INSIDER THREAT INDICATORS

GOVCLEARED360
govcleared360.com

Awareness reference for cleared personnel and security officers · 32 CFR Part 117 · NITTF / CDSE awareness themes

BEHAVIORAL INDICATORS

- Attempts to access information beyond need-to-know
- Working odd hours without authorization or need
- Removing or copying protected material unnecessarily
- Repeated disregard for security procedures
- Significant disgruntlement toward employer or government
- Unreported foreign travel or foreign contacts

One indicator alone rarely means a threat. Patterns and clusters are what matter. Report; don't investigate.

HOW ADVERSARIES APPROACH TRUSTED INSIDERS

- Flattering outreach on LinkedIn or research forums
- Fake job offers, consulting gigs, or talent programs
- Elicitation at conferences: casual, expert questions
- Romance or friendship built online, then small favors
- Front companies and academic collaboration requests
- Requests that creep: benign first, protected later

You do not need access to secrets to be a target. Access to people who have access is enough.

FINANCIAL & LIFESTYLE INDICATORS

- Unexplained affluence: spending beyond known income
- Sudden repayment of large debts
- Severe financial distress or desperation
- Substance abuse affecting judgment or reliability
- Criminal conduct

Most confirmed insiders showed concerning indicators beforehand, and coworkers noticed first.

CYBER & INFORMATION INDICATORS

- Use of unauthorized storage devices or personal email for work information
- Unauthorized downloads, mass copying, odd printing
- Attempts to bypass security controls or monitoring
- Introducing unauthorized software or hardware

Report suspected compromise immediately, even your own mistakes. Self-reporting is viewed favorably.

IF YOU SEE SOMETHING

- Report to your FSO or security office promptly
- Do not confront, investigate, or tip off the person
- Reporting early is protection, for them and for you: most reports lead to help, not punishment
- Failure to report reportable information can affect your own eligibility

Early reporting is how programs get people support before a problem becomes a case.

THE PROGRAM BEHIND THIS SHEET

- Every cleared contractor must run an insider threat program with a designated senior official (ITPSO)
- All cleared employees: awareness training before access and annually after
- Suspicious contacts must be reported to your CSA

FSOs and ITPSOs: gathering, correlating, and documenting these signals is what GovCleared360 does.