



Insider Threat Program

Overview:

- Insider Threat Program Timeline
- What Is An Insider Threat?
- Insider Threat Traits
- How To Recognize an Insider Threat
- When To Speak Up
- Significance And Impact
- Conclusion
- Questionnaire Link

Insider Threat Program Timeline

Part 1

On October 7, 2011, the President signed Executive Order 13587 which directs the heads of agencies that operate or access classified computer networks to have responsibility for appropriately sharing and safeguarding classified information.

Part 2

November 2012, the White House issued National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. These minimum standards provide the departments and agencies with the minimum elements necessary to establish effective Insider Threat Programs and safeguard classified information.

Part 3

At the end of November 2016, DSS required all cleared companies to have a have an established Insider Threat Program and a designated Insider Threat Program Senior Official.

What is an Insider Threat?

Any act by an insider who intentionally or unintentionally compromises or potentially compromises not only national security, but also proprietary and sensitive company data.

Insider Threat Traits

Not everyone who displays one or more of these traits is an insider threat. These traits have great potential to provide a pattern of events that could lead to a bona fide threat.

Emotional

- Past/Present display of depression
- Severe stress in life
- Family crisis
- Health issues

Psychological

- Conflicting Ideologies or disaffected political sympathies
- Exaggerated desire for adventure/revenge
- Ego gratification
- Irrational views of reality and misplaced anger

Behavioral

- Consistent disciplinary issues
- Excessive use of drugs/alcohol
- Financial trouble
- Need/Desire for money (gambling)

How to recognize a possible Insider Threat

Viable Indicators:

1. Repeated Security Violations
2. Failure to report foreign travel
3. Attempting access to areas not authorized
4. Irrational behavior (aggressive, disruptive, depressed)
5. Working hours inconsistent with job assignment
6. Sudden reversal of financial situation
7. Attempting to bring in unauthorized electronic device.

When To Speak Up

You are the first line of defense against insider threats. Please Speak Up and talk to your FSO if any of these situations arise:

- At any point you see an employee compromise sensitive or classified data.
- You feel uncomfortable with any situation involving a fellow employee or anyone else outside of the company.
- Receive uncomfortable information or requests via mail, email, or text from another employee or anyone else outside of the company.
- Notice an employee displaying consistent irrational behavior and/or has blatant disregard for their job.
- An employee expressing undying loyalty to another foreign government.
- Anyone making threats in any matter, even as a joke.
- See any employee make threatening, disparaging remarks about employees, the company, or talking about classified/sensitive information on social media (facebook, linkedin, twitter, etc.)

Significance and Impact

Ignoring questionable behaviors can only increase the potential damage an insider can have on national security or employee safety.

IMPACT 1

- Severe loss or compromise of classified or controlled sensitive information.

IMPACT 2

- Weapons systems cloned, destroyed, or countered

IMPACT 3

- Loss of technological superiority or intellectual property

IMPACT 4

- Physical harm or loss of life

Conclusion

Everyone has a responsibility to ensure the protection of classified and sensitive information entrusted to them. It's important to be vigilant and aware of potential issues and actions of those around you. Speak Up and start a dialogue with your tiag FSO, CM, Director or HR.

See Something, Say Something

ACTION REQUIRED

Please click the link to complete the questionnaire
(Make sure you are logged into your tiag gmail account)

<https://goo.gl/forms/dDJRnT1V4xapWBQ62>

*****Some government systems may not support Google Forms so you will need to complete the questionnaire on a home computer, tablet, or smartphone*****

Questions or want more information?

Contact your Corporate FSO

Kari Anderson

kanderson@tiag.net or 703-437-7878