Suspicious Cyber Activities & Behaviors*

- Actual or attempted unauthorized access into automated information systems or networks
- Password cracking, key logging, encryption, hacking activities, and account masquerading
- Use of account credentials by unauthorized parties
- Tampering with or introducing unauthorized elements into information systems
- Unauthorized downloads or uploads of sensitive data; unexplained storage of encrypted data
- Unauthorized use of removable media or other transfer devices
- Downloading or installing non-approved computer applications
- Unauthorized email traffic to and from foreign destinations
- Denial of service attacks or suspicious network communications failures
- Data exfiltrated to unauthorized domains
- Unexplained user accounts
- Social engineering, electronic elicitation, email spoofing, or spear phishing

** Certain cyber intrusions may fall under the reporting requirements of the National Industrial Security Program Operating Manual (NISPOM) paragraph 1-301 regardless of the classification level of information contained on the affected system*

Technology and information resident in U.S. cleared industry is under constant and pervasive threat. Timely and accurate reporting from cleared industry is the primary tool to identify and mitigate collection efforts targeting technologies and information resident in cleared industry.

Report suspicious activities, behaviors, and contacts to your facility security officer.

FSOs will report information in accordance with the NISPOM.

The activities, behaviors, and contacts listed in this brochure do not include all tactics, techniques, and procedures foreign intelligence entities may use to obtain restricted information.

For additional information, go to http://www.dss.mil

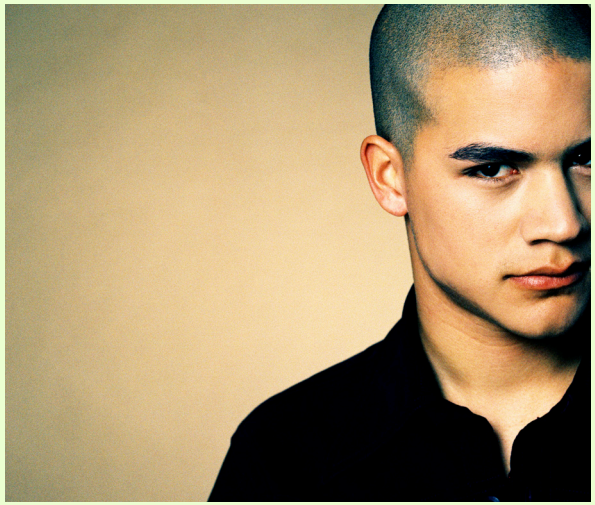
Report suspicious activity to your local security contact.
Your DSS point of contact is:

Counterintelligence AWARENESS

Examples of suspicious activities, behaviors, and contacts

This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

Suspicious Contacts



- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information resident in industry or to compromise a cleared employee
- Contact by cleared employees with known or suspected intelligence officers from any country
- Any contact which suggests the employee concerned may be the target of an attempted exploitation by foreign intelligence organizations
- Attempts to entice cleared employees into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
- Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money

Suspicious Activities & Behaviors

- Unauthorized possession of cameras or recording or communication devices in classified areas
- Transmitting classified information by unsecured or unauthorized means
- Removing or sending classified material out of secured areas without proper authorization
- Unauthorized copying, printing, faxing, emailing, or transmitting classified material
- Improperly removing or changing classification markings
- Acquiring unauthorized access to classified or sensitive information systems
- Unauthorized storage of classified material, including unauthorized storage at home
- Reading or discussing classified information in an unauthorized area or over a non-secure communication device
- Discovery of suspected surveillance devices in classified areas
- Unexplained visits to foreign diplomatic facilities by a cleared employee

Suspicious Activities & Behaviors

- Short trips to foreign countries inconsistent with logical vacation travel or not part of official duties
- Trips to foreign countries inconsistent with an individual's financial ability and official duties
- Unexplained expensive purchases not logically supported by the individual's income
- Sudden reversal of a negative financial situation or repayment of large debts
- Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system content
- Receiving requests for protected information in the guise of price quote or purchase request, market survey, or other pretense
- Foreign entities targeting cleared employees traveling overseas via airport screening or hotel room incursions