PERSEREC

Technical Report 05-6
May 2005

Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers

Suzanne Wood
Consultant to Northrop Grumman Mission Systems

Kent S. Crawford
Eric L. Lang
Defense Personnel Security Research Center

Approved for Public Distribution:
Distribution Unlimited.

Research Conducted by
Defense Personnel Security Research Center

Technical Report 05-6 **May 2005**

Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers

Suzanne Wood
Consultant to Northrop Grumman Mission Systems

Kent S. Crawford
Eric L. Lang
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD·MM·YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
31-05-2005	Technical	2002-2005

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Suzanne Wood, Kent S. Crawford, Eric L. Lang	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER TR 05-6
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	10. SPONSORING/MONITOR'S ACRONYM(S) 11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT

PERSEREC recently conducted a study of supervisor and coworker reporting of security-related information. Explanations were offered by security managers and by focus group participants as to why many security-related behaviors are under-reported. The main problem is that people are hesitant to report suitability behaviors, such as excessive drinking, because they are not able to see a direct link between the particular human problem and national security. Consequently, PERSEREC developed a clear, succinct list of behaviors that could pose a potential threat to national security and thus should be reported if observed. Members of various counterintelligence agencies in the government reviewed and edited this list. It has since been included in the new DoD Instruction 5240.6 *Counterintelligence Awareness, Briefing, and Reporting Programs* as Enclosure 3. In addition, PERSEREC developed a brochure based on these items as an educational tool to help DoD components and other departments that have need of security education materials on supervisor and coworker reporting or for counterintelligence briefings.

15. SUBJECT TERMS

Supervisor reporting; coworker reporting; counterintelligence indicators

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF REPONSIBLE PERSON
Unlimited Distribution				57	James A. Riedel, Director
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER *(Include area code)* 831-657-3000

Preface

PERSEREC recently conducted a study of supervisor and coworker reporting of information of security concern. In response to our probing for answers as to why security-related behaviors are under-reported, interviewees and participants in focus groups said that policies were written too broadly for them to implement. The participants also said that they were very willing to report serious behaviors that clearly related to counterintelligence or security, but much less willing to report on suitability types of behaviors, such as excessive drinking and personal problems, because they were not able to see the direct link between the human problem and national security. They would prefer that these personal troubles be handled through employee assistance programs or other monitored treatment programs.

In response to these research findings, PERSEREC developed a list of Counterintelligence Reporting Essentials (CORE) that contained items that were primarily behavioral and clearly linked to counterintelligence and security risk. Working with the counterintelligence community, PERSEREC honed the list to 16 items. These 16 items were included as Enclosure 3 in the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

In addition, PERSEREC created a CORE brochure that can be disseminated throughout the counterintelligence and security communities. The brochure briefly discusses the rationale for developing the CORE list, describes potential uses by security professionals, and lists the specific behaviors that should be reported. The behaviors fall under the headings, Recruitment, Information Collection, Information Transmittal, and Suspicious Behaviors.

We believe the CORE list—as a new policy enclosure and an easy-to-read brochure—responds directly to the concerns of clearance holders in a way that is likely to improve security awareness and overall reporting of security-relevant behaviors.

James A. Riedel
Director

Acknowledgements

The authors would like to express their appreciation to a number of people who helped with this research. Thanks to Troy Sullivan and Windell Courson, staff members at the Department of Defense Counterintelligence Directorate, Office of the Under Secretary of Defense (Intelligence), who worked with the authors in deciding which of PERSEREC's reportable behaviors would be included as an Enclosure to the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs.*

PERSEREC's original CORE list had circulated in October 2002 among the staff of the Joint Counterintelligence Evaluation Office (JCEO) under Mary Griggs. JCEO then distributed the list to members of the DoD Investigative Working Group (IWG), representing Army Military Intelligence, Air Force Office of Special Investigations, Defense Intelligence Agency, Defense Security Service, National Security Agency, Naval Criminal Investigative Service, and the National Reconnaissance Office, and to a number of counterintelligence personnel at the Counterintelligence Field Activity (CIFA). We are grateful to these people for their helpful comments and suggestions. Many thanks also to Virginia Kirk at JCEO for her administrative and logistical assistance.

Executive Summary

Background

In January 2003, the Defense Personnel Security Research Center (PERSEREC) published a report of a study that examined the supervisor and coworker reporting requirement within the Department of Defense's (DoD) personnel security program (Wood & Marshall-Mies, 2003). The study dealt with self-initiated reporting, when a person would see a subordinate or colleague behaving inappropriately and report the behavior to Security. One of the aims of the study was to better understand the prevalence of workplace reporting, the kinds of behaviors that are reported, and the reasons people may not report. To this end, researchers interviewed 45 security managers and management personnel in 20 DoD and non-DoD federal agencies who described the reporting rate as very low, perhaps reflecting an under-reporting of relevant behaviors. They offered a series of explanations as to why people may not report, including cultural resistance; negative perceptions of reporting; lack of knowledge and experience of the system among security officers, supervisors, and the workforce; and unclear relationships between Security, employee assistance programs, and other functions.

The PERSEREC study also included several focus groups with supervisors and employees at various federal agencies to learn participants' views and recommendations concerning reporting. Focus group participants made it clear that they are willing to report egregious behaviors that they believe pose a likely threat to national security. They simply want to know precisely what such behaviors are. Wording of policy, in their opinion, is amorphous and confusing. All participants without exception said that they would seldom report certain gray-area behaviors that they describe as too personal ("the more private things," as one put it). Such behaviors may include emotional or mental, financial, alcohol and drugs, and marital problems, and unusual personal conduct. Research suggested that participants are reluctant to report these behaviors because they cannot see a link between the behavior and national security; in other words, they are unlikely to be convinced of the security relevance of personal problems. They may also be reluctant because they do not trust the system to deal with the reports equitably and also may fear possible reprisals to themselves as so-called whistleblowers.

In an attempt to end confusion about what should always be reported, the PERSEREC study recommended the development of a list of egregious behaviors that are closely connected to counterintelligence (CI) and security. The list would not include behaviors of a suitability or reliability nature since the research showed that supervisors and coworkers have said they would be unlikely to report such matters.

The present report documents the rationale for preparing the list and describes the processes by which it was developed and its eventual inclusion as Enclosure 3 in the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

Method

Research comprised the following steps: (1) comparison of major CI policy documents; (2) review of other source documents; (3) development of a draft Counterintelligence Reporting Essentials (CORE) list of behaviors that must be reported; (4) presentation of the draft CORE list for review and editing by CI experts; (5) introduction of the final CORE list into DoD policy; and (6) promulgation and implementation of the final CORE list, through the Defense Security Service (DSS) and other CI entities, for use in security and education programs and CI briefings.

Policy Review and Review of Other Source Documents

The various key policy documents that concern the reporting of CI and security-related behaviors were compared and contrasted, exploring areas of overlap, specificity, and authoritative procedures, i.e., whether one policy superseded another. Other documents and publications that have been developed by DoD, intelligence community agencies, and PERSEREC in the area of CI awareness and education were also reviewed. Examination of these documents provided background, context, and a pool of information from which PERSEREC researchers could draw as they developed the draft CORE list.

Development and Evaluation of Draft CORE List of Behaviors

PERSEREC researchers proceeded to pull together a draft CORE list of behaviors that are observable and may be associated with potential risk to national security. This became known as the CORE list.

The draft CORE list was evaluated by staff at the Joint Counterintelligence Evaluation Office (JCEO), the DoD Investigative Working Group (IWG), and by the Counterintelligence Field Activity (CIFA). The list was then reviewed by staff at the DoD Counterintelligence Directorate in the Office of the Under Secretary of Defense (Intelligence).

Introduction of Draft CORE List into DoD Instruction 5240.6

The 16 items in the final CORE list were added as an Enclosure to the revision of DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*.

Implementation of PERSEREC's Brochure in the Field

PERSEREC developed a separate brochure that includes the 16 original PERSEREC CORE list items, along with eight others added by the DoD Counterintelligence Directorate. This brochure, which explains the rationale for the list and its potential uses, is attached to this report as a pdf file and is detachable for use in the field.

Recommendation

DoD should distribute the PERSEREC brochure to CI and security agencies for their review and possible implementation. Possible uses include security education briefings of various sorts (e.g., initial, refresher, and CI awareness). By concentrating on direct CI- 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.

Table of Contents

Background

PERSEREC in 2003 published a report that studied self-initiated reporting, where supervisors and co-workers person observe suspicious behavior by a fellow worker (usually in the workplace) and report it to a supervisor or security official (Wood & Marshall-Mies, 2003).

During the course of the study, PERSEREC staff learned from several sources—extensive literature reviews, headquarters management personnel, and people working in the field—that, despite formal policies requiring employees to report security-related behaviors, they do so only rarely. Yet employees in the field are not averse to reporting genuine security infractions. In fact, under appropriate conditions, they are quite willing to act as eyes and ears for the government. They are simply confused about precisely what is important enough to report. Many government workers anguish over reporting gray-area behaviors they do not consider to be clearly connected to security. They say the policies are written too broadly for the average person in the field. One supervisor, echoing the opinion of many, said, "We need a clear communication of what is mandatory to report." A coworker complained, "You can't ask people to do something if you don't define it…We need more definitions. How do we know which behaviors are OK and which are not?"

One of the study recommendations, therefore, was that PERSEREC, in collaboration with counterintelligence (CI) professionals, develop a clear, succinct list of behaviors that could pose a potential threat to national security and thus should be reported if observed. This list, to be known as the Counterintelligence Reporting Essentials (CORE) list, would contain behavioral examples to clarify what is considered egregious or potentially critical to national security. Use of the CORE list should then facilitate reporting of truly significant behaviors. Behaviors that raise questions about reliability, the gray-area behaviors that interviewees said they would be less willing to report, would be handled by supervisors through counseling, employee assistance programs, or other monitored treatment programs. The goal was to produce a relevant and useful CORE list, which, through adoption as policy, could be employed to improve reporting requirements and security education programs.

Method

The research methodology to produce, review, and implement the CORE list required six steps: (1) comparison of major CI policy documents; (2) review of other source documents; (3) development of a draft CORE list of behaviors that must be reported; (4) presentation of the list to CI experts for review and editing; (5) introduction of the CORE list into Department of Defense (DoD) policy; and (6) promulgation and implementation, through the Defense Security Service (DSS) and other CI entities, for use in security and education programs and in CI briefings.

Policy Review

The purpose of this section is to report our review of all of the different policy documents related to supervisor and coworker reporting and to compare and contrast the requirements of various entities with regard to this subject. PERSEREC researchers reviewed the policies, Directives, and Executive Orders that concern the reporting of CI- and security-related behaviors. The review explored areas of overlap, specificity, and authoritative procedures, i.e., whether one policy superseded another.

The Clinton administration's Presidential Decision Directive PDD/NSC-12, *Security Awareness and Reporting of Foreign Contacts* (August 5, 1993) requires that government employees report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information, or the employee is concerned that he or she may be the target of actual or attempted exploitation by a foreign entity.

Executive Order 12968 (August 4, 1995) states in Sec. 6.2(a) that employees should protect classified information from unauthorized disclosure; report all contacts with persons, including foreign nationals, who seek to obtain classified information; report all violations of security regulations to appropriate security officials; and comply with all other security requirements of the order. It adds in Sec. 6.2(b): "Employees are also encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

Title 50, USC, Chapter 23, Subchapter 1, Sec. 797, lays out the penalties for violating security regulations at a variety of government facilities and under a variety of circumstances. Such a violation will constitute a misdemeanor and carry with it, upon conviction, a fine not to exceed $5,000 or imprisonment for not more than one year, or both.

The Director of Central Intelligence Directive (DCID) 6/4, *Personnel Security Standards* (July 2, 1998), lists (Annex E, 6 [a] – [m]) several general categories of behavior that are reportable if observed in the workplace. These are similar to the adjudicative guidelines (in the DoD Directive 5200.2-R) except that they do not include the brief behavioral descriptions that appear in the adjudicative guidelines. The categories, which—like the adjudicative guidelines—mix CI, security and reliability issues, are listed below. Only two—(b) and (c)—are strictly related to CI issues.

(a) Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.

(b) Foreign influence concerns/close personal association with foreign nationals.

(c) Foreign citizenship or foreign monetary interests.

(d) Sexual behavior that is criminal or reflects a lack of judgment or discretion.

(e) Unwillingness to comply with rules and regulations or to cooperate with security processing.

(f) Unexplained affluence or excessive indebtedness.

(g) Alcohol abuse.

(h) Illegal or improper drug use/involvement.

(i) Apparent mental or emotional disorder(s).

(j) Criminal conduct.

(k) Noncompliance with security requirements.

(l) Engagement in outside activities that could cause a conflict of interest.

(m) Misuse of information technology systems.

The 1996 DoD Instruction 5240.6 (*Counterintelligence [CI] Awareness and Briefing Program*) (July 16, 1996) differed significantly from the DCID 6/4. DoD Instruction 5240.6 is the fundamental, workhorse instruction for CI awareness and briefing programs for DoD. (For an analysis of the new DoD Instruction 5240.6, please see pp. 9-10 below.)

In the 1996 DoD Instruction 5240.6, the 13 reportable items from DCID 6/4 were described only briefly and included items that were not strictly CI-related, e.g., sexual behavior, alcohol abuse, illegal or improper drug use/involvement, apparent mental or emotional disorders. While several items were quite specific, e.g., behaviors such as contacts with foreign intelligence or terrorist organizations, requests for unauthorized access to classified or unclassified controlled information, contacts with known or suspected foreign intelligence officers, and contacts with foreign diplomats, the instruction went on to list (at 6.1.2) an amalgam of behaviors, strung together in one sentence and describing 10 broad areas that lack specificity and are often repetitive of themselves. "…DoD personnel who have information about activities pertaining to espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, unauthorized release of classified or unclassified controlled information, or unauthorized instructions into automated information systems."

The military services published their own instructions, based on the 1996 DoD Instruction 5240.6. The Air Force's AFI71-101V4, *Counterintelligence* (August 1, 2000), closely mirrors the 1996 DoD Instruction 5240.6, as does the Navy's SECNAVINST 3875.1A *Counterintelligence and Awareness Briefing Program* (February 19, 1999).

The Army, however, expands considerably on reporting requirements in its AR 381-12 *Military Intelligence Subversion and Espionage Directed Against the U.S. Army (SAEDA)* (January 15, 1993). In Chapter 3, *Reporting Requirements*, it addresses three areas: *SAEDA Incidents*, *Additional Matters of CI Interest*, and *Indicators of Espionage*. The segment on SAEDA incidents describes the incidents and situations that must be reported, these items reflecting the old DoD 5240.6 but in much more detail. The next section, *Additional Matters of CI Interest*, expands greatly the reportable behaviors. These include, for example, the discovery of listening devices; unauthorized absence of Department of the Army (DA) personnel with high-level clearances; reports of attempted or actual suicide; COMSEC insecurities; assassination (or attempts) of anyone by terrorists or agents of foreign powers; defection, or attempted or threatened defections; detention of personnel by a foreign government with interests inimical to those of the US; impersonation of DA intelligence personnel; willful compromise of the identify of US intelligence personnel engaged in clandestine intelligence and CI activities; and incidents in which foreign countries offer employment to US personnel involved in the development of nuclear weapons.

The third section of AR 381-12, *Indicators of Espionage*, lists 19 behaviors that may be indicative of espionage, although the regulation stresses that while a single indicator by itself does not necessarily mean that a person is engaged in espionage, it must be reported. This list is reproduced below:

(a) Any attempt to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities or attempting to obtain information for which the person has no authorized access or need to know.

(b) Unauthorized removed of classified materials from work area.

(c) Extensive use of copy, FAX or computer equipment to reproduce or transmit classified material that may exceed job requirements.

(d) Repeated or unrequired work outside normal duty hours, especially unaccompanied.

(e) Obtaining witness signatures on classified document destruction forms when witness did not observe the destruction.

(f) Bringing unauthorized cameras, recording devices, computers or modems into areas where classified data is stored, discussed, or processed.

(g) Unexplained or undue affluence, including sudden purchases of high-value items where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

(h) Opening several bank accounts containing substantial sums of money where no logical income source exists.

(i) Free spending or lavish display of wealth which appears beyond normal income.

(j) Sudden reversal of financial situation or sudden repayment of large debts or loans.

(k) Correspondence with persons in countries of special concern.

(l) Unreported contact with officials of countries of special concern.

(m) Frequent or unexplained trips of short duration to foreign countries.

(n) Attempts to offer extra income from an outside endeavor to personnel with sensitive jobs or to entice them into criminal situations that could lead to blackmail.

(o) Homesteading or repeatedly requesting extensions to tours of duty in one assignment or location, especially when the assignment offers significant access to sensitive information or the job is not desirable.

(p) Repeated involvement in security violations.

(q) Joking or bragging about working for a foreign intelligence service.

(r) Visits to a foreign embassy, consulate, trade, or press office.

(s) Business dealings with nationals or firms of countries of concern.

In summary, DoD Instruction 5240.6, flowing from higher-level policies such as a Presidential Decision Directive and an Executive Order, lays out the basic requirement for CI awareness and briefing programs in the DoD. Air Force and Navy wrote instructions that closely parallel the DoD instruction; the Army elaborated on the instruction, providing more details and specifics. Requirements vary somewhat from one entity to another. PERSEREC staff decided that a short, succinct list of reportable behaviors is needed rather than having supervisors, coworkers, and agencies deal with the plethora of different approaches and degrees of specificity found in the different policies.

Review of Other Source Documents

Having completed the policy review, PERSEREC staff reviewed a selection of publications and documents that have been developed by DoD, intelligence community agencies and PERSEREC in the area of counterintelligence awareness and education. These would provide the context and information required to construct PERSEREC's draft CORE list.

DSS published in January 1998 a For Official Use Only (FOUO) document, "Recognition of Potential Counterintelligence Issues." The document was intended to aid the facility security officers of cleared U.S. defense contractors in recognizing potential CI issues.

PERSEREC's *Employees' Guide to Security Responsibilities* has a section on CI indicators.[1] This contains 23 items grouped into five categories: (1) potential motivation, (2) potential indicators of information collection, (3) potential indicators of information transmittal, (4) potential indicators of illegal income, and (5) other potential indicators. (The Guide also has a list of security and suitability behaviors, organized according to the 13 adjudicative guidelines, e.g., alcohol consumption, allegiance to the United States, criminal conduct, drug involvement, etc.)

DoD 5220.22-M, *National Industrial Security Program Operating Manual* (January 1995), Section 1-300 General, under *Reporting Requirements*, states that contractors are required to report certain events that have an impact on the status of the facility clearance, impact on the status of an employee's personnel clearance, affect proper safeguarding of classified information, or indicate classified information has been lost or compromised. Contractors are required to establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the facility security officer, the FBI, or other Federal authorities as required by the Manual, the terms of a classified contract, and U.S. law. The manual states that contractors must provide complete information to enable the authorities to ascertain whether classified information is adequately protected. Contractors must submit reports to the FBI, and to their local security officials. This appears to be the only place in the National Industrial Security Program Operating Manual (NISPOM) where reporting requirements are mentioned.

DSS publishes an annual brochure for security professionals, CI personnel, and cleared contractors, *Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry.* The brochure is designed to help employees recognize suspicious contacts. The most frequent information-gathering method employed by foreign entities is simply to request information from individuals working in U.S. defense industry science and technology programs. The brochure lists indicators to watch for and appropriate security countermeasures to apply. Other methods include inappropriate conduct during visits;

[1]For more detail, see the *Employees' Guide to Security Responsibilities* on the Web at www.dss.mil/training/securityawareness.htm.

suspicious work offers; international exhibits, conventions and seminars; joint ventures/joint research; foreign acquisition of technology and companies; co-opting former employees; and targeting cultural commonalities. For each of these methods, DSS provides a list of indicators and recommended security countermeasures.

The following agency brochures and booklets were also reviewed:

- CIA orientation briefing, "Reporting of Security-Relevant Behavior Requirements"
- CIA brochure, "Why We Care: A Guide for Understanding Suitability and CI Indicators" (FOUO)
- DIA brochure, "Plenty of Excuses But No Good Reasons"
- DIA brochure, "Countering Espionage"
- DISA Newcomers' Briefing
- DSS's "Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed against the U.S. Defense Industry"
- DOE brochure, "Counterintelligence in our Changing World"
- DOE brochure, "Clues to Spotting a Spy"
- FBI "Security Handbook"
- Navy "Security Awareness Chronicle"
- NCIS list, "Indicators of Espionage"
- NIMA "MSSR," unclassified video briefing on espionage, recruitment, security, reporting requirements, etc.
- NSA booklet, "Foreign Intelligence Recruitment Approaches"
- State Department's booklet, "Counterintelligence for the 1990s and Beyond"

Each agency mentioned above had its own perspective on the subject of CI awareness programs, producing guides, learning tools, manuals, studies, handbooks, brochures and booklets that contain all the indicators and behaviors that agencies have considered to be of CI concern. Review of the above documents provided background and a pool of information from which PERSEREC researchers could draw as they prepared the draft CORE list. Researchers were able to cull items from the above publications and re-arrange them in a more systematic way that would make sense to employees in the field.

Development of Draft CORE List of Behaviors

Having reviewed the various policies and related materials listed above and compared and contrasted the strengths and weaknesses of each in terms of clarity and level of detail, PERSEREC researchers developed from the documents a list that included behaviors that should be reported when observed because they are genuine security violations or have serious CI significance. Researchers focused on behavioral items that clearly reflect security and CI risk. Items that were too vague, non-behavioral (e.g., that

required an observer to intuit another person's state of mind), or not clearly associated with a security risk were eliminated.

The draft CORE list was developed in a series of steps, each step building on the previous one. As we sequentially reviewed the documents listed below we added new items not covered in the previous documents until we reached a saturation point where we had captured all items that fell within our selection criteria, i.e., behaviors that are observable and may be associated with a risk to national security. The aim was to construct a list that was simple, short, effective, and credible to the reader. Below are listed the steps we followed in constructing the draft CORE list.

(1) Reviewed DCID 6/4 (13 adjudication guidelines).

(2) Compared DCID 6/4 with DoD Instruction 5240.6 "Counterintelligence Awareness and Briefing Program."

(3) Compared the above two documents with SAEDA regulations and unclassified briefing, "Indicators."

(4) Then added items from PERSEREC's "Employees' Guide to Security Responsibilities."

(5) Then reviewed assorted agency brochures and booklets to see what reportable behaviors might have been missed.

(6) Incorporated all the behaviors culled from the above materials into one list, using as the selection criterion the fact that the behavior clearly should be reported because it is a CI- or security-related violation. The draft CORE list was then carefully reviewed by a panel of five additional researchers at PERSEREC who attempted to eliminate any items that were essentially non-behavioral (e.g., mostly required judgment calls on the part of the potential reporter).

Having developed a draft CORE list, it was important to have it evaluated by professional CI experts.

Evaluation of Draft CORE List by Counterintelligence Experts

In October 2002, the draft CORE list was circulated among the staff of the Joint Counterintelligence Evaluation Office (JCEO) for their review. In turn, JCEO distributed the list to members of the DoD Investigative Working Group (IWG) and to a number of retired FBI officials working for the Counterintelligence Field Activity (CIFA). These individuals provided editorial and substantive comments on the draft CORE list, and their responses were incorporated. The list was then reviewed in April 2003 by CI personnel in the DoD Counterintelligence Directorate under the Office of the Under Secretary of Defense (Intelligence) (OUSD[I]). Directorate staff reviewed the items and made

valuable changes to some. Of PERSEREC's original 30 items, the CI staff advised PERSEREC to reject three, either because the items were not supported by policy or because items raised legal concerns. PERSEREC staff subsequently eliminated these three and eliminated an additional item because it duplicated another. A few items were combined.

Introduction of Draft CORE List into DoD Instruction 5240.6

PERSEREC reviewed an early draft of the new DoD Instruction 5240.6, *Counterintelligence Awareness, Briefing, and Reporting Programs*, dated April 21, 2003, for potential coordination with the CORE list. PERSEREC staff members worked with DoD Counterintelligence Office staff who wrote the instruction and wanted to include PERSEREC's draft CORE list into the new instruction. The instruction was promulgated August 7, 2004.

The instruction, in Item 6 *Procedures*, adds a new section (6.1.) that discusses awareness and briefing programs. It then describes in 6.1.3. the kinds of information that must be included in CI briefings: information about early detection of espionage and other suspected foreign intelligence and terrorist activities; comprehensive tailored threat information focusing on foreign intelligence, terrorism and other threats; information about the DoD anomalies program;[2] and reporting responsibilities and procedures. In Item 6.2, *Reporting Requirements*, the new instruction states (at 6.2.1) that DoD personnel "shall report information pursuant to E.O. 12968 and DoD 5200.2-R…concerning security violations and other information with potentially serious security significance regarding someone with access to classified information employed in a sensitive position." The new instruction refers the reader to an Enclosure 3, where specific behaviors that must be reported are listed. This is an extremely important device that provides the reader explicit examples of reportable behavior.

Item 6.2.2 states "DoD personnel shall expeditiously report any contacts or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national security information…or controlled unclassified information…" These are relatively vague terms, but then 6.2.3 proceeds to list several explicit counterintelligence circumstances in which contacts must be reported. These include requests of people for unauthorized access to classified information; when contacts may indicate that DoD personnel may be targets for exploitation; contacts with intelligence officers from any country; contacts where information is received about terrorism, espionage, sabotage, subversion, or other intelligence activities; intrusions into U.S. automated information systems; contacts with foreign government interests that may be reportable under separate procedures (e.g., for attaches or arms control negotiators); and other situations where personnel hold sensitive positions and may be required to inform

[2] Pursuant to White House Memorandum, *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, August 23, 1996 and ASD(C3I) Memorandum, *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, October 15, 1996.

their commanders of the nature of any intended contact with a foreign diplomatic establishment. For the full wording on the above items, please see Item 6.2, *Reporting Requirements*, on pp. 6-7 of the new instruction.

The new DoD Instruction 5240.6 is creative and forward-looking in that it sets out a specific and explicit set of CI behaviors that should be reported and then refers the reader to Enclosure 3 where a further set of behaviors is listed. Prompted by the CI Directorate's review of PERSEREC's draft CORE, this is the first time that such a list has been included in any such instruction.

DoD Instruction 5240.6, Enclosure 3, contains 14 items taken directly from PERSEREC's CORE list of 16 items. These are behaviors that are clear violations and must be reported immediately; no judgment is required of the person reporting. The CI Directorate added other items to Enclosure 3. These additions were the kinds of items that had initially been rejected by researchers at PERSEREC who recognized such items as potentially security-relevant but: (1) were open to different interpretations that might have little bearing on security, or (2) were behaviors that could not normally be known to a supervisor or coworker. These additional items, several borrowed from the Army's SAEDA list, included volunteering for assignments beyond the normal scope of responsibilities; use of copy machines, faxes or computers to transmit materials that may exceed job requirements; working outside normal duty hours; unexplained or undue affluence; sudden reversal of a bad financial situation or repayment of large debts; attempts to entice DoD personnel into situation that could place them in a compromising position; attempts to place DoD personnel under obligation through special treatment; and short trips to foreign countries or travel within the US for reasons that appear unusual or inconsistent with a person's interests or financial means. Counterintelligence Directorate staff included these items because they have been previously mentioned in policy and have thus traditionally been part of a set of behaviors of possible security concern.

Implementation of CORE Brochure in the Field

After PERSEREC's CORE list was included in policy, PERSEREC transformed it into a brochure for use in the field. The brochure is designed for distribution to DoD components and other departments and agencies that have a need for security education materials and educational tools in the area of supervisor and coworker reporting. It contains the rationale for creating the CORE list so that people using it in the field will understand why items are included. Reportable behaviors are then presented in three major categories: (1) recruitment, (2) information collection, and (3) information transmittal. A fourth section contains a number of discretionary items, i.e., behaviors that are worth noting if one observes them. This fourth section in the brochure is labeled Suspicious Behaviors and is included because the items have long been covered in policy. (Please see the PERSEREC brochure at Appendix B.)

Recommendation

DoD should distribute the CORE brochure and its developmental rationale to CI and security agencies for possible implementation. Potential uses include security education briefings of various sorts (e.g., initial, refresher, and CI awareness) and distribution to cleared personnel. By concentrating on direct CI- 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.

References

Wood, S., & Marshall-Mies, J.C. (2003). *Improving supervisor and coworker reporting of information of security concern* (PERS-TR-02-3). Monterey, CA: Defense Personnel Security Research Center.

Appendix A

Department of Defense Instruction 5240.6 (August 7, 2004)

Department of Defense

INSTRUCTION

NUMBER 5240.6
August 7, 2004

USD(I)

SUBJECT: Counterintelligence (CI) Awareness, Briefing, and Reporting Programs

References: (a) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness and Briefing Program," July 16, 1996 (hereby canceled)
(b) Presidential Decision Directive/NSC No.12,[1] "Security Awareness and Reporting of Foreign Contacts," August 5, 1993
(c) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997
(d) Executive Order 12829, "National Industrial Security Program," January 6, 1993
(e) through (y), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a), implements reference (b) within the Department of Defense (DoD), and establishes procedures for conducting and administering DoD counterintelligence awareness, briefings and reporting as required by reference (c).

1.2. Provides procedures for the handling of other threat information affecting the security of DoD personnel, information, resources, installations, and operations.

1.3. Reaffirms the requirement for a foreign intelligence and international terrorist threat awareness and briefing programs for DoD military, civilian employee, and contractor personnel.

[1] Authorized users may contact the CI Directorate, DUSD(CI&S), USD(I), Room 3C260, Pentagon for a copy.

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. DoD contractor personnel with security clearances for their briefing and reporting requirements as specified under E.O. 12829 (reference (d)), (hereafter referred to collectively as "the DoD contractors").

2.3. Active and Reserve military personnel, DoD civilian employees, and DoD contractors (hereafter collectively referred to as "the DoD personnel").

3. DEFINITIONS

Definitions for this Instruction are in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The DoD personnel report any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD or other U.S. resources, and classified national security information (hereafter referred to as "classified information"), or controlled unclassified information under E.O. 12958, DoD Directive 5230.24, DoD 5400.7-R, and DoD Directive 5210.83 (references (e) through (h)) to an appropriate authority. Judicial and/or administrative action may be taken when DoD personnel fail to report such required information.

4.2. The DoD personnel shall receive periodic briefings on the threats posed by foreign intelligence services, international terrorists, computer intruders and unauthorized disclosures, and individual reporting responsibilities. This shall include insider threats and the crimes of spying and treason.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall oversee the DoD Counterintelligence (CI) awareness, briefing, and reporting programs and ensure:

5.1.1. The Deputy Under Secretary of Defense (Counterintelligence and Security) (DUSD(CI&S)) shall establish and sustain the DoD CI awareness, briefing, and reporting programs.

5.1.2. The Director, Counterintelligence, under the DUSD(CI&S), shall:

5.1.2.1. Recommend policy on CI awareness, briefing, and reporting programs to the DUSD(CI&S) and the USD(I).

5.1.2.2. Provide oversight to the DoD CI Program.

5.1.2.3. Participate in DoD and national-level forums concerning CI awareness, briefing, and reporting programs.

5.1.2.4. Serve as the staff point of contact within OSD for issues related to CI awareness, briefing, and reporting programs.

5.1.3. The Director, Counterintelligence Field Activity (CIFA), under the DUSD(CI&S), shall:

5.1.3.1. Manage and provide functional oversight of the Department's CI awareness, briefing, and reporting programs.

5.1.3.2. Brief the USD(I) on significant CI investigative referrals received pursuant to this Instruction in accordance with DoD Directive 5105.67 (reference (i)).

5.1.3.3. Recommend policy changes through the DUSD(CI&S) to the USD(I).

5.1.3.4. Provide additional training to Component CI personnel on the skills required for the CI awareness, briefing, and reporting programs.

5.1.3.5. Represent the Department with other Government and management agencies regarding implementation of all DoD CI matters pursuant to reference (i).

5.1.4. The Director, Defense Security Service, under the DUSD(CI&S), shall recommend changes to DoD 5220.22-M (reference (j)) to the DUSD(CI&S), to implement this Instruction within cleared defense contractor facilities.

5.2. The Heads of the DoD Components shall:

5.2.1. Develop and implement CI briefing, awareness, and reporting programs within their organizations.

5.2.2. Promptly report any CI information developed from these programs to their organic or lead CI agency and to the CIFA pursuant to USD(I) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003 (reference (k)).

5.2.3. Establish time-sensitive reporting procedures pursuant to paragraph 6.3., below, for the DoD personnel during official or non-official overseas travel.

5.2.4. Ensure Component CI agencies report CI information through the Portico system.

5.2.5. Ensure Component CI agency CI information is appropriately documented in the Portico system. Information collected responsive to validated collection requirements shall be published via Intelligence Information Report on the Portico system.

5.3. The Director, Defense Intelligence Agency, shall, in addition to the responsibilities listed in paragraph 5.2., above, and in coordination with the Director, Joint Staff, develop and implement CI awareness, briefing, and reporting programs for the Chairman, Joint Chiefs of Staff.

5.4. Defense Agencies with organic CI organizations shall:

5.4.1. Ensure reported information regarding contractor personnel is referred to the Defense Security Service (DSS) and the Federal Bureau of Investigation (FBI).

5.4.2. Ensure reported information regarding military or DoD civilian personnel is referred to the appropriate Military Department CI agency or the FBI, as appropriate. Any information reported to the FBI shall also be reported to the CIFA pursuant to DoD Instruction 5240.4 (reference (l)).

5.5. The Secretaries of the Military Departments shall:

5.5.1. Ensure Department CI agencies refer reported information regarding contractor personnel to the DSS and the FBI.

5.5.2. Refer reported information regarding DoD civilian employees to the FBI for possible CI investigative or operational action where the Department does not otherwise have investigative authority. Any information reported to the FBI shall also be reported to the CIFA pursuant to reference (l).

6. PROCEDURES

6.1. Awareness and Briefing Programs

6.1.1. The DoD awareness and briefing programs shall promote threat and reporting awareness responsibility, enable DoD personnel to identify CI threats, and the reporting of suspicious situations and incidents to appropriate authorities.

6.1.2. Threat awareness may be enhanced through a variety of methods, including but not limited to publications, posters, live presentations, and recorded media.

6.1.3. CI Briefings shall include:

6.1.3.1. Information about early detection of espionage and other suspected foreign intelligence and international terrorist activities to include the crimes of sabotage, subversion, treason, and spying.

6.1.3.2. Comprehensive, tailored threat information focusing on foreign intelligence, international terrorism, and other threats to include insider threats relevant to the DoD Component's mission, functions, activities and locations.

6.1.3.3. Information addressing the DoD anomalies program pursuant to White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996 and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996 (references (m) and (n)), which remain in effect.

6.1.4. Briefings shall be presented at or near the time of initial entry or hire and thereafter at least every 12 months. More frequent briefing intervals should be instituted if conditions warrant. Some DoD Component organizations or personnel may require more frequent briefings predicated on the nature of their duties.

6.1.5. Briefings should be presented by the Component CI agency when feasible. If the servicing Component CI agency is not used, the briefings should be coordinated with them for content and accuracy.

6.1.6. Briefings conducted pursuant to this Instruction do not satisfy the requirement of DoD Directive 2000.12 (reference (o)).

6.2. Reporting Requirements

6.2.1. The DoD personnel shall report information pursuant to E.O. 12968 and DoD 5200.2-R (references (p) and (q)) concerning security violations and other

information with potentially serious security significance regarding someone with access to classified information or who is employed in a sensitive position. Examples of information or observed behaviors that should be reported are listed in enclosure 3.

6.2.2. Pursuant to this Instruction, the DoD personnel shall expeditiously report any contacts or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national security information or controlled unclassified information to an appropriate DoD authority.

6.2.2.1. Appropriate authorities for active duty and Reserve military personnel and DoD civilians and DoD contractors working in DoD Component facilities include security officers, supervisors, commanders, and organic or lead CI agencies. Security officers, supervisors, and commanders shall expeditiously refer any information they receive pursuant to this Instruction to their supporting CI agency.

6.2.2.2. Appropriate authorities for DoD contractors at cleared contractor facilities shall include Facility Security Officers, Military Department CI Agencies, the FBI, or the DSS pursuant to reference (l).

6.2.3. The DoD personnel shall report contacts pursuant to the following situations:

6.2.3.1. A request by anyone, regardless of nationality, for unauthorized access to classified information under DoD 5200.1-R (reference (r)); controlled unclassified information under references (f), (g), and DoD Directive 5230.25 (reference (s)); or information systems containing such information.

6.2.3.2. Contact with an individual, regardless of nationality, under circumstances that suggest the DoD personnel may be the target of an attempted exploitation by a foreign intelligence service or international terrorist organization.

6.2.3.3. Contact with a known or suspected intelligence officer from any country.

6.2.3.4. Contact with anyone receiving information of planned, attempted, actual, or suspected international terrorism, espionage, sabotage, subversion, or other intelligence activities against the Department of Defense, other U.S. facilities, U.S. organizations, or U.S. citizens.

6.2.3.5. Actual or attempted unauthorized access into U.S. automated information systems and/or unauthorized transmissions of classified or controlled unclassified information over on-line computer services and telephones.

6.2.3.6. Close and continuing associations with foreign nationals may also be reportable under Director of Central Intelligence Directive (DCID) 6/1, reference (t) and DCID 6/4, reference (u).

6.2.3.7. In addition to the aforementioned reporting requirements, personnel who occupy positions designated by their DoD Component as sensitive shall apprise their commanders or supervisors of the nature and purpose of any intended contact with any foreign diplomatic establishment whether in the United States or abroad.

6.3. Sanctions. The DoD personnel who fail to report information required by this Instruction may be subject to judicial and/or administrative action under applicable law and regulations, including the Uniform Code of Military Justice (reference (v)), and other applicable sections of the United States Code.

6.4. Other

6.4.1. DoD acquisition program personnel working with Critical Program Information pursuant to DoD Directive 5200.39 (reference (w)) shall notify their servicing security personnel of all projected foreign travel. Such personnel shall receive foreign intelligence threat briefings and anti-terrorism briefings prior to overseas travel.

6.4.2. The DoD personnel with access to Sensitive Compartmented Information (SCI) pursuant to DCID 1/20 (reference (x)) incur special security obligations that include advance foreign travel notification for official and/or unofficial travel and defensive travel briefings.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Stephen A. Cambone
Under Secretary of Defense for Intelligence

Enclosures - 3
- E1. References, continued
- E2. Definitions
- E3. Examples of Reportable Employee Behaviors

E1. ENCLOSURE 1

REFERENCES, continued

(e) Executive Order 12958, "Classified National Security Information," April 17, 1995
(f) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(g) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(h) DoD Directive 5210.83, "Department of Defense Unclassified Nuclear Information (DoD UCNI)," November 15, 1991
(i) DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002
(j) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1999
(k) Under Secretary of Defense (Intelligence) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003
(l) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 22, 1992
(m) White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996[2]
(n) Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996[3]
(o) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(p) Executive Order 12968, "Access to Classified Information," August 2, 1987
(q) DoD 5200.2-R, "Personnel Security Program," January 1987
(r) DoD 5200.1-R, "DoD Information Security Program," January 16, 1997
(s) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
(t) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995[4]
(u) Director of Central Intelligence Directive 6/4, "Personnel Security Standards," July 2, 1998[5]
(v) Section 801-940, Chapter 47, of title 10, United States Code, "Uniform Code of Military Justice"
(w) DoD Directive 5200.39, "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection," September 10, 1997

---

[2] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.
[3] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.
[4] Available to authorized users via DoD Secure Internet Protocol Route Network (SIPRNET).
[5] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

(x) Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI)," December 29, 1991[6]
(y) Sections 792-799, Chapter 37 of title 18, United States Code

[6] Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

E2. ENCLOSURE 2

DEFINITIONS

E2.1. DEFINED TERMS

E2.1.1. Anomalies. Foreign power activity or knowledge suggesting foreign knowledge of U.S. national security information, processes or capabilities.

E2.1.2. Classified Information. Information requiring protection in the interest of national security, classified "TOP SECRET, SECRET, or CONFIDENTIAL" according to reference (x).

E2.1.3. Contact. Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact for social, official, private, or other reasons.

E2.1.4. Controlled Unclassified Information. Data bearing distribution limitation statements such as "For Official Use Only" in accordance with reference (g) and other information marked under references (f) and (g).

E2.1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

E2.1.6. Counterintelligence Investigations. Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

E2.1.7. Defensive Travel Briefings. Formal advisories alerting personnel of the potential for harassment, exploitation, provocation, capture, or entrapment while traveling. These briefings, based on actual experience when available, include

information on courses of action helpful in mitigating adverse security and personnel consequences and advise of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

E2.1.8. DoD Component CI Organizations. The organic CI elements of the Army, the Navy, the Air Force, the Marine Corps, the Joint Staff, the Combatant Command Staffs, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Defense Security Service, the Defense Threat Reduction Agency, and the Missile Defense Agency and the CIFA.

E2.1.9. Espionage. Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference (y)) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference (v)).

E2.1.9.1. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace.

E2.1.9.2. Reference (y) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial.

E2.1.9.3. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (y).

E2.1.9.4. Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (y).

E2.1.9.5. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (y).

E2.1.10. Foreign Diplomatic Establishment. Any embassy, consulate, or interest section representing a foreign country.

E2.1.11. Lead CI Agency. A Military Department CI Agency that has been designated by the USD(I) to provide defined levels of CI support to one or more of the DoD Components.

E2.1.12. Military Department CI Agencies. The Military Department CI Agencies include the U.S. Army Counterintelligence, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

E2.1.13. National Security. A collective term encompassing both national defense and foreign relations of the United States.

E2.1.14. Portico. A program managed by the CIFA to provide automation support, through web-enabled software hosted on a robust infrastructure, to the DoD CI Community. Portico enables CI enterprise business processes; facilitates information sharing, and coordination across DoD Services and Agencies; and provides management tools for each CI functional area, as well as supporting tools and services for managing the CI process in the functional areas of Collection; Investigations; Analysis and Production; Operations; and CI Functional Services.

E2.1.15. Sabotage. An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (y).

E2.1.16. Spying. During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere.

E2.1.17. Subversion. An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the United States.

E2.1.18. Terrorism. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

E2.1.19. Treason. Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2831 of title 18, U.S. Code, reference (y)).

E2.1.20. Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

E3. ENCLOSURE 3

EXAMPLES OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1. LIST OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1.1. Unauthorized contact with an individual who is known or suspected of being associated with a foreign intelligence, security, or terrorist organization.

E3.1.2. Illegal activity, conduct or requests for participation in illegal activities or other conduct that might make someone susceptible to blackmail or result in a security violation.

E3.1.3. Reading or discussing classified or controlled unclassified information in an unauthorized location, such as while using public transportation.

E3.1.4. Attempts to obtain classified or other protected information in any format to which the requesting person does not have authorized access.

E3.1.5. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

E3.1.6. Unauthorized possession and/or operation of cameras, recording devices, computers, or modems in areas wherein classified information and data are stored, discussed, or processed.

E3.1.7. The existence or use of any unauthorized listening or surveillance devices in sensitive or secure areas.

E3.1.8. Keeping classified material at home or any other unauthorized place.

E3.1.9. Acquiring access to classified or unclassified automated information systems without proper authorization.

E3.1.10. Transmitting classified material over unclassified FAX or computer.

E3.1.11. Seeking to obtain access to sensitive information inconsistent with present duty requirements.

E3.1.12. Removing classified or controlled unclassified material from work areas without appropriate authorization by any means.

E3.1.13. Improperly removing security classification markings from documents.

E3.1.14. Discussing classified information on a non-secure, unencrypted telephone.

E3.1.15. Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities.

E3.1.16. Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements.

E3.1.17. Repeated or un-required work outside of normal duty hours, especially unaccompanied.

E3.1.18. Unexplained or undue affluence, including sudden purchases of high value items (i.e., real estate, stocks, vehicles, or vacations) where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

E3.1.19. Sudden reversal of a bad financial situation or repayment of large debts.

E3.1.20. Attempts to entice DoD personnel into situations that could place them in a compromising position.

E3.1.21. Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money or other means.

E3.1.22. 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.

Appendix B

COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE)

A Practical Guide for Reporting Counterintelligence and Security Indicators

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 colleagues 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.