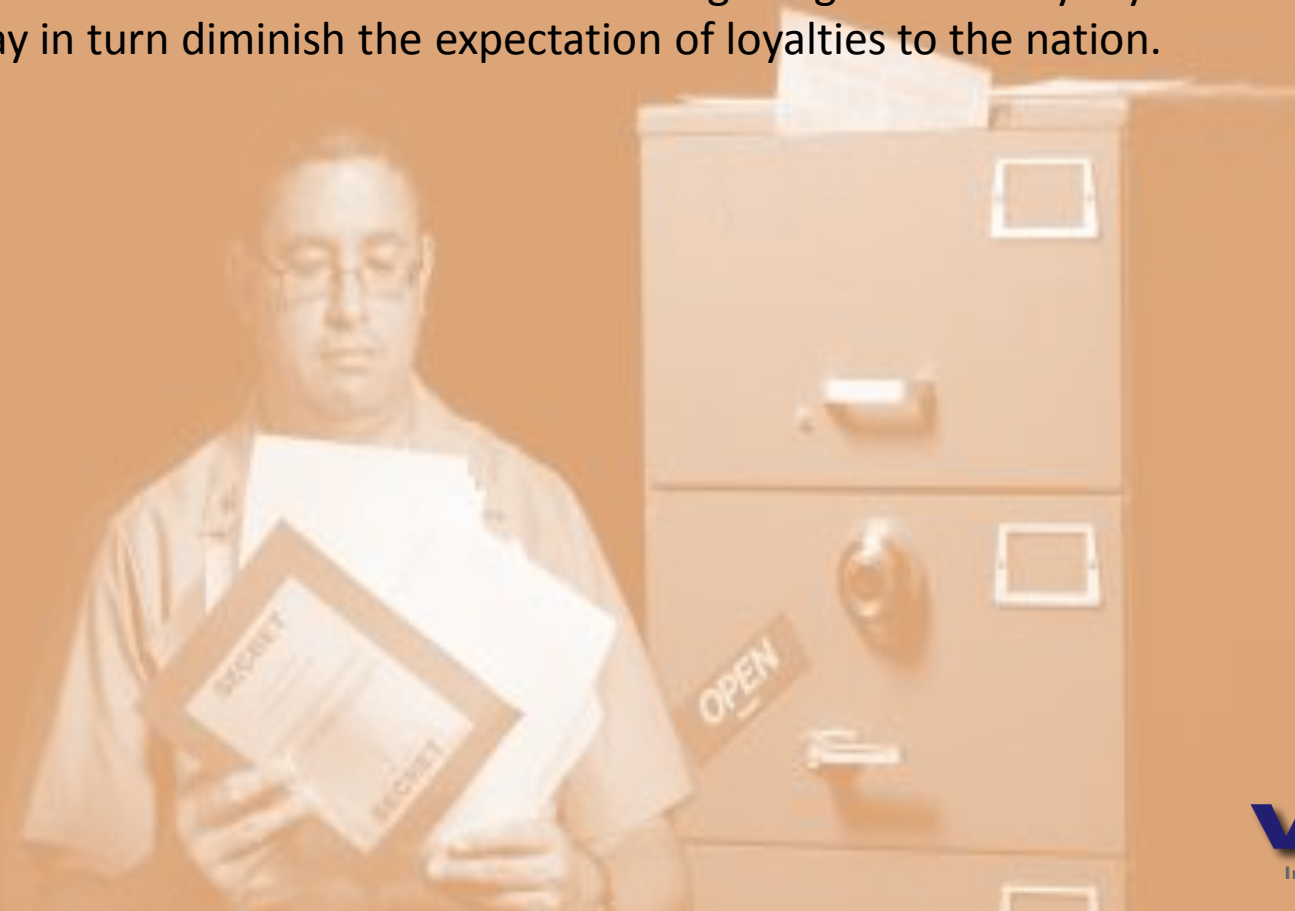
## Section 1.

### Policy.

**Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management. This order directs structural reforms to ensure responsible sharing and safe-guarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.**

**A threat posed by Insider activity in support of foreign power, criminal enterprises, and terrorist groups has the potential to endanger lives, compromise resources, and significantly diminish our capacity to execute our mission.**

However changing business environment definitely affects the threat of insider activity with layoffs and downsizing, furloughs, sequestration, transferring jobs overseas, all of which could contribute to our workforce losing obligations of loyalty in the workforce, which may in turn diminish the expectation of loyalties to the nation.



**An Insider Threat won't have on a ski mask or a disguise  
so you can tell he's a threat.**



Edward  
Snowden



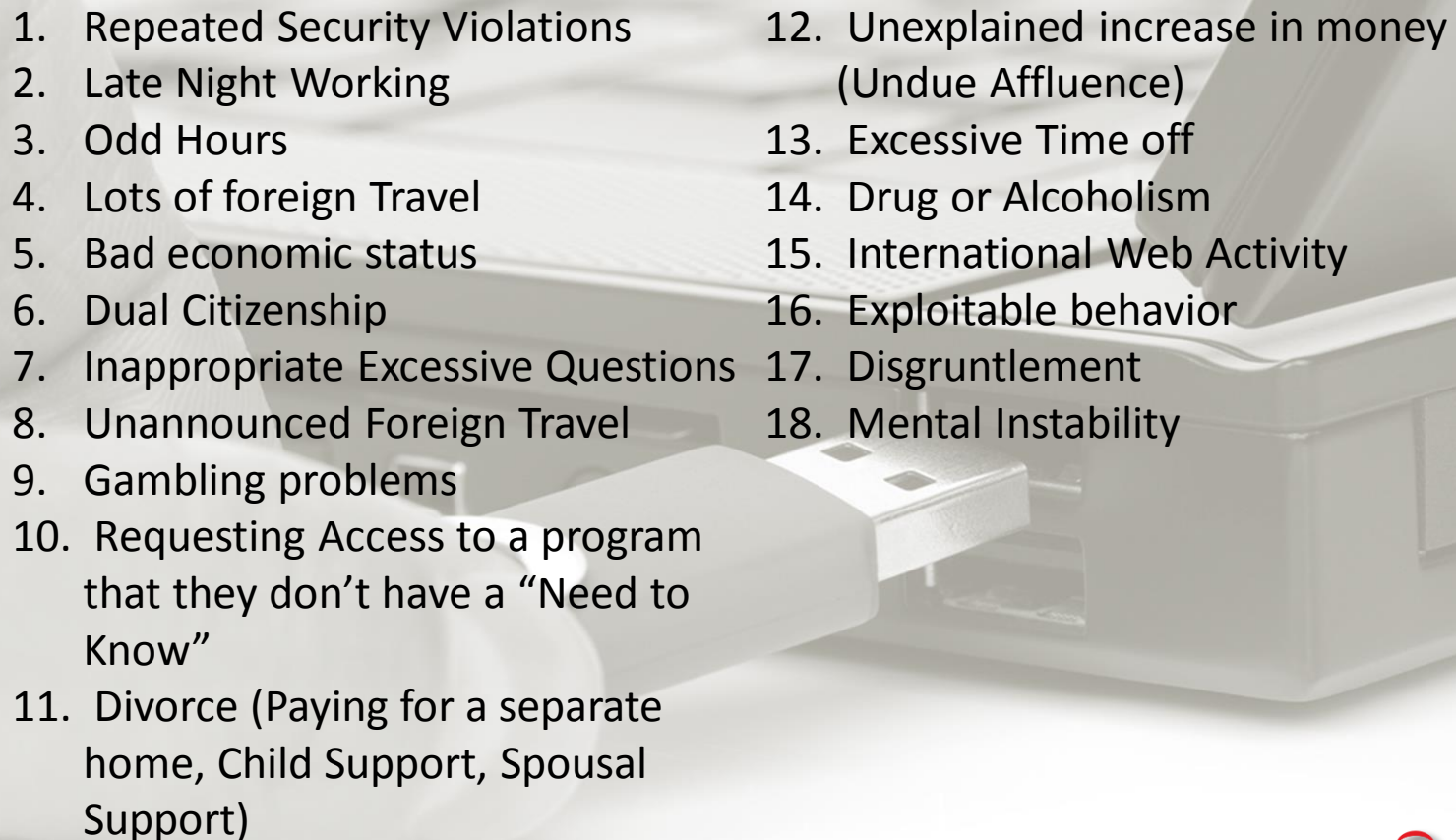
Army Pfc.  
Bradley  
Manning

**Industry has increasingly become more vulnerable to insider threats due to the increased access to sensitive information. Snowden and Manning are excellent examples of cases where, maybe their access should have been restricted to the programs or duties for which they were assigned. Also frequent travel, conflicting national loyalties, the vulnerabilities created by all of these trends increase the risk of Insider Activity.**

## What are some of the more common PEIs or Potential Espionage Indicators?

Someone may very easily have a few of these indicators.

**For example: Someone may need to work late because they can't drop off the kids until later in the morning. Also They may be going through a divorce so they're heavily in debt due to paying for 2 homes. Also because of the divorce they may be seeing a Psychologist.**

- 
- |  |   |
|--|---|
| 1. Repeated Security Violations  | 12. Unexplained increase in money (Undue Affluence) |
| 2. Late Night Working  | 13. Excessive Time off                              |
| 3. Odd Hours   | 14. Drug or Alcoholism                              |
| 4. Lots of foreign Travel  | 15. International Web Activity                      |
| 5. Bad economic status   | 16. Exploitable behavior                            |
| 6. Dual Citizenship  | 17. Disgruntlement                                  |
| 7. Inappropriate Excessive Questions                                     | 18. Mental Instability                              |
| 8. Unannounced Foreign Travel  |   |
| 9. Gambling problems   |   |
| 10. Requesting Access to a program that they don't have a "Need to Know" |   |
| 11. Divorce (Paying for a separate home, Child Support, Spousal Support) |   |

## What happens if you know someone who does have 1 or 2 of the characteristics? Should you report them?

Not to say that every person who exhibits one or more of these indicators is involved with illicit behavior, but most of the persons who have been involved in insider activity in the past were later found to have displayed at least some of these indicators. Their former co-workers and supervisors rarely felt compelled to report this behavior to the proper authorities.

If there is a situation where a foreign intelligence entity appears to have knowledge or possession of information that are not expected to have. An example would be the appearance of classified or proprietary design features of US weapon, or communication systems and you see that in comparable systems produced by a foreign defense industry, our space shuttles, our helicopters, satellites, all of those are great examples of anomalies.

Trends of individuals who have committed espionage:

- 1/3 of spies are naturalized U.S. Citizens
- More than 1/3 of spies had no security clearance
- Twice as many spies volunteered as were recruited we've seen that with Manning and Snowden. They were just volunteers.
- Most recent spies have been solo actors
- Nearly 85% passed information before being caught
- The most recent cases, 90% used computers in their espionage, 2/3 used the internet
- 80% received NO payment for their spying

When it comes to the security of our nation it's better report if you suspect something. For example: You notice a coworker seems to be gambling and drinking a lot and becomes very agitated when you ask him/her about these problems. **IF IN DOUBT = REPORT IT** Then if it turns out to be nothing then at the very least you may be getting that person help for his/her gambling and drinking problems.



# Is money the reason? Is loyalties to other countries the reason?

#1 reason a person spy's it is no longer money. It is when a person is divided with their loyalties. One motivation and followed by disgruntlement. Money is now last, so the motivation for spying has shifted greatly. Also due to multiple citizenships, and country of interest cards, layoffs, furloughs, all of which contribute to Insider Activity.



Chi Mak an Engineer and a naturalized US citizen. Convicted of spying on US for China. He held dual citizenship but remained loyal to China.



Dongfan "Greg" Chung also was an Engineer and a US naturalized US citizen. Convicted of spying on US for China. He held dual citizenship but remained loyal to China.



Bradley E. Manning a US Army soldier. After disclosing to WikiLeaks nearly three-quarters of a million classified or unclassified but sensitive military and diplomatic documents. Manning was 286 years old when he was sentenced in 2013 to 35 years imprisonment and dishonorably discharged from the Army.



Edward Snowden a computer professional, former CIA employee, former contractor for the US government. He revealed thousands of classified NSA documents to journalists. The material appeared in "The Guardian, The Washington Post, Der Spiegel and The new York Times. He is currently living in Russia but he will need to seek asylum elsewhere soon. As his asylum in Russia will soon run out.

# **Reporting Requirements of Potential Espionage Indicators:**

## **The DoD Directive 5240.06 is the Counter Intelligence Awareness and Reporting Directive.**

DoD personnel who fail to report information as required, may be subject to judicial or administrative action, or both, pursuant to application law and regulations.

Contractor personnel are required to report certain events that have an impact on the status of an employee's personnel security clearance. Employee are required to report the following items to the security officer.

1. Adverse Information
2. Suspicious contacts
3. Change in Cleared Employee Status
  - Death
  - Change of Name
  - Termination of Employment
  - Change in Citizenship
  - When the possibility of access to classified information in the future has been reasonably foreclosed.
4. Citizenship by Naturalization (If a non-US citizen employee granted a Limited Access Authorization becomes a citizen through naturalization).
5. Employees Desiring Not to Perform on Classified Work
6. Refusal by employee to sign the SF312 which is the Classified Information Nondisclosure Agreement.
7. Change Conditions Affecting the Facility Clearance
8. Changes in Storage Capability
9. Inability to Safeguard Classified Material
10. Security Equipment Vulnerabilities
11. Unauthorized Receipt of Classified Material
12. Employee Information in Compromise Cases
13. Disposition of Classified Material Terminated From Accountability
14. Foreign Classified Contracts
15. Reports of Loss, Compromise, or Suspected Compromise
16. Individual Culpability Reports

# Conclusion:

## YOU ARE THE FIRST LINE OF DEFENSE

- The Insider Threat is the most damaging
- Most were authorized access in conjunction with their work assignments
- May have circumventing the need-to-know principle
- Insiders are recruited or volunteer

Counter Intelligence, Security, and Information Awareness Core Mission is to: Protect against the loss or compromise of critical U.S. Classified information and technologies by preventing penetrations by Foreign Intelligence Services and detecting, deterring and mitigating the threat posed by “Insiders”. This is our core mission and this is what we need to take away from this briefing report.

FBI Tips and Public Leads - <https://tips.fbi.gov/>



**With my signature and date below I am stating that I have read the Insider Threat training.**

**PRINTED FULL NAME**

---

**SIGNATURE**

---

**DATE OF COMPLETION:** 

---