

---

# **COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)**

**A Practical Guide  
for Reporting  
Counterintelligence  
and Security Indicators**

Defense Personnel Security Research Center (PERSEREC)

---

---

# INTRODUCTION

Supervisors and coworkers are the first line of defense against espionage. The government relies on you to protect national security by reporting any behavior that you observe that may be related to a potential compromise of classified information. You are encouraged, sometimes obliged, by Executive Order, Presidential Decision Directive and U.S. Code, as well as by DoD Directives, Regulations, Instructions, to report such behaviors. However, judgment calls are often required by the potential reporter, and this often leads to indecision or choosing not to report anything.

Therefore, presented below is a focused list of serious counterintelligence- and security-related behaviors that, if observed or learned about, should be reported immediately to appropriate counterintelligence or security authorities. All these behaviors are serious and require little or no speculation.

Upon receiving your report, a security professional will follow up with appropriate verification. If you are at all uncertain, it is better to err on the side of reporting than not. The counterintelligence and security people will know how to handle your report.

The list of behaviors is not intended to be exhaustive. You should report any additional observed behaviors that may parallel or exceed the concerns listed in this brochure.

The brochure can be used by supervisors, coworkers, and security professionals in initial and refresher briefings and in counterintelligence briefings. By concentrating on direct counterintelligence- and security-related behavior, personnel in the field are likely to develop a better understanding of exactly what to report and a greater commitment to reporting it.

If you want only the CORE items,  
print the last four pages of this document.

---

---

# BACKGROUND

The Defense Personnel Security Research Center (PERSEREC) conducted research on how employees with clearance access understand the requirements to report suspicious behavior that they observe.\*

Finding: Supervisors and coworkers are willing to report on behaviors that have a clear connection to security, such as transmitting classified documents to unauthorized personnel, but they are unwilling to report on colleagues' personal problems, such as alcohol abuse. Because it was difficult to discern which reporting requirements were clearly related to security, there was very little reporting.

Outcome: PERSEREC, in collaboration with counterintelligence professionals, developed a clear, succinct list of "Coworker Reporting Essentials" (CORE) behaviors that could pose a possible threat to national security and thus should be reported if observed. The draft CORE was reviewed and edited by counterintelligence professionals at the Counterintelligence Field Activity (CIFA), and was coordinated by the DoD Investigative Working Group (IWG).

PERSEREC also coordinated with the DoD Counterintelligence Directorate in the Office of the Under Secretary for Defense (Intelligence), who included the PERSEREC CORE list in DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

---

\*Wood, S., & Marshall-Mies, J.C. (2003). Improving supervisor and coworker reporting of information of security concern. Monterey, CA: Defense Personnel Security Research Center.

---

# COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)

If you become aware of any of the following behaviors or activities, you should report them to your security officer or supervisor. These behaviors are derived from the DoD Instruction 5240.6 *Counterintelligence Awareness, Briefing, and Reporting Programs*.

## RECRUITMENT

Foreign intelligence entities are on the lookout for people who can be solicited to commit espionage against the U.S. At the same time, willing would-be spies often approach foreign intelligence operatives on their own initiative, thus volunteering for recruitment. It is a major task of counterintelligence to intercept these relationships. The recruitment cycle requires, first, that contact be established between the foreign intelligence agency and the potential spy, whether by direct recruitment or by volunteering. While the recruitment relationship almost always involves contacts with foreigners, an already-committed U.S. spy may approach you or a colleague on the job for recruitment into espionage.

## Reportable Behaviors

- ■ ■ you become aware of a colleague having contact with an individual who is known to be, or is suspected of being, associated with a foreign intelligence, security, or terrorist organization.
  - ■ ■ you discover that a colleague has not reported an offer of financial assistance by a foreign national other than close family.
  - ■ ■ you find out that a colleague has failed to report a request for classified or unclassified information outside official channels to a foreign national or anyone without authorization or need to know.
  - ■ ■ you become aware of a colleague engaging in illegal activity or if a colleague asks you to engage in any illegal activity.
-

---

# INFORMATION COLLECTION

Before classified or other kinds of sensitive materials can be passed to a foreign intelligence agency, they must be collected. They can simply be stolen (e.g., paper placed in a briefcase and taken out of the office), photographed, collected via computers, or obtained through eavesdropping or other surveillance devices. The computer age, with its e-mail and database capabilities, has offered new opportunities to potential spies for collecting data. While technical countermeasures can control some situations, it is up to coworkers to watch for and, if possible, identify breaches in the system that allow classified and sensitive information to be collected for espionage purposes.

## Reportable Behaviors

- ■ ■ a colleague asks you to obtain classified or other protected information in any format to which the person does not have authorized access.
- ■ ■ a colleague asks you to witness signatures for destruction of classified information when you did not observe the destruction.
- ■ ■ you observe a colleague operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed.
- ■ ■ you become aware of the existence of any listening or surveillance devices in sensitive or secure areas.
- ■ ■ you find out that a colleague has been keeping classified material at home or any other unauthorized place.
- ■ ■ you discover a colleague acquiring access to classified or unclassified automated information systems without authorization.
- ■ ■ you observe a colleague seeking to obtain access to sensitive information inconsistent with present duty requirements.



---

# INFORMATION TRANSMITTAL

In former days the transmittal of classified or sensitive information took the form of stealing documents and physically handing them to the foreign intelligence agent. In addition, spies could photocopy paper materials, smuggle materials out in briefcases, even illicitly take photographs in the workplace. Nowadays, there are many more opportunities to transmit information. With the advent of e-mail, faxes, and other technological capabilities, it is possible to transmit large quantities of information without being immediately caught. Coworkers must be aware of this problem and, if an illicit transmission is detected, report it directly and immediately to the designated cognizant counterintelligence or security authorities.

Once a relationship with a foreign intelligence agent is established and information begins to flow, illicit trips abroad by the recruited spy usually follow (meetings are easier to arrange abroad than in the U.S.). These journeys are often concealed by the person and the foreign contact is not reported. If you learn of such journeys or contacts, you should report.

## Reportable Behaviors

- ■ ■ you see someone removing classified material from the work area without appropriate authorization, either by physically taking it home or on travel, or by e-mailing or faxing it out of the office. The same rule applies for other protected materials, such as export-controlled or proprietary items.
- ■ ■ you observe a colleague using unclassified FAX or computer to transmit classified material.
- ■ ■ you observe a person improperly removing the classification markings from documents.
- ■ ■ you hear a colleague discussing classified information on a nonsecure telephone.
- ■ ■ you become aware that people with TS/SCI or contractors with a reporting requirement have attempted to conceal any work-related foreign travel and any personal foreign travel.



---

# SUSPICIOUS BEHAVIORS

The new DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs* (August 7, 2004) lists an additional series of eight items that, while not exactly clear-cut violations, have been traditionally considered behaviors that may well be connected to counterintelligence and security problems. These behaviors do require some degree of judgment before reporting. Often you might not know about them directly but only by hearsay. Often they may easily carry plausible alternative explanations. They are included here with the caveat that they do require a judgment call before reporting. If you are at all uncertain, it is better to report the behavior than to make no report at all.

- > 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, especially unaccompanied.
  - > Unexplained or undue affluence, including sudden purchases of high value items (e.g., real estate, stocks, vehicles, or vacations) where no logical income source exists. Attempt to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.
  - > Sudden reversal of financial situation or sudden repayment of large debts or loans.
  - > Attempts to entice DoD personnel into situations that could place them in a compromising position.
  - > Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money, or other means.
  - > 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.
-