Reporting Requirements and Examples

If you are unsure of what you are required to report, contact your FSO.
When in doubt, report an event or behavior to your FSO.

What to Report

The National Industrial Security Program Operating Manual (NISPOM) requires contractors to report certain events that affect:

- Status of facility clearance
- Status of employee's personnel security clearance
- Proper safeguarding of classified information
- Indication of classified information loss or compromise
- Possible cyber intrusions

Contactors must specifically report:

- Security violations
- Suspicious contacts
- Indications of:
  - Potential Insider Threats
  - Espionage
  - Sabotage
  - Terrorism
  - Subversive activity

Whom to Report To

Report to your:

- Facility Security Officer (FSO)*
- DSS Industrial Security Representative (IS Rep)
- DSS Counterintelligence (CI) Specialist

**Note: The contractor shall promptly submit a written report to the FBI with a copy to DSS regarding information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities.*

Examples of Reportable Events or Behaviors

The following is not intended to be an exhaustive list. When in doubt, report an event or behavior.

Recruitment

Report events or behaviors including, but not limited to:

- Contact with an individual associated with a foreign intelligence, security, or terrorist organization
- An offer of financial assistance by a foreign national other than close family
- A request for classified or unclassified information outside official channels
- Engaging in illegal activity or a request to do so

Information Collection

Report events or behaviors including, but not limited to:

- Requests to obtain classified or protected information without authorization
- Requests for witness signatures for destruction of classified information when destruction was not witnessed
- Operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed
- Presence of any listening or surveillance devices in sensitive or secure areas
- Unauthorized storage of classified material
- Unauthorized access to classified or unclassified automated information systems
- Seeking access to sensitive information inconsistent with duty requirements
- Making statements expressing support of or sympathy for a terrorist group
- Making statements expressing preference for a foreign country over loyalty to the U.S.
- Expressing radical statements or actions threatening violence against a coworker, supervisor, or others in the workplace

Information Transmittal

Report events or behaviors including, but not limited to:

- Unauthorized removal of classified or protected material from the work area without appropriate authorization
- Transmission of Classified material via unsecured means
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure telephone
- Concealment of foreign travel

Suspicious Behavior

Report behavior including, but not limited to:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements
- Repeated or un-required work outside of normal duty hours
- Unexplained or undue affluence
- Sudden reversal of financial situation or sudden repayment of large debts
- Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means
- Indications of terrorist activity

Derived from NISPOM Section 1-302