National Insider Threat Special Interest Group (NITSIG)

Suitability, Counterintelligence & Behavioral Indicators Of Concern For Insider Risk Management Programs

This guide while intended for use by the DoD, contains many employee behavioral indicators that private sector companies and organizations should be concerned with.

1. Suitability Issues:

1.1. Drug or alcohol abuse.
1.2. Repeated irresponsibility.
1.3. An "above the rules" attitude.
1.4. Financial irresponsibility.
1.5. Repeated impulsive behaviors.
1.6. Extreme immaturity.
1.7. Willingness to violate the rights of others to achieve one's own ends.
1.8. Accumulating or overwhelming life crises or career disappointments.
1.9. Willingness to break rules or violations of laws and regulations.

2. Alcohol Or Other Substance Abuse / Dependence:

2.1. Appearing intoxicated at work.
2.2. Irregular work schedules.
2.3. Sleeping at the desk.
2.4. Driving while intoxicated.
2.5. Concealing alcohol at work or in the car.
2.6. Ability to consume five or more drinks with little effect.
2.7. Unexplained, repeated absences on Monday and/or Friday.
2.8. Going "on and off the wagon."
2.9. Cannot remember something that happened while drinking.
2.10. Use of alcohol to cope with stress.
2.11. Use of illicit/illegal substances.
2.12. Misuse of prescription medication (other than as prescribed).
2.13. Uncharacteristically slurred speech, disorientation, or lack of coordination.

3. Mental Health Issues:

3.1. Unexplained changes in mood.
3.2. Increased nervousness or anxiety.
3.3. Decline in performance or work habits.
3.4. Changes in personal hygiene.
3.5. Expression of unusual thoughts, perceptions, or expectations.
3.6. Pattern of lying.
3.7. Talk of or attempt to harm one self.

4. Extreme, Persistent Interpersonal Difficulties:

4.1. Argumentative or insulting behavior toward work associates or family that has generated workplace discussion or has disrupted the workplace environment.
4.2. Tends to isolate self, rejects any social interaction, apparent lack of social supports, unexplained and manifested depression.
4.3. Verbal out bursts, usually drawing attention of those not directly involved in the exchange.
4.4. Exploitation or mis-treatment of others, usually through intimidation or abuse of power of position.
4.5. Disruptive workplace behavior that resists supervisory direction or counseling.

5. Hostile Or Vindictive Behavior:

5.1. Verbal or physical threats toward work associates or family.
5.2. Extreme or recurrent statements demonstrating level of bitterness, resentment, vengeance, or disgruntlement.
5.3. Any occasion of violence, throwing things.
5.4. Stalking-type behavior (such as unwanted following, harassing phone calls).
5.5. Threats or attempts to get even with work associates.
5.6. Extreme or recurrent violation of rule(s) or law(s).

6. Criminal Behavior:

6.1. Theft
6.2. Fraud (for example, misuse of leave, voucher, tax, travel or training advances, or government credit cards).
6.3. Spouse or child abuse or neglect.
6.4. Attempts to enlist others in illegal or questionable activity.

7. Finances:

7.1. Financial Irresponsibility or Troubles
7.1.1. Calls at work from creditors.
7.1.2. Denial of credit.
7.1.3. Garnishments.
7.1.4. Bounced or bad checks.
7.1.5. Repossessions, unfavorable judgments, or other indications of difficulty.
7.1.6. Bankruptcy.
7.1.7. Negligent/tardy child or spousal support payments.
7.1.8. Reckless or compulsive spending trends, frequent gambling, or evident gambling debt.
7.1.9. Improper handling of organization finances or property, including repeated delinquent accountings for advances, unexplained cash.
7.1.10. Shortages or loss of property, sloppy handling of cash funds, disregard for financial/property administration regulations.
7.2. Unexplained or Sudden Affluence
7.2.1. Living/spending beyond one's apparent means.
7.2.2. Unexplained or sudden large sums of cash.
7.2.3. Sudden windfalls or settlement of large debt.
7.2.4. Claims of significant independent income from inheritance, wealthy relatives, gifts, investments, family business, etc.
7.2.5. Personal possessions inconsistent with salary.

8. Unreported Or Concealed Contacts With Foreign Nationals:

8.1. Unreported personal contacts with:
8.1.1. Foreign intelligence services.
8.1.2. Foreign governments or organizations.
8.1.3. Unauthorized persons seeking classified information.
8.1.4. Unreported Close Continuing Contact With foreign nationals, including intimate encounters, shared living quarters or marriage.
8.2. Unreported relatives, associates, or person sharing living quarters connected with:
8.2.1. Foreign governments.
8.2.2. Foreign intelligence services.
8.2.3. Criminal or terrorist activities.
8.2.4. Disloyalty toward the U.S.

9. **Divided Loyalty Or Allegiance To The U.S.**:

9.1. Personal possession and use of a foreign passport.
9.2. Strongly voiced advocacy of acts of force or violence against the U.S. Government.
9.3. Association or sympathy with persons advocating such acts.

10. **Duty, Access, And Handling Of Classified Information:**

10.1. Unexplained absences.
10.2. Keeping unusual work hours.
10.3. Repeated or unusual overtime.
10.4. Sudden deterioration of work performance or attitude.
10.5. Unusual use of or requests made for classified publications or technical order libraries.
Indicators of Espionage
10.6. Inappropriate, unusual, or excessive interest in classified information (outside current assignment)
10.7. Inquiries about operations and projects to which he or she no longer has access.
10.8. Attempting to gain new accesses without the need to know
10.9. Other violation of need-know principle.
10.10. Mishandling of Classified Information:
10.10.1. Revelations to unauthorized persons.
10.10.2. Leaks to media.
10.10.3. Unauthorized contact with media.
10.10.4. Unauthorized removals, including magnetic media.
10.10.5. Collecting /storing classified material outside approved facilities.
10.10.6. Lax security habits that resist management counseling (such as discussing classified information on unsecure phone, not properly securing classified information or areas, working on classified material at home).
10.10.7. Statements or actions that demonstrate an individual believes that the rules do not apply to him or her.
10.11. Any attempt to obtain information without a need to know.
10.12. Unauthorized removal of classified material from work areas.
10.13. Placing classified material in a desk or briefcase.
10.14. Repeated volunteering for special assignments providing a different or higher access.
10.15. Using equipment in other offices to reproduce classified material when copiers are available in person's own area.
10.16. Borrowing, making notes of, or obtaining witness signatures on classified documents not associated with assigned duties.
10.17. Bringing cameras or recording devices into areas storing classified data.

11. **Financial:**

11.1. Sudden purchases of high value items, such as real estate, vehicles, or vacations, where no logical income source exists.
11.2. Opening of substantial savings accounts where no logical income source exists.
11.3. Opening of savings or stock accounts with foreign banks or brokerage houses.
11.4. Large tipping, free spending, large display of cash.
11.5. Display of expensive acquisition or large amounts of cash, especially after recent leave.
11.6. Extensive and regular gambling losses.
11.7. Sudden repayment of large loans.
11.8. Purchase of expensive miniature cameras and related equipment.
11.9. Purchase of good international or ham radio-band equipment by other than a known hobbyist.

12. Leave And Travel:

12.1. Any unreported personal foreign travel.
12.2. Repeated Short Leaves:
12.2.1. Short trips overseas or in the continental United States for unusual purposes.
12.2.2. Recurring quick weekend trips not associated with recreation or family.
12.2.3. Trips with cost out of proportion to short time spent at the location.
12.2.4. Hesitation or inability to adequately describe the location visited upon return from trip.
12.3. Foreign Travel:
12.3.1. Frequent foreign travel without trying to use low-cost air fares or space-available travel.
12.3.2. Any foreign travel not identified in an individual's passport.
12.3.3. Mention of border crossing, visa, or police problems in foreign countries.

13. Social And Family:

13.1. Visits from relatives or friends from countries whose interests may be inimical to the United States.
13.2. Requests to assist relatives or friends in countries whose interests may be inimical to the United States.

14. Situations Conducive To Espionage:

14.1. Local National Association and Access:
14.1.1. Local national attempts to entice Air Force members with sensitive jobs into criminal situations that could lead to blackmail.
14.1.2. Local national base employees frequent Air Force clubs, consistently seek to befriend Air Force members, and attempt to draw conversation to base operations or security.
14.1.3. Unusual incidents involving magazine sales or door-to-door sales to military members in overseas areas, usually associated with requests for information.
14.1.4. Membership in ethnic clubs or associations that may be hostile to the U.S.
14.2. Unit Security Awareness
14.2.1. Frequent classified document loss or control problems.
14.2.2. Continually seeking interim clearances for personnel while procrastinating on documentation.
14.2.3. Poor physical security and control in sensitive areas.
14.3. Unreported unofficial contact with a non-US citizen employed by a foreign diplomatic establishment.

15. Computer User Activity:

15.1. Excessive printing of documents either sensitive but unclassified (export controlled/FOUO/LE sensitive) or classified.
15.2. User accessing folders and files on the network server which are not associated with his/her duties
15.3. User has unauthorized software loaded on the government computer
15.4. User emails foreign and/or non-DoD entities large volumes of information either inside the text of the email or via attachments
15.5. User visits foreign language websites from DoD computer
15.6. User visits free On-Line file storage websites from DoD computer
15.7. User visits hacker associated websites containing hacker tools
15.8. Use of high capacity removable media such as thumb drives and USB hard drives
15.9. Use of wireless computer networking technology
15.10. Accessing databases without authorization.
15.11. Unauthorized searching/browsing through computer libraries.
15.12. Unauthorized purposeful destruction of information on Agency computers.

16. Computer Activity (Attended / Unattended):

16.1. A computer is sending excessive amounts of data out of the network to either DoD, non-DoD entities or foreign IP addresses

16.2. A computer sends beacon messages out of the network on standard and non-standard ports

16.3. A computer is used to search the network for and extract files from other computers and file servers, and then stores them

16.4. A computer is used to attack other computers within the network or outside the network (reported by local or outside agencies)

17. Phone Activity:

17.1. Phone calls to foreign embassies

17.2. Phone calls to foreign phone numbers

17.3. Excessive phone calls to the same phone number

17.4. Phone calls to 'known' or suspected IO's

17.5. Modem detected at the end of phone line located within a SCIF. This may be connected to a classified computer inside the SCIF, with the goal to exfiltrate data from the network and/or grant remote access to FISS.

COMPUTER SYSTEM / NETWORK ACTIVITIES OF CONCERN

When there are employee suitability concerns that are coupled with computer and network activities of concern, this may require the immediate attention of the Insider Threat Program Manager, Insider Threat Analyst or Investigator.

- An employee that has anomalous work hours and / or computer & network activity. Employee work hours not approved by supervisor
- An employee that is unwilling to allow someone to assume their duties
- An employee that is conducting multiple searches for key words and an inordinately high number of cut and paste operations, followed either by printing or generating an encrypted outbound message
- An employee who is doing web searches for web browser extensions, encryption, password cracking tools, hacking tools, computer key loggers, steganography tools, Etc.
- An employee that is attempting to execute or has executed an unauthorized self running executable software program on their computer (Steganography, Remote Control Programs (Teamviewer), Etc.)
- An employee unauthorized / attempted installation of software on their computer
- An employee downloading a large volume of files to a portable storage device
- An employee copying a significant number of files from the network to their computer hard drive
- An employee unauthorized / attempted modification of computer operating system security related settings on their computer
- An employee that has an unauthorized file transfer protocol (FTP) server running on their computer
- An employee that has unauthorized storage of encrypted data on their computer
- An employee who exceeds their normal web activity and who sends many emails using commercial web based email services
- An employee who is using web based encrypted e-mail services for malicious purposes. (ProtonMail, Tutanota, Etc.)
- An employee who has installed unauthorized virtual machine software on their computer
- An employee that has installed unauthorized web browser extensions (Chrome Remote Desktop, Screen Leap Screen Sharing, VPN, Etc)
- An employee that is sharing work related file without authorization using Social Networking / Web Collaborations Tools (Facebook / Facebook Messenger, Instant Messaging Tools, Go To Meeting, Skype, Zoom, Etc.)
- An employee who is using web based large file transfer services for malicious purposes (Ability To By Pass Network Security Tools) (**Example:** www.transfernow.net)

- An employee who's computer has a high rate of network activity / traffic outside of normal working hours
- An employee who uses their computer to charging their cell phones (Cell Phone Can Also Be Used As Storage Device)
- An employee unauthorized / attempted modification of network security devices such as routers and firewalls (Privileged User)
- An employee doing a network search for files that do not relate to their normal job
- An employee that is detected of trying and failing at least three times to access shared files on a network server for which they does not have access permissions
- An employee unauthorized installation of a printer on their computer (Bypass Network Print Monitoring)
- An employee who downloads multiple picture files from external websites (Could Indicate The Use Of A Steganography Software Program To Hide Files And Exfiltrate)
- An employee who renames files for malicious purposes to bypass network security tools (Example: JPG To PDF. JPG File Contains Hidden Documents Using Steganography Software)
- An employee who's computer has outbound web connections to an overseas destination, for which there is no valid business reason
- An employee that is attempting to circumvent auditing (Example: Clear Audit Logs On Their Computer)
- An employee who has or is attempting to change shared folder and file permissions on the network
- An employee that has installed a USB key logger on another employees computer to steal passwords
- An employee who connects their computer to their smartphone's hotspot to bypass network security monitoring tools
- An employee who has an unusual interest in network topologies (Firewall, Security Hardware / Software, Hacking, Penetration Testing, Etc.) that is outside their job responsibilities