National Insider Threat Special Interest Group (NITSIG)

INSIDER THREAT INDICATORS - BEHAVIORS OF CONCERN

The majority of the indicators listed below are taken from the DoD Directive 5240.06 - Counterintelligence Awareness and Reporting (CIAR). The reporting requirements apply to the DoD. The applicability statement mentions that these reporting requirements will be incorporated into DoD contracts, as appropriate, and made applicable to those contracts.

While many of these indicators apply to personal with access to classified information and classified areas, some of the indicators should be of concern to any organization that wants to ensure the protection of sensitive data, information systems, networks and personnel.

Reportable Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social networking sites that is not related to official duties.
2.	Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or sensitive information in the form of facilities, activities, personnel, technology or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence) or automated systems intrusions.
3.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
4.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
5.	Acquiring, or permitting others to acquire, unauthorized access to classified information systems.
6.	Attempts to obtain classified information by an individual not authorized to receive such information.
7.	Persons attempting to obtain access to information inconsistent with their duty requirements.
8.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
9.	Discovery of suspected listening or surveillance devices in classified or secure areas.
10.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
11.	Discussions of classified information over a non-secure communication device.
12.	Reading or discussing classified information in a location where such activity is not permitted.

13.	Transmitting or transporting classified information by unsecured or unauthorized means.
14.	Removing or sending classified material out of secured areas without proper authorization.
15.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
16.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
17.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
18.	Unwarranted work outside of normal duty hours.
19.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
20.	Attempts to entice personnel or contractors into situations that could place them in a compromising position.
21.	Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.
22.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
23.	Requests for information that make an individual suspicious, to include suspicious or questionable requests over the internet or social networking sites.
24.	Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
25.	Personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen: a. Exhibits excessive knowledge of or undue interest in personnel or their duties beyond the normal scope of friendly conversation. b. Attempts to obtain classified or unclassified information. c. Attempts to place personnel under obligation through special treatment, favors, gifts, money or other means. d. Attempts to establish business relationships that are outside the scope of normal official duties.
26.	Incidents in which personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security or intelligence organization and a. Are questioned about their duties. b. Are requested to provide classified or unclassified information. c. Are threatened, coerced or pressured in any way to cooperate with the foreign official. d. Are offered assistance in gaining access to people or locations not routinely afforded Americans.

27.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to inheritance luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.
28.	Contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which: a. Illegal or unauthorized access is sought to classified or otherwise sensitive information. b. The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.
29.	Any contact with the media where the media seeks access to or results in the unauthorized disclosure of classified information, unclassified, or other information not approved for public release.
30.	Arrests, charges, convictions, and criminal court appearance (with the exceptions of a summons for jury duty or to appear as a witness or provide other testimony when the individual is not being charged or otherwise being prosecuted). Traffic infractions where the fine was less than $300 and did not involve alcohol or drugs are not reportable. All reports should include dates, jurisdiction, name of the court, nature of the issue, and disposition, if available. Changes in the status of any previously reported court involvement shall also be promptly reported.
31.	Adverse changes to financial status to include, but not limited to, garnishments, foreclosures, liens, judgments, delinquent taxes, and/or bankruptcy filings.
32.	Any hospitalization for a mental health condition.
33.	Use of or involvement with illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants.
34.	Voluntary or involuntary treatment for abuse of alcohol or illegal use of controlled substances.
35.	Close and continuing association with foreign nationals.
36.	Unwillingness to comply with rules and regulations, or to cooperate with security requirements.
37.	Alcohol abuse.
38.	Apparent or suspected mental or emotional condition where there is reason to believe the condition may affect the individual's judgment, reliability, or ability to protect classified information.
39.	Criminal conduct.
40.	Any activity that could constitute a conflict of interest with U.S. Government employment.
41.	Misuse or abuse of U.S. Government property or information systems.

Reportable Suspected Terrorism or Work Place Violence Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.
11.	Possessing weapons in the work place.
12.	Threatening to kill or harm supervisors, co-workers or anyone else within or outside of the work place.
13.	Sending emails or posting on social media sites threatening communications against supervisors, co-workers or anyone else within or outside of the work place.

Reportable Behaviors Associated With Cyberspace Contacts, Activities, Indicators

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data ex-filtrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.