PERSEREC

Technical Report 02-3
January 2003

Improving Supervisor and Coworker Reporting of Information of Security Concern

Suzanne Wood
Defense Personnel Security Research Center

Joanne C. Marshall-Mies
Swan Research, Inc.

Research Conducted by
Defense Personnel Security Research Center

Technical Report 02-3 **January 2003**

Improving Supervisor and Coworker Reporting of Information of Security Concern

Suzanne Wood
Defense Personnel Security Research Center

Joanne C. Marshall-Mies
Swan Research, Inc.

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, California 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)*
January 2003	Technical	December 2000 - September 2002

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Improving Supervisor and Coworker Reporting of Information of Security Concern	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Suzanne Wood Joanne C. Marshall-Mies	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Defense Personnel Security Research Center 99 Pacific Street, Bldg. 455-E Monterey, CA 93940-2497	Technical Report 02-3
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITOR'S ACRONYM(S)
Defense Personnel Security Research Center 99 Pacific Street, Bldg. 455-E Monterey, CA 93940-2497	11. SPONSORING/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT	
13. SUPPLEMENTARY NOTES	

14. ABSTRACT
PERSEREC examined government requirements that cleared supervisors and employees report to security managers behavior they observe among subordinates and coworkers that they believe to be security-relevant. Despite formal policies, very few reports are made. Authors reviewed research literature and discussed the topic with personnel security and management personnel in 20 government agencies and with supervisors and coworkers in focus groups. While supervisors and employees are not averse to reporting genuine security infractions, they rarely report other behaviors. They are confused about precisely what to report and anguish over reporting gray-area behaviors they do not consider to be necessarily connected to security. The study recommends that DoD Directive 5200.2-R be modified to include supervisor and coworker reporting as a priority and to protect the confidentiality of people who report, if requested. It recommends that PERSEREC, with the help of counterintelligence and security personnel, develop a list of behaviors that pose a palpable threat to national security and must be reported, if observed. The list will contain behavioral examples to clarify what is considered egregious and critical to national security. It is also recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD [C3I]) issue a memorandum advising certain changes be made in the government's philosophy, i.e., that the personnel security community be more proactive in ensuring that personal problems get addressed before they become security problems. The memorandum should also emphasize enhanced training, including developing clear guidance as to what *must* be reported and making the personnel security system more accessible and transparent to employees. It also recommends that the Joint Personnel Adjudication System (JPAS) Program Office develop a system for tracking supervisor and employee reports, and that PERSEREC field a series of surveys in DoD to establish much-needed trend data on the incidence of security-related behaviors and the reporting of such behaviors.

15. SUBJECT TERMS
Security-relevant reporting requirements, security policy, supervisor and coworker reporting

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

Preface

Federal and departmental policies are designed to ensure that the cleared workforce is reliable, trustworthy, and loyal. One of these policies requires supervisors and coworkers who work in classified environments to report to security managers any behavior they observe among workplace colleagues that may be of security concern. Supervisors and coworkers also are required to report security-related concerns during periodic reinvestigation (PR) interviews. In essence, supervisors and coworkers are being asked to be the eyes and ears of the government since they are in the best position to observe behaviors that might suggest a risk to national security.

Anecdotal and empirical evidence gathered prior to this study suggested that, although supervisors report more often than coworkers, self-initiated reporting (i.e., reporting initiated by supervisors and coworkers on their own without being prompted or questioned by an investigator), along with reporting rates during PR investigations, are very low.[1] Supervisors and coworkers are reluctant to inform security managers about many behaviors that they observe in the workplace, unless the behaviors are egregious and are obviously related to national security. Tension exists between government requirements and supervisors' and employees' willingness to report.

The current study examined present reporting policies, described supervisor and employee reporting behavior, and recommended ways to reduce the disconnect between reporting requirements and reporting behavior. The ultimate aim was to recommend changes in policy and practice that might lead to the establishment of conditions under which supervisors and coworkers would be more likely to report egregious security-relevant behaviors.

This report includes a comprehensive review of current security policy and research literature concerning supervisor and coworker reporting. It describes the views of security policymakers and practitioners at headquarters concerning implementation of reporting requirements and the opinions of supervisors and employees in the field on how the problem of reporting is handled at the grass-root level. It also describes these individuals' recommendations for changing reporting policy and how it is implemented.

Results of the study will be of primary interest to Department of Defense (DoD) policymakers who administer security policy. The study will also be of use to security professionals responsible for making personnel security decisions and ultimately to supervisors and employees in classified environments. These people all share a desire to make the personnel security system more effective so that espionage and other compromises of classified information can be prevented.

---

[1]During PRs, supervisors and employees are asked direct questions by investigators about cleared employees who are undergoing a security review. In this report, responses to the direct questioning of investigators during a PR are distinguished from self-initiated reporting which occurs between PRs and is the result of supervisors or employees voluntarily reporting to the security manager or supervisor a security-relevant behavior of a cleared colleague that they have observed in the workplace.

The report's Executive Summary is a synopsis of the larger report and is designed for the policymaker. The larger report contains in detail all the findings and will be of special interest to someone wishing to acquire a deeper understanding of this subject.

James A. Riedel
Director

Acknowledgements

The authors would like to thank the many managers, supervisors, and employees in the military services, Department of Defense (DoD) agencies, and non-DoD agencies, both at headquarters and in the field, who supported this study and provided valuable input. We promised all interviewees that they would not be identified in this report. However, we would like to express our gratitude for the time they took to describe reporting policy and its application within the workplace. We value their insights concerning impediments to reporting and their recommendations concerning how reporting policy can become more effective.

We are also appreciative of the individuals who volunteered to participate in the focus groups. Their perspectives as supervisors and employees helped us understand the context in which reporting may take place and the reasons why others in the workforce may be reluctant to report their subordinates and coworkers.

Executive Summary

The Problem

In the Department of Defense (DoD) personnel security system, once people receive security clearances they are subject to continuing evaluation over time to ascertain their continuing reliability, trustworthiness and loyalty. If a security manager receives a report that is indicative of a security-related issue in a cleared employee's life, the report is forwarded to a central adjudication facility where the issue is evaluated. Such continuing evaluation reports come from a variety of sources, such as police departments, credit bureaus, periodic reinvestigations (PRs), etc. However, information from these sources cannot possibly cover all aspects of an employee's life or raise real-time questions about the employee's behavior. To fill this vacuum, the government asks supervisors and coworkers to help out as its eyes and ears and to report issues that may potentially impact national security. The present Defense Personnel Security Research Center (PERSEREC) study examines this specific and important aspect of the continuing evaluation program.

Supervisors and coworkers who work in classified environments are required by Federal policy (Executive Order 12968, 1995, Director of Central Intelligence (DCI) policy (e.g., DCID 6/4, 1998), and DoD policy (e.g., DoD Directive 5200.2, 1999 and 5200.2-R, 1987, revised 1996) to report immediately to security managers any behavior they observe among workplace colleagues that may be of security concern. They also are required to report such behaviors during PR interviews. The study primarily focused on self-initiated reports and only secondarily on reports made during PR interviews.

Since they are in the best place to observe workplace behaviors, supervisors and coworkers can serve as adjuncts to the implementation of security policies. In theory, the supervisor and coworker reporting of security-relevant behavior should play a key role in the continuing evaluation of cleared personnel. In fact, there appears to be a tension between the requirement to report and supervisors' and employees' willingness to adhere to the policy.

The following examples illustrate the importance of the problem of supervisor and coworker reporting, for they place the subject in a context directly related to espionage and its consequences.

While espionage cases are statistically rare, spies have in fact been caught as a result of supervisor and coworker reporting. A famous case described widely in the media was that of Jonathan Pollard, a Naval intelligence analyst arrested for espionage on behalf of Israel, whose arrest was the result of, first, a supervisor's suspicion and then a coworker's report. Pollard's supervisor had had doubts about him, not only when he was caught lying about his dealings with another government agency but also when the supervisor noticed that he was late in completing work assignments. He was also requesting so many Top Secret documents that it was becoming a burden on the clerk

who had to log them in. For these and other reasons, the supervisor perceived Pollard as an undesirable employee and resolved to get rid of him. He did not suspect a security problem, however, until a coworker reported seeing Pollard take a package of Top Secret material out of the building late on a Friday afternoon and get into a car with his wife. Investigations confirmed that Pollard was regularly removing and compromising large quantities of highly classified documents (Blitzer, 1989).

The colleagues of Navy spy, Jerry Whitworth, observed him monitoring and copying a sensitive communications line without authorization, saw classified papers in his personal locker, and knew he took classified materials home. However, they assumed he was doing it only to keep his work current (Barron, 1987). None of these coworkers reported the activities before Whitworth's arrest as part of the John Walker spy ring. Their failure to inform security personnel about Whitworth's activities allowed the Walker ring to continue, with significant damage to national security.

Supervisors and coworkers are not just being asked to report on a person whose behavior is inappropriate. They are in a position to help their colleagues get treatment before problems result in compromise of security or loss of their jobs. One convicted spy, Jeffrey Carney, in an interview from prison, spoke of how he wished someone had stepped forward to give him the help he needed; this might have prevented his committing espionage. "If you want to do people with problems a favor—and I'm talking from experience—say something!... If somebody had said, 'I think Jeff's got a problem and I don't think that he's handling it very well. Supervisor, do something,' that would have been enough to stop the process, at least for a while" (NIMA, 2000). The problem is that most people are hesitant—for a variety of culturally imbued reasons—about reporting or, as they may see it, *informing* on their subordinates and coworkers when they observe people suffering from problems not directly connected in their minds with national security.

The Pollard case illustrates how alert supervisors and coworkers can make a difference when they report suspicious behavior. Pollard exhibited egregious and observable behavior in his flagrant breaking of security rules. The Whitworth case shows the tragic results of supervisors and coworkers not reporting. The Carney case suggests that some people in fact would appreciate the helping hand of a supervisor or coworker.

Purpose of the Research

The research described in this report concentrated on issues concerning supervisor and coworker reporting of security-relevant behaviors, where relevant behaviors were defined as those covered in the adjudicative guidelines (DoD Directive 5200.2-R). While the study focused on the DoD Directive 5200.2-R, the findings may also have implications for intelligence community policy (i.e., DCID 6/4). The purpose of the study was to examine the subject of supervisor and coworker reporting, mainly to determine the extent to which the reporting requirement is being complied with, the environment in which reporting occurs, and the types of behavior reported. The ultimate aim was to understand self-initiated reporting and to recommend ways to reduce the disconnect

between reporting requirements and how people actually behave. In turn, increased reporting should help ensure that the workforce is reliable, trustworthy, and loyal.

Methodology

The research methodology consisted of four steps: (1) reviewing policies, commission studies, and other research related to supervisor and coworker reporting; (2) conducting an extensive literature review to learn about the willingness of people in general to report on their colleagues; (3) interviewing military service, DoD, and non-DoD security and other management personnel to determine the frequency of reporting and to gather recommendations for improving reporting policy and its implementation; and (4) conducting focus groups with supervisors and coworkers in the field to discuss their reporting responsibilities, willingness to report, and recommendations.

Findings

This study found that, despite Federal and DoD policy, supervisors and coworkers likely underreport security-related issues. Exploring reasons why this is so, Sarbin (2001), suggested that lack of reporting in the workplace is due to cultural prohibitions against informing on one's colleagues and friends—a code of civility—especially for behaviors that are not strictly violations of security rules but are of a personal nature. Except in cases where the behavior is egregious, Sarbin questioned the effectiveness of current DoD policy that requires supervisors and coworkers to inform on their fellow workers. Reviewing proxy measures of reporting in different fields, such as whistleblowing, Giacalone (2001), also found that supervisors and coworkers in the general workplace report only a small percentage of the questionable behaviors they observe. In spite of the low rate of reporting and the cultural injunction not to inform on others, Giacalone recommended several interventions to help increase the rate of reporting. These interventions were designed to make policies clearer and more transparent and to train supervisors and workers on these policies, the behaviors of concern, and the nexus between these behaviors and national security.

A review of commission studies (DoD Security Review Commission, 1985; Joint Security Commission, 1994; Joint Security Commission II, 1999) and related research (Bosshardt, DuBois, & Crawford, 1991; Kramer, Crawford, Heuer, and Hagen, 2001 Fischer & Morgan, 2002; Wood, 2001; Erdreich, Parks, & Amador, 1993) and interviews with security and other management personnel confirmed Sarbin and Giacalone's findings that few individuals report security-related issues. Although precise data were not available, the commission studies and related research found that supervisors provide more solicited and unsolicited information than are coworkers, but neither is a very productive source. Security and other management personnel supported these estimates that the most frequent self-initiated and PR reports are self-reports, followed by a minimal number of supervisor reports, and even fewer coworker reports. Commenting on the underreporting of incidents and why this is so, one manager said, "We work as a team and train as a team so we hang together. Big Brother is not the American way."

Supervisors and coworkers in focus groups supported the managers' estimates on the frequency of supervisor and coworker reports. They noted their reluctance to turn in their colleagues, fearing that their colleagues will be harmed or that there will be repercussions to them for reporting. However, people said they are not resistant to reporting serious infractions. In the words of one supervisor, "When it's really important, there is no one in this room who wouldn't report to Security. If we thought there was a threat, we would report it. But the things that are questionable are the personal things...You don't want to play God. Who is qualified to do that? There are gray areas. When we don't know, we are inclined to give people the benefit of the doubt [and not report]." Coworkers expressed similar sentiments.

The DoD Directive 5200.2-R reporting requirements are perceived by supervisors and coworkers as being too broad and amorphous and, thus, very difficult to implement. The regulation requires that supervisors be trained in recognizing "indicators that may signal matters of personnel security concern" and that supervisors and coworkers report "information with potentially serious security significance." While these phrases may have been clear to the original framers of the directive, they are far from obvious to supervisors and coworkers in the field. Noted a supervisor, "We need a clear communication of what is mandatory to be reported and what is discretionary. We need clearer rules about what should be reported up the chain. Knowing where we have discretion would be good; knowing where Security has discretion would also be good." Coworkers are even less clear about what to report. "At the moment, it is all just confusing," said one employee. Even in the absence of guidance, supervisors and coworkers intuitively distinguish between behaviors that are directly related to national security (which they say they have no problem reporting) and behaviors that are associated with reliability and suitability for employment (which they are hesitant to report).

One of the reasons that supervisors and employees gave for seldom reporting is that they personally could not see the precise connection—the nexus—between certain behaviors and national security. They said that they do not know where to draw the line between egregious security-related behaviors and gray-area suitability or personal behaviors—the kinds of problems that, while important, are seen as less critical in terms of security risk management and are not directly linked in people's minds with the compromise of security or with espionage. If the connection is made apparent, supervisors and employees said they will be more motivated to report in order to protect their country and national security. They also indicated that they will encourage others to obtain help with their personal problems before these problems become a security issue.

Given these findings, the question to be answered is: Should the DoD Directive 5200.2-R, which requires supervisors and coworkers to report, be retracted, kept in place, or modified to better reflect the reality of the workplace? Security managers, management personnel, supervisors, and coworkers who participated in this study all agreed that the reporting requirement is reasonable and should remain in place. A coworker confirmed this, saying, "Yes, reporting is our responsibility. If we don't do it, who will? The requirement is reasonable. And the government needs to have eyes and

ears." Instead of dropping or changing the requirement, they recommended that the policy be interpreted more clearly for those in the field who are called upon to act as adjuncts to the security system. (The authors went one step further in that they recommend changes in DoD Directive 5200.2-R [see page xiv]).

Problems in an employee's personal life and in the workplace may lead to the disclosure of classified or sensitive information, intentionally or inadvertently. This is why security managers are concerned about suitability issues dealing with finances, substance abuse, and certain emotional/mental issues, "the more private things," as one study interviewee put it. However, these behaviors are the very ones that research shows are not likely to be reported by supervisors and coworkers because that they *are* so personal. If people are asked to report behaviors without even the remotest connection to security (including "the more private things"), as they are now, security-related behavior will likely continue to be underreported.

Conclusions

This report concludes that there will always be some tension between the rules associated with supervisor and coworker reporting and cultural values not to inform on colleagues. This is especially likely in cases where the "infraction" is not perceived to be an illegal activity or security violation but a common, and often transient, personal problem. Yet, provided they understand the nexus, study participants have no objection to being the eyes and ears of the government. They believe that transient personal problems may be better handled in a different manner, perhaps by the supervisor through referral to employee assistance programs or to other kinds of monitored treatment programs.

This study points to the need to increase the reporting of critical and obvious security-related behaviors, which employees say they are willing to report. It suggests drawing a clearer distinction between the reporting and consequences of egregious security-related behaviors and suitability-type behaviors of a more personal nature that realistically are not likely to be reported. By clearly communicating this distinction to supervisors and coworkers and by encouraging supervisors to become more proactive in addressing suitability issues, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD[C3I]) may be able to increase reporting of truly serious security infractions.

Recommendations

1. **ASD (C3I) change the DoD Directive 5200.2-R to make reporting security-relevant behavior a priority and to provide anonymity for people who report.**

   DoD Directive 5200.2-R acknowledges in Chapter IX that people will only meet their security responsibilities if they understand them, thus, emphasizing the importance of security education. Supervisor and coworker reporting is not mentioned in descriptions of the various types of security education briefings (initial, refresher, foreign travel, and termination) in Section 2 of Chapter IX. It is recommended that DoD Directive 5200.2-R be amended to include supervisor and coworker reporting requirements as a priority.

   There is also no provision in DoD 5200.2-R for ensuring the reporter's anonymity. Since many interviewees in this study expressed their hesitancy to report because they feared possible adverse consequences for themselves, wording should be inserted into the directive that assures the confidentiality of reporters will be protected and guaranteed, if requested, and that only security managers will know the identity of the reporter. Safeguarding the reporter should also be a topic in security education briefings.

2. **PERSEREC develop a list of behaviors of national security concern that must be reported if observed.**

   This study's findings show that supervisors and coworkers are willing to report egregious behaviors that pose a palpable threat to national security. Because supervisors and coworkers also say they are unclear as to exactly what these behaviors are, PERSEREC should develop a list of these behaviors. The list would not include behaviors of a suitability and reliability nature since the research has shown that people are hesitant to report such matters anyway. If the list is limited to truly egregious and critical behavior, then the rate of reporting will likely increase.

   The list should be developed with the help of CI and security personnel, with a final draft being submitted for review to a sample of rank-and-file supervisors and employees in the field. Each item in the list will be accompanied by scenarios and behavioral examples to make clear to employees exactly what the security and CI world considers egregious and critical. Subsequently, the final list should be communicated to the components by policy memorandum.

   Supervisors would be accountable for reporting serious security-related behaviors and for ensuring that their cleared employees understand the behaviors that must be reported. They would also be responsible for referring people with less-critical issues (from a national security standpoint) to employee assistance programs or other remedial programs. Cleared employees will also be required to report serious security-related behaviors.

3. **ASD (C3I) issue a security policy memorandum advising that certain changes must be made in the government's approach to supervisor and coworker reporting.**

A major, unstated policy issue concerning the role of security managers underlies this report. What is their responsibility for continuing evaluation? Is it only to decide when some adverse action needs to be taken relating to a person's clearance? Or does it also include being proactive and ensuring that people's personal problems get addressed before they become security problems? The authors recommend that the DoD make more explicit its security policy to, first and foremost, protect national security, particularly in cases where there are indications of potential CI activity. It should also clarify the circumstances under which supervisors should refer troubled employees to employee assistance programs or other remedial programs before their problems become a security concern.

ASD (C3I) should issue a memorandum making it explicit that security managers and supervisors have a proactive role to play in preventing security problems due to suitability issues. In this statement, ASD (C3I) should outline policies regarding how and under what circumstance security managers will refer personnel for assistance rather than punishment when their actions are reported. This memorandum should also clarify the relationship between Security, employee assistant programs, and other functions.

Related to the above, the memorandum should address the problem of making reporting policies and procedures as transparent as possible for all employees. There should be more clarity in the security system, with clearer-cut rules as to what to report. There should be closer coordination and feedback between security managers, supervisors, and employees. Security managers at the very least should acknowledge a report was received and, if appropriate, inform the reporter of the eventual outcome. The reporter's confidentiality must be honored and protected.

The memorandum should also re-emphasize the importance of training for both supervisors and coworkers. This training should regularly remind supervisors and coworkers of their reporting responsibility. It should provide practical guidance on indicators that may signal matters of security concern and should outline personnel security policies and procedures, including categories of behavior to be reported and provisions for helping troubled employees. Such training would be developed by the Joint Security Training Center (JSTC) and provided to the components for implementation. The training should be conducted in person, not via the Internet, and should allow ample time for participants to interact with the presenter and among themselves.

4. **Joint Personnel Adjudication System (JPAS) Program Office develop and implement a system for recording and tracking in JPAS supervisor and coworker reporting of security-related concerns.**

At the present time, data do not exist concerning the extent of reporting by supervisors and coworkers, to whom the information was reported, and the results of the reporting. Without a tracking system, it will not be possible to precisely describe the problem and to evaluate the impact of steps taken to increase reporting. Thus, it is recommended that the JPAS Program Office add data fields to the JPAS database so that the source (including supervisors and coworkers) and nature of the information reported can be captured and evaluated. Security managers will be provided with guidance on how to code and enter reporting data into the JPAS. At the same time, they will report the information to the CAFs. In this way, it will be possible to track reporting behaviors and to evaluate and adjust policy and training as needed.

5. **PERSEREC develop and field a survey to establish trend data concerning security-related behaviors that are observed and reported.**

To address a related concern about behaviors that are not reported, it is recommended that PERSEREC conduct a periodic survey of supervisors and employees within the DoD. The survey would be similar to the Whistleblower Survey of fraud, waste, and abuse behaviors, in that it would take the pulse of the workplace (Erdreich, Parks, & Amador, 1993). It would identify behaviors related to the adjudicative guidelines that are observed in the workplace, the extent to which these behaviors are reported, and the results for both the person reported and the person who reported. It would also elicit reasons why supervisors and coworkers do not report the overwhelming majority of the behaviors they observe.

The first three recommendations will clarify and explain reporting policy. The JPAS tracking data, in combination with the survey data, could result in an effective feedback mechanism whereby reporting policies are evaluated and, if need be, altered. Combined, these recommendations have the potential to increase the rate of reporting and to encourage employees to obtain assistance before their problems become a security issue.

Table of Contents

Appendices

List of Tables

Introduction

The Problem

In the Department of Defense (DoD) personnel security system, once people receive security clearances they are subject to continuing evaluation over time to ascertain their continuing reliability, trustworthiness and loyalty. If the security manager receives a report that is indicative of a security-related issue in a cleared employee's life, the report is forwarded to a central adjudication facility where the issue is evaluated. Such continuing evaluation reports come from a variety of sources, such as police departments, credit checks, periodic reinvestigations (PRs), etc. However, information from these sources cannot possibly cover all aspects of an employee's life or raise real-time questions about the employee's behavior. To fill this vacuum, the government asks supervisors and coworkers to help out as its eyes and ears and to report issues that may potentially impact national security. The present study examines this particular and important aspect of the continuing evaluation program.

To ensure a reliable, trustworthy, and loyal cleared workforce, executive orders, directives, and regulations require supervisors and coworkers who work in a classified environment to report to security managers any behavior they observe among workplace colleagues that may be of security concern. Alert supervisors and coworkers are presumed to be the first line of defense against espionage. In theory, the reporting of security-relevant behavior by supervisors and coworkers should play a key role in the continuing evaluation of cleared personnel. However, anecdotal evidence and prior Defense Personnel Security Research Center (PERSEREC) research suggest that people are not reporting in significant numbers. Supervisors report more often than coworkers, but it still appears that both they and coworkers may hesitate to inform security managers about many behaviors that they do in fact observe. A natural tension exists between the requirement to report certain behaviors observed in the workplace and employees' and supervisors' willingness to adhere to this policy.

The study primarily focused on self-initiated reports and only secondarily on reports made during PR interviews.

By asking employees to report on colleagues, the government seeks to use employees as adjuncts to the formal continuing evaluation system. Government investigators are the primary agents in the process of initially vetting potential clearance-holders and re-examining the individuals periodically to ensure that they can be reasonably expected to remain trustworthy until the next review cycle. Supervisors and coworkers are being used to augment the government's official procedures. It is reasoned that supervisors, by the very nature of their jobs, observe employees' job performance and are naturally in a position to advise or require troubled employees to seek help, or to report them to security authorities. Coworkers, who are around their colleagues all the time at work, are likely to observe behaviors that might suggest a risk to national security, and thus they are encouraged and, in some instances required, to report them.

Understanding the context in which reporting is required and recommending ways to reduce the disconnect between reporting requirements and what people actually do (report very little) constitutes the problem addressed by this study. The following examples illustrate the importance of the problem of supervisor and coworker reporting, for they place the subject in a context directly related to espionage and its consequences.

While espionage cases are statistically rare, spies have in fact been caught as a result of supervisor and coworker reporting. A famous case described widely in the media was that of Jonathan Pollard, a Naval intelligence analyst arrested for espionage on behalf of Israel, whose arrest was the result of, first, a supervisor's suspicion and then a coworker's report. Pollard's supervisor had had doubts about him, not only when he was caught lying about his dealings with another government agency but also when the supervisor noticed that he was late in completing work assignments. He was requesting so many Top Secret documents that it was becoming a burden on the clerk who had to log them in. For these and other reasons, the supervisor perceived Pollard as an undesirable employee and resolved to get rid of him. He did not suspect a security problem, however, until a coworker reported seeing Pollard take a package of Top Secret material out of the building late on a Friday afternoon and get into a car with his wife. Investigations confirmed that Pollard was regularly removing and compromising large quantities of highly classified documents (Blitzer, 1989).

Another prominent case illustrates the consequences of not reporting. The colleagues of Navy spy, Jerry Whitworth, observed him monitoring and copying a sensitive communications line without authorization, saw classified papers in his personal locker, and knew he took classified materials home. However, they assumed he was doing it only to keep his work current (Barron, 1987). None of these coworkers reported the activities before Whitworth's arrest as part of the John Walker spy ring. Their failure to inform their security manager about Whitworth's activities allowed the Walker ring to continue, with significant damage to national security.

Supervisors and coworkers are not just being asked simply to report on a person whose behavior is inappropriate. They are in a position to help their colleagues get treatment before problems result in compromise of security or loss of their jobs. One convicted spy, Jeffrey Carney, in an interview from prison, spoke of how he wished someone had stepped forward to give him the help he needed; this might have prevented his committing espionage. "If you want to do people with problems a favor—and I'm talking from experience—say something!... If somebody had said, 'I think Jeff's got a problem and I don't think that he's handling it very well. Supervisor, do something,' that would have been enough to stop the process, at least for a while" (NIMA, 2000). The problem is that most people are squeamish—for a variety of culturally imbued reasons—about reporting or, as they may see it, *informing* on their subordinates and coworkers when they observe people suffering from problems not directly connected in their minds with national security.

The Pollard case illustrates how alert supervisors and coworkers can make a difference when they report suspicious behavior. Pollard exhibited egregious and

observable behavior in his flagrant breaking of security rules. The Whitworth case shows the tragic results of supervisors and coworkers not reporting. The Carney case suggests that some people in fact would appreciate the helping hand of a supervisor or coworker.

Purpose of the Research

The research described in this report focused on issues concerning supervisor and coworker reporting of security-relevant behaviors, where relevant behaviors were defined as those covered in the adjudicative guidelines (Department of Defense [DoD] Directive 5200.2-R). While the study focused on the DoD Directive 5200.2-R, the findings also are likely to have implications for intelligence community policy (i.e., Director of Central Intelligence Directive [DCID 6/4]). The study primarily focused on self-initiated reports and only secondarily on reports made during PR interviews. The purpose of the study was to examine the subject of supervisor and coworker reporting, mainly to determine the environment in which reporting occurs and the types of behavior reported. The ultimate aim was to recommend changes in policy and practice that might lead to the establishment of certain conditions under which supervisors and coworkers would be more likely to report despite a natural reluctance to inform on subordinates and colleagues.

Method

The research methodology to examine supervisor and coworker reporting policy and the implementation of this policy consisted of the following four steps.

1. Background Review. Review policies, commission studies, and other research related to supervisor and coworker reporting. This step included examination of the productivity of different investigative sources and the uniqueness of the information provided by these sources in identifying security-relevant behaviors. It provided the context for conducting the remaining research steps.
2. Literature Review. Extensive review of the literature relevant to the subject of supervisor and coworker reporting. The goals were better to understand issues related to reporting and to identify lessons learned.
3. Security Manager Interviews. Semi-structured interviews with 45 security managers and management personnel at 20 DoD and non-DoD Federal agencies to learn about their experience with, and recommendations concerning, supervisor and coworker reporting.
4. Employee Focus Groups. Focus groups with supervisors and employees at DoD and non-DoD Federal agencies to learn their views and recommendations concerning supervisor and coworker reporting.

The findings from each of these research steps follow.

Findings

Findings from the Background Review

The project staff undertook a review of policies that regulate supervisor and coworker reporting, findings of commission studies, and recent research of the productivity of various sources of investigative information.

Policy Review

Policy documents, such as executive orders, directives, and regulations, focus on reporting requirements of different populations. Below, the main executive orders and other Federal policies are reviewed. Appendix A describes how these policies have been translated into military service- and agency-specific regulations.

Executive Order. Over time, the personnel security system moved from a reactive, law-enforcement model of personnel security towards a more proactive and supportive model. Through various executive orders, the government took steps to offer a helping hand to troubled employees. This new approach was exemplified by Executive Order 12564, *Drug-free Federal Workplace* (1986), which was issued in an effort to eliminate the use of illegal drugs by all Federal civilian employees, whether cleared or not. The order requires agencies to develop a plan to achieve a drug-free workplace and provide the programmatic means to do so. It requires that the Federal government "show the way towards achieving drug-free workplaces through a program designed to offer drug users a helping hand and, at the same time, demonstrate to drug users and potential drug users that drugs will not be tolerated in the Federal workplace." It also requires training of supervisors in identifying and addressing illegal drug use by employees. There is no reference in E.O.12564 to coworker reporting.

In August 1995, Executive Order 12968, *Access to Classified Information*, addressed the subject of employee responsibilities. The order states that employees should protect classified information; report all contacts with people, including foreigners who seek to obtain unauthorized access to classified information; report all violations of security regulations; and comply with all other security requirements. Employees are 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." The order also expands prevention, treatment, and rehabilitation programs beyond drug and alcohol abuse and emphasizes retaining personnel while they deal with a wide range of problems through counseling, medical treatment, or the development of appropriate life-skills. Such problems include physical as well as emotional and mental disorders, financial concerns, and other issues that, if left untreated, could impact the employees' job performance or ability to protect national security. In fact, the order mandates that information about the availability of employee assistance programs be included in security education programs for the cleared workforce.

This new, supportive approach was grafted onto the old personnel security system, introducing a degree of dissonance. For example, security professionals may have different views from the average worker about what kinds of behavior are deemed relevant to national security and are thus reportable. Meanwhile, employees may be reluctant to seek help or to report their colleagues because they do not really understand what to report and what will happen to those they do report.

***Director of Central Intelligence Directive* (DCID) 6/4**, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (July 2, 1998), covers individuals with access to sensitive compartmented information (SCI). It requires that security awareness programs be established for supervisors to "ensure that supervisory personnel recognize and discharge their special responsibility to safeguard SCI." Such programs should provide practical guidance on indicators that may signal matters of security concern. Supervisors also must be briefed on reporting procedures "to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his or her vulnerability (12.3)."

In Paragraph 9, Reporting Requirements, DCID 6/4 discusses individuals' responsibilities for reporting observed activities by anyone, including their coworkers, that could conflict with those individuals' ability to protect highly classified information. Employees have an obligation to report to authorities all activities or conduct of any SCI-cleared person that relate to the 13 adjudicative guidelines. No details of specific behaviors to be reported are given.

DoD Directives and Regulations. DoD Directives 5200.2 and 5200.2-R are the basic policy and regulatory documents for the DoD personnel security program. The DoD Directive 5200.2, *DoD Personnel Security Program* (April 9, 1999), states that military, civilian, and contractor personnel with security clearances must be reliable and trustworthy, and there must be "no reasonable basis for doubting their allegiance to the United States." The fact that all appointments and assignments must clearly be consistent with the interests of national security is stressed, and the "qualifications" for people seeking clearances are listed. As stated in paragraph 3.4 of DoD Directive 5200.2, those qualified for clearances are:

> "U.S. citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the U.S., strength of character, trustworthiness, honesty, reliability, discretion and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."

DoD Directive 5200.2-R, *Personnel Security Program* (January, 1987, amended 1996 and soon to be completely revised), is the corollary regulation to DoD Directive 5200.2 and implements the personnel security requirements of various executive orders.

This security directive outlines personnel security policies and procedures, including categories of behavior to be reported and provisions for helping troubled employees. The categories of behavior, which serve as adjudicative guidelines and are to be reported, are as follows:

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Emotional, Mental, and Personality Disorders
- Criminal Conduct
- Security Violations
- Outside Activities
- Misuse of Information Technology Systems.

DoD Directive 5200.2-R, Chapter IX, Continuing Security Responsibilities, states that all DoD components must develop programs to evaluate on a continuing basis the status of personnel with respect to security eligibility. This program should ensure "close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available...is considered in the personnel security process." The chapter specifies the various responsibilities of managers, supervisors, and coworkers.

Asking supervisors and coworkers to report to security managers has been part of the personnel security system for some time. The supervisor-reporting requirement dates back to at least the first version of the DoD Directive 5200.2-R in 1979. The most recent DoD Directive 5200.2-R (1987, revised 1996) states that supervisors should be trained to recognize indicators that may signal matters of personnel security concern. The directive also states that *specific* instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect national security as well as to provide necessary help to individuals to correct any personal problem that may have a bearing upon their continued eligibility for access. Employees, in their turn, must be aware of the standards of conduct required of them in their positions of trust and must recognize and avoid the kind of personal behavior that may result in loss of their clearance. In other words, the directive firmly places on the individual "the ultimate responsibility for maintaining continued eligibility for a position of trust."

The coworker requirement was first introduced in the DoD Directive 5200.2-R in 1987, in which a very brief paragraph (9-104) refers to the responsibilities of coworkers. They are required to inform supervisors or appropriate security officials when they

"become aware of information with potentially serious security significance regarding someone with access to classified information or employees in a sensitive position."

Section 2 of Chapter IX of the DoD Directive 5200.2-R concerns security education and makes the point that people cannot meet their security responsibilities unless they understand them, hence the necessity for security education. Supervisor and coworker reporting is not specifically mentioned in the descriptions of the various types of briefings (initial, refresher, foreign travel, and termination). Rather, four major topics are to be covered: specific security requirements of a person's particular job; techniques employed by foreign intelligence activities; prohibition against disclosing classified information to unauthorized persons; and penalties for security violations. Supervisor and coworker reporting would presumably fall under "specific security requirements of a person's particular job."

Summary of Reporting Policies. In summary, executive orders, Federal acts, department directives, and agency instructions vary considerably in their coverage of supervisor, coworker, and employee reporting responsibilities for those with Top Secret, Secret and Confidential clearances and SCI-cleared personnel and the relationships of Security to employee assistance programs and other functions. In general, the responsibilities of different populations are as follows:

- Supervisors. Supervisors *are responsible* for matters pertaining to personnel security with respect to employees under their supervision. They *are required* to report significant adverse information that may have a bearing on their subordinates' continued eligibility to access to classified information. Supervisor training and security awareness programs are required to cover indications of security concerns, reporting procedures, and employee assistance programs.
- Coworkers. Employees with Top Secret, Secret or Confidential clearances *are encouraged and expected* to report information that raises doubts as to another's continued eligibility for access to classified information. Employees with access to SCI *have an obligation* to report activities or conduct of any SCI-cleared person that could conflict with their ability to protect highly classified information or that relate to the 13 adjudicative guidelines.
- Employees. All cleared employees *shall/must* report their own foreign contacts and security violations. In addition, SCI employees *must* report their own personal problems and seek guidance or assistance.
- Security versus Employee Assistance Programs and Other Functions. While policies do not clarify the relationship between Security and employee assistance programs in reporting and handling security issues, all agencies *are required* to establish such programs for cleared employees; *are encouraged* to use these programs to help employees with financial, medical, and emotional problems; and *should establish*, where appropriate, tailored monitoring programs for SCI-cleared employees.

Commission Studies

The DoD Security Review Commission (1985), known as the Stilwell Commission, emphasized the role that humans play in creating and handling national secrets and in reporting incidents of possible espionage. The commission acknowledged that formal reporting channels in DoD tend "to discourage reporting of pertinent information since the typical employee is reluctant to 'inform' on fellow employees and, in most cases, is unable to gauge whether the information is sufficient enough to justify the unpleasant consequences which may follow." The commission also reported that commanders and supervisors in DoD, while charged by regulation to report adverse information about their subordinates, report relatively little. This lack of supervisors' involvement in the security process was deemed a cause of concern "because the command/supervisory system offers the most likely means of identifying security problems, including indicators of espionage, among cleared personnel. In virtually every recent espionage case there has been evidence of conduct known to the commander or supervisor that, if recognized and reported, might have had a bearing on the continued access of the individual." Given the importance of supervisors' roles in providing a climate for security within their organization, the commission recommended that "DoD require reports to appropriate counterintelligence and investigative authorities concerning any employee who is known to have been responsible for repeated security violations over a period of one year, for appropriate evaluation."

The Joint Security Commission (1994), the first significant post-Cold War examination of government security policies and practices, stated that personnel security is at the very heart of our security system, but made no specific mention of supervisor and coworker reporting. In its sequel (Joint Security Commission II, 1999), however, there was discussion of the need to develop a "security-aware environment...that requires vigilance, awareness of people and their problems..."

Related PERSEREC Research

Several recent PERSEREC studies, summarized in this section, are directly relevant to supervisor and coworker reporting and show how little self-initiated reporting or reporting during PRs generally occurs. The first two studies, one on continuing assessment of cleared personnel and the other on revocations, address both self-initiated reporting and reporting during PRs. The second two studies, concerning Single-Scope Background Investigation-Periodic Reinvestigations (SSBI-PR) and unique sources of issue information, focus solely on reporting during PRs.

Continuing Assessment of Cleared Personnel. Bosshardt, DuBois, & Crawford (1991) identified three broad categories of continuing assessment criteria for cleared personnel in the military: (1) security compromise, (2) personnel suitability, and (3) personnel security duties. The first category focuses on the occurrence, or increased risk, of security compromise and includes such behaviors as espionage, unauthorized disclosure of classified information, disloyal activities, security violations, falsification of security-related information, and association with foreign nationals. The second covers

unsuitable conduct, e.g., drug use, alcohol abuse, sexual misconduct, financial irresponsibility, criminal behavior, and unreliable behavior. The last category focuses on cleared individuals' failure to carry out their security duties, e.g., improper handling or storage of classified documents, failure to report derogatory information, etc. The authors also identified a need to clarify the relationships among these criteria and to empirically link these criteria to the compromise of classified information.

In this study, security managers rated the willingness of various sources to report continuing assessment information with the Security Office and the value of the information reported. Using a 10-point scale, where "1" was defined as very unwilling and "10" as very willing, the average ratings for supervisors and coworkers were 5.8 and 3.2, respectively. Using a similar scale describing the usefulness of the information reported, where "1" was defined as very little usefulness and "10" as extremely useful, the average ratings for supervisors and coworkers were 7.1 and 5.7, respectively. Thus, when asked which sources of continuing assessment information have the most *unrealized potential*, security managers listed both supervisors and coworkers.

Problems identified by these security managers as limiting reporting include inadequate training to instruct commanders, supervisors, and cleared individuals on their continuing assessment responsibilities; inadequate training on how to spot, interpret, and manage the early-warning indicators of personnel security risk; concerns about operational readiness and unit mission accomplishment; concerns about hurting the employee's career, and perception that problems reflect negatively on leadership.

Revocation Study. Fischer & Morgan (2002) examined the reasons why people's clearances are revoked. Researchers studied one year (FY98) of revocation cases (864) at five central adjudication facilities, looking for what behaviors triggered a case to be opened and the different sources from which issue information was gleaned. Populations under study were enlisted personnel, military officers, civilian government employees, and defense contractor employees. As Table 1 shows, Subjects and supervisors are the most productive sources. Supervisors are a much greater source of issue information than are coworkers, especially in the military where commanders by tradition have more knowledge of their subordinates' lives. Coworkers are the least productive source of issue information.

Table 1
Percent of All Issue Information in Revocation Cases Derived from Each Source by Occupational Group

Source	Enlisted %	Officers %	Civilians %	Contractors %
Subject	16	16	17	19
Supervisor	13	13	4	5
Coworkers		1	1	
Criminal Investigation	8	7	2	
Local Agency Check	5	6	6	13
Periodic Reinvestigation	5	10	16	6
Background Investigation	4	3	2	5
Special Investigative Inquiry	1		9	14
Creditors	6	6	7	4
Police Reports	8	8	8	10
Unit Security Office	13	13	10	2
Initial Background Investigation			2	6
UCMJ Proceedings	9	4		1
Urinalysis	4	3	3	2
Medical Records	4	4	6	7
Other Agencies	2	3	5	5
Total	98	97	98	99

Note. Column totals are less than 100% because cell values show percentages above 1%, rounded to the nearest whole percentage. For sources not listed, values were less than 1%.
Data derived from Fischer & Morgan (2002).

Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) Study. Kramer, Crawford, Heuer, and Hagen (2001) examined the information acquired on a Subject from various sources by investigators who conduct interviews for PR background investigations. Among such sources are the *SF-86, Questionnaire for National Security Positions,* which is the form that personnel complete when applying for a security clearance. Other sources include Subject interviews; credit reports; employment references, such as supervisors and coworkers; neighbors; listed references (i.e., people whom a Subject lists as a reference on the *SF-86*); and references developed as follow-ups to these sources. This study explored the kinds of issue-relevant information that emerged from such sources during the course of the SSBI-PR. To accomplish this, a team of personnel security adjudicators reviewed a random sample of 4,721 case files at four agencies that routinely conduct SSBI-PRs. These were the Department of Defense (DoD), Office of Personnel Management (OPM), Central Intelligence Agency (CIA), and National Reconnaissance Office (NRO).

One segment of the study explored what categories of interviewees provided the richest issue-relevant information about a Subject. Table 2 presents the proportion of SSBI-PR cases in which a particular source was part of the investigation and that source provided issue-relevant information. For example, in these randomly selected DoD PR cases, where supervisors were part of the investigation, only 3% provided issue-relevant information; similarly, in DoD PR cases, where coworkers were part of the investigation, 1% provided issue-relevant information. Overall, a very small percentage of supervisors and coworkers, who were queried about the Subject as part of an SSBI-PR investigation, provided issue-relevant information to investigators. Listed references, developed references, and neighbors also were not rich sources. In contrast, much higher percentages of ex-spouses (16% - 29%) and medical personnel (31% - 57%), who were queried as part of an investigation, provided issue-relevant information to investigators, as did area security managers (67%) in one of the intelligence agencies.

Table 2

Percent of SSBI-PR Cases in Which Source Types Yielded Issue-Relevant Information [a]

Source	Agencies Conducting Single-Scope Background Investigations—Periodic Reinvestigation			
	DoD %	OPM %	CIA %	NRO %
Interviews of Others				
Supervisors	3	5	5	2
Coworkers	1	3	3	1
Listed references	1	1	3	1
Developed references	2	0	3	1
Neighbors	<1	2	1	1
Ex-spouses[b]	16	24	29	29
Medical personnel[b]	31	0	57	53
Area security managers	-	-	67	-
Miscellaneous [b]	0	29	0	9

Note. Percentages represent the proportion of cases in which the source provided issue-relevant information.

[a] Interviews are not conducted by the agency with these sources; 0 = No cases emerged.

[b] While these percentages are relatively high compared to other sources, it should be noted that only in a very small percentage of the cases were these sources part of the investigation.

If so little information can be gleaned in response to direct questions from an investigator in a PR interview, then one has to ask how likely it is that supervisors and coworkers would initiate a report to authorities concerning a subordinate's or a colleague's troubling behavior. While this raises the question of whether the investigator is asking the proper questions in the interview to elicit a useful response, it is likely that supervisors and coworkers know more about their colleagues and subordinates than these data indicate.

Differences between the percentages in Table 1 and Table 2, particularly in regard to supervisors, can be attributed to the different types of cases reviewed. The revocation study reviewed only cases in which a final revocation occurred, regardless of whether or not a PR was undertaken, whereas the SSBI-PR study reviewed a random sample of PR cases, most of which did not uncover issue information. These studies provide evidence that: (1) supervisors are a more productive source of unsolicited issue information than are coworkers in revocation cases; (2) supervisors are not a very productive source of issue information when part of a SSBI-PR investigation; and (3) coworkers are not a productive source either in revocation cases or when part of a SSBI-PR investigation.

Study of Unique Sources of Issue Information in PR Cases. As part of the current study, the research staff selected and conducted an in-depth review of a very small sample (N = 49) of PR cases in which supervisors and coworkers provided information of a security nature (see Appendix B). The objective of this case review was to determine the degree of uniqueness of the information provided by different sources during PR investigations. Unique information was defined as that provided by a *single* type of source (e.g., only the Subject or only current supervisors). From a cost-benefit perspective, unique sources of information were considered most valuable because, without these sources, potentially important issue information might not have been uncovered.

The 49 cases were *not* intended to be representative of all PR cases; rather, they were selected to provide insights concerning the types of issues reported by supervisors and coworkers during PR investigations and the uniqueness of the information reported by these sources. It is important to note that the information provided in these cases did not result in revocation of the employees' clearances. It is also important to note that, due to the nature of the investigative reports, the researchers could not distinguish between information that the individuals being interviewed volunteered on their own and information they provided in response to the investigator's direct questions.

This research found that Subjects and their supervisors, when interviewed directly, can be valuable sources of unique, security-relevant information. It also found that current coworkers and coworkers identified during the investigation may provide unique information in a very small percentage of cases; and that coworkers listed by the Subject and coworkers who are neighbors generally cannot be expected to provide unique information.

Other Related Research

Trends in Public Attitudes. A study of trends in public attitudes towards government security programs found that the public does not object to coworkers turning in their colleagues for violating security rules. Four-fifths of the respondents said that they would report their coworkers, half immediately and half if their colleague's behavior continued after they had asked them to stop (Wood, 2001). While there is no evidence that in real life the respondents themselves would actually follow through on such statements, these data show that the public feels workers have a responsibility to report

certain behavior if that behavior occurs in the context of a higher cause—the protection of national security. The data also indicate that people's distaste for reporting colleagues might be diminished when classified information is being compromised.

U.S. Merit Systems Protection Board Study. A study by the U.S. Merit Systems Protection Board (Erdreich, Parks, & Amador, 1993) used an anonymous survey that asked government employees if they had observed serious fraud, waste, or abuse behaviors in the workplace in the last 12 months and, if so, whether or not they reported it. The study also examined why employees reported or did not report what they saw and what happened after they reported improper activity.

The study found that 18% of those surveyed had in the previous 12 months personally observed or obtained direct evidence of activities believed to be illegal or wasteful. These individuals, referred to as observers, most frequently observed or had direct evidence of waste caused by a badly managed program, waste caused by unnecessary or deficient goods or services, and other serious violations of the law or regulation. Of the observers, one-half (i.e., 50% of the observers or 9% of those surveyed) reported the behavior, most often to their immediate supervisor or to someone above their immediate supervisor. Of those who reported the behavior, two-fifths said that they had experienced or had been threatened with some sort of retaliation. Reasons given for not reporting the behavior included a belief that nothing would be done, fear of reprisal, and not knowing what types of behaviors to report.

This study found that between 1983 and 1992 there has been a significant decrease in the percentage who observed serious fraud, waste, or abuse (23% in 1983, 18% in 1992) and a significant increase in the percentage of observers who actually reported that activity to someone other than a friend, family member, or coworker (30% in 1983, 50% in 1992). Erdreich, Parks & Amador surmised that this could be at least in part related to the passage of the Whistleblowing Protection Act in 1989. This act emphasized the importance of Federal employees sharing information about the problems they observe in the workplace and provided protections to those who report. Also, during this decade some agencies initiated programs to empower employees by encouraging them to identify problems and to help devise solutions.

The 1992 survey yielded information on four items related to illegal or improper activity that provides a proxy measure for coworker and supervisor reporting. These items are: use of an official position for personal benefits, stealing Federal property, stealing Federal funds, and accepting bribes or kickbacks. Table 3 shows that these serious activities were observed by 491 (over 3.6%) of the 13,432 respondents. For example, 281 of the 13,432 respondents (i.e., 2%) observed someone using an official position for personal benefit, but only one-third (35%) of those who observed the behavior reported it. In contrast, 23 of the 13,432 respondents (i.e., two-tenths of 1%) observed someone accepting bribes or kickbacks; however, of those who observed someone accepting bribes and kickbacks, slightly over three-fourths (78%) reported the behavior.

Table 3

Number of People Who Observed Illegal or Improper Activity by Others in the Workplace and, of Those, the Percentages Who Reported the Behaviors

Type of Activity	Number of People Who Observed	Percentage of Observers Who Reported [a] %
Use of an official position for personal benefit	281	35
Theft of Federal property	140	37
Theft of Federal funds	47	53
Accepting bribes or kickbacks	23	78
Total	491[b]	

[a] Behaviors were reported to someone other than a friend, coworker or family member. Most often this was to a supervisor or to someone above their immediate supervisor.

[b] A total of 13,432 respondents completed the survey; of these, 491(3.7%) observed the target behaviors.

The high percentage of people who reported these behaviors, compared to other data in the present report concerning self-initiated supervisor and coworker reporting, is probably explained by the egregiousness of the activities that were observed and shows that, if an infraction is perceived as extremely serious, people are more likely to report.

Summary of Commission Studies and Related Research

The commission studies and related research described above showed that Subjects and supervisors are more productive sources of security information than are coworkers, who seldom report their colleagues despite their opportunity to observe colleagues on a daily basis. This research revealed that, in some situations, such as those involving fraud, waste, and abuse, coworkers are more likely to report than in the security field. Nevertheless, reporting rates by supervisors and coworkers in the workplace appear to be much lower than the incidence of likely reportable behaviors.

The research also suggested that supervisors and employees might be willing to report security-related issues under certain circumstances. These circumstances include increased knowledge as to what to report and how to report, understanding that certain actions are serious and could actually endanger people's lives or negatively affect our government, belief that something will be done to address the situation, and assurances that they will not become the object of retaliation if they do report.

Findings from Current Literature Reviews

In April 2001, two scholars, Robert Giacalone and Theodore Sarbin, synthesized findings from two separate literature reviews in several disciplines. Based on their

independent reviews, Giacalone and Sarbin each wrote a position paper that described the phenomenon of reporting, identified factors affecting reporting, discussed the disconnect between current DoD reporting policy and its implementation, and made recommendations for dealing with this disconnect.

Review of Research on Proxy Measures

Knowledge about what makes coworkers and supervisors willing to report behaviors such as those outlined in the adjudicative guidelines has been limited largely to research on non-security fields. Thus, Giacalone (2001)[2] conducted an extensive review of the literature in a number of non-security areas that were identified as proxies for the reporting of security-relevant behavior. These areas included whistleblowing and peer reporting, employee assistance program referrals, ethical climate, and moral decision-making. Although he used these areas as proxies, Giacalone believes that the rate of reporting security-related behaviors will be even lower than the levels seen in these proxy areas. He hypothesizes that this is because people do not believe there is a connection between many of the behaviors they are being asked to report and national security. For example, they can, without special explanation, immediately understand a connection between alcoholism and self-destructive behavior, but not between alcoholism and national security.

Giacalone presented a description of the conditions under which people are or are not likely to report security-related behavior. The literature suggests that a person's decision to report a given behavior of a coworker varies as a function of the information to be reported, the organizational context in which the behavior occurs, and the perceived costs and benefits of reporting.

Information to be Reported. Reporting varies as a function of the clarity of information and the perceived severity of the behaviors. It is important that people clearly understand their reporting responsibilities, i.e., whether they have a responsibility to report, what kinds of behavior are reportable, and where to go to make the report. As clarity increases, the likelihood of people reporting should increase.

Reporting also varies as a function of the perceived severity of the behavior, perceived repercussions for the person reported and for the reporter, and perceived repercussions if the behavior continues. Training personnel about their reporting responsibilities, how to recognize security-related behavior, and the relationship of the behavior to security may help increase the amount of reporting.

Organizational Context. Reporting varies as a function of several characteristics of the organization and the individuals involved. These include:

---

[2] The material that follows is abstracted from a paper presented by Giacalone at a colloquium sponsored by PERSEREC in April of 2001. Giacalone's paper, along with its extensive bibliography, is available upon request to PERSEREC.

- The extent to which the observer is dependent upon the individual exhibiting the behavior. As the observer's dependency on that individual increases, the less likely the observer is to report the behavior.
- The observer's perception of his or her relationship with the organization and management. In those organizations where employees trust management, employees are more likely to report, feel they will be protected, and believe that action will be taken as a result of their report. Where management and the organization treat the employees well, employees are likely to be motivated to help out the organization by reporting.

Once information has been reported, it is likely to be filtered in different ways depending upon the status and dependency of the person who reported the information and how the information was reported.

Perceived Costs and Benefits. Reporting also varies as a function of the perceived costs and benefits to the person disclosing the information and to the person whose behavior is being disclosed. The higher the benefits and lower the costs are to the individual reporting the information, the more likely the behavior will be reported. In situations where repercussions to the person being reported are perceived by the potential reporter to be very serious, the individual may hesitate to report. Especially if the behavior is not perceived as being problematic or directly related to security concerns, there may be reluctance to report because of a desire to protect the person.

The literature review provided ample evidence that if security-related reporting follows the pattern of proxy reporting, the expected level of disclosure is going to be low, except perhaps when the observed behaviors are egregious. While Giacalone's examination of the literature led him to believe that very little reporting can be expected, he suggested various interventions that might be introduced at the field level to slightly increase the rate of reporting. Summarized, they suggest the introduction of more clarity and transparency into the system so that the rules and boundaries are clear. While there will always be gray areas, effort should be made to make explicit as much of the material as possible. Orientation and refresher training should explain how reportable behavior is connected to national security. Also, this training should cover:

- policies relevant to reporting and reportable behaviors
- employees' and supervisors' responsibility to report and, with the provision of examples, precisely what behavior to report
- how to recognize employee performance and behavioral changes related to reportable behaviors
- available sources of information on reporting policy, responsibility, and procedures
- how employees (supervisors, coworkers, human resource staff, security managers) can play a key role in identifying reportable behaviors
- reporting procedures, including where to go to make a report

- examples of how reports can lead to positive outcomes for the organization and for the reported employee
- existing safeguards to protect the person who reports.

Review of Reporting Policy Versus Practice

Sarbin (2001)[3] synthesized a broad and diverse body of literature from the 1920s to the present and applied his findings to DoD policy and the reality of reporting security-relevant behaviors. The workplace is the most frequent setting in which government employees—military and civilian—attempt to compromise secret information. Hence, security experts introduced the idea of enlisting supervisors and coworkers to voluntarily come forward to report certain behaviors on the part of fellow employees, as outlined in the DoD Directive 5200.2-R, that may suggest the employees are not reliable, trustworthy, and loyal or pose a risk to national security.

It is one thing to expect employees to detect and report egregious violations of security rules; it is quite another to expect them to report on perceived deviations from conduct encoded in security directives, such as the DoD Directive 5200.2-R. Sarbin believes that such directives have been developed over the years on the premise that any evidence of unreliable, untrustworthy and disloyal behavior represents a character flaw and that defects of character predispose a person to engage in espionage. Such premises have been repeatedly controverted in systematic research beginning in the 1920s. Applied to security issues, a person may engage in a morally unacceptable way in a particular situation and yet be morally circumspect in others.

Sarbin argues that the premises for the expectation that employees would report DoD Directive 5200.2-R-related behaviors fail to take into account a number of long-standing observations about the negative moral value placed on informing or snitching. Through the medium of stories told, stories read, and stories lived, human beings are socialized to place a positive value on loyalty to playmates and peers and to regard informing as a serious moral breach.

Sarbin believes that it will be unproductive to assign to coworkers the responsibility for reporting workmates' conduct that might predispose them to become security risks. Except in rare instances, e.g., the case of Jonathan Pollard, observations of workplace conduct yield little useful information on a person's readiness to become a spy. Because informing on the behavior of a coworker is an elective act, an appeal to the broad issue of national security, or to the narrower moral injunction of "I am my brother's keeper," is not likely to overcome the deeper moral injunction against being a snitch.

It is generally recognized that every organization embraces explicit codes of conduct, the written law. At the same time, members of these organizations also embrace

[3] The material that follows is abstracted from a paper presented by Sarbin at a colloquium sponsored by PERSEREC in April of 2001. Sarbin's paper is available upon request to PERSEREC.

unwritten laws—tacit, implicit codes of conduct. It would be a violation of the unwritten laws to inform on a coworker's spending habits, gambling, drinking, or sexual promiscuity—actions that on the surface appear only loosely related to national security. In the occasional case where an employee informs authorities of the questionable conduct of a coworker, the informer may become a pariah, even in the presence of written codes.

Increasing reliance on communication via computer networks has had the effect of decreasing personal interactions in the workplace, especially in large organizations. Recent studies suggest that impersonal work environments may minimize the influence of the loyalty motive (Manning, 1996; 1999) so that workers might be more ready to reported suspicious behavior. Under conditions in which the moral force of loyalty is diminished, another moral force—civility—operates in contemporary work organizations and other social systems as a means of maintaining harmony. The code of civility acts as a restraint on informing, for example, about a fellow worker's extravagant spending habits, immoderate use of alcohol, or other conduct that is identified as relevant to the government's adjudicative criteria.

We must recognize, says Sarbin, that the moral development of most government employees leads to an implicit set of beliefs that is contrary to the premises that are subtexts of the government's adjudicative guidelines. An obstacle to the implementation of a policy that expects employees to report on the behavior of their workmates is the tenuous connection between acts of espionage and a person's engaging in certain behaviors on or off the job—behaviors outlined in the DoD Directive 5200.2-R that may suggest the person is not reliable, trustworthy, and loyal, or is a security risk. People find it hard to see how common human problems, such as alcohol abuse, can be related to espionage.

Sarbin believes that it is unreasonable to expect employees to violate the deeply entrenched moral rule against volunteering to inform on the conduct of their coworkers. The fact that very little supervisor and coworker reporting occurs lends credence to his proposition.

Summary of Findings from Current Literature Reviews

Both Giacalone and Sarbin provided evidence from the literature that the level of reporting of security-related behaviors is, and will most likely continue to be, quite low. The one exception is when the behaviors observed are perceived by those in the workplace to be egregious and to clearly pose a threat to national security or the safety of others in the workplace. Sarbin points out that current policy directly contradicts years of systematic psychological research that shows that many of the behaviors that are required to be reported by the DoD Directive 5200.2-R do not, in and of themselves, make a person a security risk. He states that reporting policy, no matter how explicit, may not be powerful enough to overcome the code of civility and "the deeper moral injunction against being a snitch." In spite of the current low rate of reporting and the cultural injunction not to inform on others, Giacalone recommended several interventions to help increase the rate of reporting. These interventions were designed to make the policies

clearer and more transparent and to train supervisors and workers on these policies, the behaviors of concern, and the nexus between these behaviors and national security.

Findings from Interviews with Security and Management Personnel

Interviews with security and other management personnel provided some understanding of the complex of issues surrounding supervisor and coworker reporting. These interviews were held with 25 individuals in 10 DoD agencies and 20 individuals in 10 non-DoD agencies. (See Appendix C for a list of the agencies where these interviews were conducted.) Participants included the Director of Security or designee; and, in some agencies, representatives from Personnel or Human Resources, Equal Employment Opportunity (EEO), Internal Affairs, employee assistance programs, and the Inspector General (IG).

Following a semi-structured interview protocol (presented in Appendix D), the interviewers focused on issues concerning supervisor and coworker reporting of security-relevant behaviors, where security-relevant behaviors were defined as those covered in the adjudicative guidelines. The topics addressed included the existence or use of hotlines and other reporting mechanisms, security education and training, problems and successes with reporting, and recommendations to encourage reporting.

Use of Hotlines and Other Reporting Mechanisms

Those interviewed in over one-half of the agencies said that their employees have access to one or more hotlines. The majority of these agencies has access to the DoD IG Hotline and a few agencies have access to a local agency IG Hotline. These hotlines are primarily designed for reporting fraud, waste, and abuse and are rarely, if ever, used to report security-related behaviors. In addition, a few agencies have CI hotlines and individual agencies have Commander's, Internal Affairs, and Safety Hotlines; yet, these also yield few reports.

In all agencies, security-related concerns can be reported to headquarters (HQ) and local command or component Security Officers; Personnel, Information, and CI security managers; Internal Affairs Officers; and the IG. In addition, cleared personnel in all agencies are subject to PRs that provide the opportunity for supervisors and coworkers to report their concerns. Other mechanisms include forms to report foreign contacts, travel, terrorism, and security violations; and triggers from other sources, such as non-judicial punishment or police blotters. A few agencies have annual certifications in which supervisors sign statements assuring that their employees do not have security-related issues.

None of the agencies interviewed maintains data on the usage or effectiveness of these mechanisms for reporting security-related behaviors. No centralized, automated tracking systems exist to gather baseline data on the issues reported by source, and no mechanisms exist for determining what types of behaviors exist but are not reported. In a

few agencies, hard copy case files are kept at HQ Security; in others, reports handled in the field are not reported to HQ Security.

Across all of the agencies, those interviewed agreed that very few reports of security-related concerns come directly from hotlines and that the few concerns that are reported come directly from other reporting mechanisms (e.g., reports to command or local security managers). Commenting on the low incidence of reporting and why that would be, one manager said, "We work as a team and train as a team so we hang together. Big Brother is not the American way."

The information provided by the security managers was very consistent with data gathered in previous PERSEREC research and with the literature surveys conducted in this study. In general, those interviewed agreed that:

- Self-reports are most frequent, but still represent a minimal proportion of employees. Self-reports often occur immediately prior to PRs.
- Supervisor reports are the next most frequent and vary considerably within and across agencies. However, supervisors often deny the seriousness of behaviors and delay reporting until it is too late to prevent a breach of security or to help the employee.
- Coworker reporting is very infrequent. The few reports that are made tend to focus on overt behaviors that may directly affect the reporter or other workers. Such behaviors include safety breaches, workforce violence, child abuse, CI issues, serious emotional issues, and sometimes alcohol and drug use.

Security Education and Training

All agencies are required to have general security awareness education for their workforce. This most often takes the form of annual security and orientation briefings. Some agencies also have separate Foreign Intelligence and CI Awareness and Foreign Travel briefings. Specialized programs existing in individual agencies include CI Chronicles or Newsletters, Layman's Guide to Security Management, the Integrity Awareness Program, and promotion for hotlines.

Training for security managers and supervisors also varies considerably from agency to agency and within agencies. Some agencies require all new supervisors to attend training; however, this training most often focuses on other roles and responsibilities and provides little guidance as to how supervisors should carry out their responsibility for identifying and reporting security-related concerns. A few agencies have developed special programs to train local or command security officers, e.g., Command Security Officer Training, CI Tools Course, and quarterly security managers' meetings.

Typically, supervisor and workforce security awareness training covers general reporting responsibilities. Rarely does it provide specific guidance as to what types of

behaviors must be reported, how these behaviors are related to national security, and what are the consequences to the individuals involved—both the person doing the reporting and the person reported.

Problems with Reporting

In an attempt to understand the low rate of reporting, interviewers asked about the major problems associated with reporting in their agency. They also asked if these problems differ for employee assistance program- related issues (e.g., drugs, alcohol, financial problems) and CI-related issues (e.g., foreign influence, foreign contacts, security violations).

Mentioned by those interviewed in one-fourth to one-third of the organizations as problems were the following: (1) cultural resistance; (2) negative perceptions of reporting; (3) lack of knowledge and experience of security officers, supervisors, and the workforce; and (4) unclear relationships between Security, employee assistance programs, and other functions.

It was generally agreed that within their organizations and in our society at large there is cultural resistance to reporting on others. People are very hesitant to rat or squeal on others; instead, they are taught to protect their own.

This resistance is supported by employees' negative perceptions of reporting. Most believe that the government's zero tolerance policy discourages self- and coworker-reporting and reinforces the belief that reporting does not help the employee. Employees, who might otherwise report, may refrain from doing so because they are fearful of retaliation or legal liability.

The workforce does not have a working knowledge of reporting regulations and policies, nor does it know which types of behaviors must be reported. Several of those interviewed described this as a lack of skills needed to differentiate security-related behaviors from other risky behaviors. In addition, supervisors and security officers often lack experience in handling the issues reported, especially emotional and mental issues.

A related problem is the unclear relationship between Security, employee assistance programs, and other functions (e.g., EEO, Internal Affairs, IG, and Personnel). In essence, executive orders and directives have inadvertently codified conflicts between these functions, especially between Security and employee assistance. While it is clear that security managers are responsible for protecting national security and that the employee assistance program is responsible for assisting employees, it is not clear whether these are competing or cooperative functions. As a result, several agencies noted that competition exists among Security, employee assistance programs, IG, and HR. Others noted that, while competition may not be intentional, these functions often fail to communicate or cooperate. Highlighting this impact of conflicting policy, several noted that upper management, Security, employee assistance programs, and the workforce have

different perceptions as to whether individuals can be given safe harbor while they are receiving treatment or help if they self-report issues covered by the guidelines.

Other problems were cited by individual agencies. One agency was concerned that security managers are perceived as separate and not as part of the organization's culture; this breeds an us-against-them attitude. Other agencies noted that security managers either over-react to or ignore reports. Also, security managers are splintered throughout the agency.

Successes with Reporting

Interviewers also asked about the major successes associated with reporting in their agency and whether these successes differ for employee assistance- and CI-related issues. Successes with reporting were, for the most part, unique to specific agencies. Among those described as most effective were drug-free workplace and violence in the workplace programs. Also mentioned were successes handling emotional and mental issues, focusing on at-risk employees, encouraging self-reporting, and collaboration between Security and employee assistance. PRs, continuing evaluations, annual inspections and management certifications, security briefings and awareness efforts, security officer training, and IG promotional programs were all described as encouraging reporting and having the potential to reveal security-related issues. In addition, organizational factors were thought to have a positive impact on reporting; these included top-management support of security and education, centralization of security programs and information, and the tracking of security managers' performance.

Recommendations to Encourage Reporting

The interviewers asked for recommendations that would encourage supervisors and coworkers to value and take action on reporting of security-related issues. As with the questions on problems and successes, they asked if these recommendations differ for employee assistance- and CI-related issues. Recommendations provided by the security managers and other management personnel focused on three areas: (1) improving security education and training; (2) clarifying reporting requirements, policies, and procedures; and (3) changing the reporting policy.

Interviewees from one-half of the sites recommended improving training for supervisors and improving security education for the workforce. Specific recommendations included:

- Require mandatory security education and training for all personnel, including those without clearances.
- Identify which behaviors are a security concern as well as how and when to report these behaviors.
- Demonstrate the utility or value of the reporting policy in terms that the current workforce can understand.

- Provide continuous reminders of security responsibilities.
- Develop and share training resources among agencies.

Interviewees from one-third of the sites recommended that requirements and reporting responsibilities be made more specific in order to encourage accountability. This would involve holding agencies accountable for training of all personnel and, in particular, the training of supervisors and managers. It would also involve setting policy to remove conflicts between the Security Office and other functions, especially employee assistance.

Interviewees from one-third of the sites also recommended changing the philosophy from one of reporting (with its negative implications) to a more positive one that emphasizes helping and early intervention. This would require making employees stakeholders in the process, reinforcing confidentiality of the reporter, and assuring that the employees reported would have an opportunity to receive help before losing their jobs. This might also include the establishment of a safe-harbor program to protect those who self-report and the development of a means to track the effectiveness of such a program.

Specific recommendations made by interviewees from a few sites included:

- Improve relationships between the Security Office and other functions. This would require a closer working relationship between Security, employee assistance programs, and other functions (e.g., Personnel, EEO, Internal Affairs) to work with high-risk employees and encouraging cooperation among various reporting channels (e.g., IG and security hotlines). For example, a memorandum of understanding (MOU) can be used to clarify roles between functions in the field. The MOU can provide a legal statement of relationships of other functions with Security.
- Strengthen the continuing evaluation program. The creation of a more viable continuing evaluation program within the various commands and components might include focusing on high-risk employees with extensive knowledge and travel in intelligence and other agencies, enhancing PRs to require polygraphs and medical and mental evaluations, and the training of managers in risk management as it relates to Security.
- Improve the flow of security information. The development of a centralized security database would improve the flow and distribution of information on employees; this, in turn, would improve PRs, investigations, and early detection. As part of this centralization effort, the Joint Personnel Adjudication System (JPAS) should include information that would allow the tracking of reporting issues and sources.
- Empower security managers. To ensure that the new policies and education and training are effectively implemented, interviewees recommended that top

management provide strong leadership and financial support for the security program.

Findings from Supervisor and Employee Focus Groups

Two focus groups, one consisting of supervisors and one of nonsupervisory personnel (referred to as coworkers), were conducted at two military installations and in one intelligence community agency. PERSEREC staff got in touch with security points of contact (POC) at each venue. These POCs, in turn, invited cleared personnel within their agencies to attend the focus groups. The POCs were encouraged to invite personnel who could provide the perspectives of different areas of the organization. The majority of participants had Top Secret or SCI clearances.

The purpose of the focus groups was to discuss issues related to supervisor and coworker reporting of behaviors that may raise questions about a cleared colleague's willingness and ability to protect classified information. Participants were encouraged to discuss the topic with their colleagues prior to the focus group, so that their contributions would reflect a combination of their own personal experience as well as what they had learned from others.

Ground rules for the focus groups ensured the agencies and the participants complete anonymity (Appendix E). The focus group protocol (Appendix F) consisted of five very broad questions:

1. Are you aware of the requirement that supervisors and coworkers are to report certain kinds of behaviors by their cleared colleagues to security managers or other authorities? What does this requirement mean to you? How well does it work around here?
2. Do you think the government should even try to get people to report? Why? Why not?
3. Do you have any recommendations concerning the reporting requirements or the way in which reporting works or is handled here in your agency?
4. What could the government do to encourage people to report subordinates or coworkers who may be a security risk?
5. Are there ways that the reporting requirement could be explained more succinctly so that the rules and boundaries are clear?

A total of 20 supervisors and 19 coworkers participated in the six focus groups. Findings from these groups provided additional insights into the infrequent reporting of security-related behaviors and to the impediments to such reporting. In the sections to follow, topics that emerged from the focus groups are described.

Supervisor Focus Group Themes

Several themes surfaced from the supervisor focus groups. These included supervisors' knowledge and acceptance of the reporting requirement, clarity of the reporting system, effectiveness of the security system, and security awareness and training.

Knowledge and Acceptance of Reporting Requirement. Asked if they knew about the requirement in the DoD Directive 5200.2-R that supervisors must report security-relevant behaviors, the supervisors indicated that they clearly understand and wholeheartedly accept their responsibility to report behaviors that have "a direct nexus with security." "If you have knowledge of a violation and you do nothing about it, you are equally responsible." Examples of these behaviors included foreign contacts, security violations, theft of credit cards, unexplained affluence, abuse of computers, and violence in the workplace. Most supervisors do report people who represent a danger to fellow employees, e.g., people who threaten to kill their boss, people who pull knives on others in the parking lot. These are direct threats to the safety of workers. Supervisors also are concerned about people who are angry and threatening.

Supervisors were somewhat less clear about their understanding and willingness to accept their responsibility to report behaviors that are not clearly linked to national security, e.g., alcohol abuse, marital problems, emotional/mental disorders, and sexual behavior. Supervisors try to handle internally those behaviors they perceive to be less egregious rather than reporting them to security managers. "I would only report egregious acts for which people would lose their jobs. Most other behaviors, such as marital problems, are not reported up the chain. We get intelligence on our employees if they are having marital problems, but we tend not to report these kinds of things to Security. We don't want our staff to lose their jobs. Employees are afraid of Security and losing their clearance. If someone has, say, a drinking problem, we manage it internally and keep an eye on the person's behavior and counsel him." "I want to protect national security, but I also want to protect the integrity of the person. I would try to take care of the problem before reporting it to Security. But if it's something that directly affects security, that is a different ball game."

Another person expressed a similar opinion on reporting obvious breaches of security. "When it is really important, there is no one in this room who wouldn't report to Security. If we thought there was a threat, we would report it." However, that same person would hesitate in reporting less obvious behaviors. "But the things that are questionable are the personal things...You don't want to play God. Who is qualified to do that?" "There are gray areas. When we don't know, we are inclined to give people the benefit of the doubt [and not report]." "With things like alcohol and emotional/mental, for every case that is reported, 100 are not."

In an interesting twist, supervisors at one agency suggested that "reporting responsibilities should not be foisted solely on the supervisor. Sometimes you hardly ever see your employees." Others affirmed that supervisors are critical to the chain. "The

supervisor is going to know most about an individual's performance and can actually act as a protection for the person."

The Reporting System Is Unclear. "The rules are not clear-cut. For myself, if I am ever unsure, I call Security. If it's a theft of security material, it is one thing. But if it isn't a risk to security [personal problem], you are not going to turn it over to Security because you don't know what Security's going to do with it. We [supervisors] know our people better than Security. Even though the Security Office here is very willing to work with people and listen, they don't know the person being reported, and we supervisors do. We are constantly dealing with risks and gray areas."

Supervisors feel that "employees in general don't understand the security system. They don't know what is going to happen if, say, they declare bankruptcy or have a divorce. When we hit gray areas we try to protect the people who work for us. Why can't these reporting requirements be made clearer to employees? We should be told, 'Here are the rules.' "

According to these supervisors, there is another layer. Not only are employees confused about what the local Security Office does with reports, the local Security Office is confused about what the centralized adjudication facility (CAF) does with reports it forwards up the line. There is no feedback between security managers at an installation and the CAF at headquarters.

"We need a clear communication of what is mandatory to be reported and what is discretionary. We need clearer rules about what should be reported up the chain. Knowing where we have discretion would be good; knowing where Security has discretion would also be good. We need to have an idea of a sliding scale of seriousness of behaviors so that we'll know what we absolutely must report."

Again, reluctance to report the more personal issues was stated. "Most supervisors do report bad things. But these little things, on-the-edge, gray areas. These are the problems." One participant suggested that all behaviors be categorized as Red, Yellow and Green, just like traffic lights. Red would be a stopper (really egregious behavior), and Yellow caution. In this way there would be a prioritization of behaviors to be reported.

Effectiveness of the Security System. The supervisors indicated that the security system is often ineffective in addressing problems. "The security system is grinding. We must feel that if we do go out on a limb something will happen." Supervisors are concerned with losing control once the report has been made because at the point they can no longer help the person. Said one participant, "When things go to Security, they are pretty much out of our hands. As supervisors we can see the entire picture; a person may be just going through a bad time. I don't want the big axe to fall on the head of one of my people."

Security managers are seen as inflexible, strict law-enforcement personnel that follow the letter rather than the spirit of the law. They are also seen as wresting control

from supervisors. "With Security, it's the death penalty!" said one participant, jokingly. Another, not joking, said, "Supervisors fear loss of control when the problem goes to Security." As an alternative, many supervisors prefer to handle problems via Human Resources. "With Security you're in or you're out. It's black or it's white. You get the clearance or you don't and, if you don't, you don't work. On the other hand, Human Resources [another place to report problems] operates on a sliding scale, with its own gradations of punishments."

"Reporting is a big step and it weighs very heavily. It's a black mark on people's records. You had better be sure that the person has really done something illegal before reporting him." Another participant described her anguish about reporting someone she didn't feel should hold a clearance. The person wasn't a direct subordinate, yet she did find the nerve to speak out during a PR interview. "It took so much for me to say that, and I will think two or three times before I ever do something like that again. I was very worried about it [the employee's behavior], but they dismissed my report. Not long after, the woman I had reported had a total and complete nervous breakdown." "It's easy to monitor performance: performance can be seen, documented, justified. But how do you assess security risk? That's the big question."

Despite the previously cited examples of security as ineffective, some supervisors indicated confidence that Security is the quickest and most effective way to address certain problems, i.e., when you want to terminate someone from government employment. "Security is the quickest way to get rid of people. Human Resources (HR) can take months, years." A story told by one of the supervisors illustrates this point. "An employee came on site and brought an argument he'd had outside the workplace to the workplace. He pulled a knife on someone in the parking lot. I was the person on call that night so I got the call. Pulling the clearance and getting him off site was the easy bit; the HR process is very difficult to deal with and it can take a long time [to fire him]."

One participant also saw security managers as a support for supervisors. "I don't know how to take care of the problem myself. I don't know what I am able to do about it. Will I be able to change someone's behavior? I would report the problem to Security. I am not going to take this on as a personal challenge. If it is a potential threat, that has to be reported. What can I do to relieve the situation as a supervisor? You have to employ the professionals [security personnel]."

Security Awareness and Training. There seems to be a desire for the old, theater-style briefings instead of Internet training. "We used to have education. Briefings in the theater. Real briefings for everyone—All Hands. Now Security is short-handed and we get our training on the Internet."

"I think refresher courses should be given on the subject of reporting requirements. Supervisors have good training, although a lot has been done on-line. For security training, we need a single person to give the briefing, perhaps at a monthly meeting, instead of sending people to their computers. It makes it more real to have a live person give the presentation."

"We need to get out examples and tell people that they should not have to be frightened to report things."

Summary of Recommendations by Supervisors. Supervisors clearly understand and are willing to accept their responsibility to report security-relevant behaviors, but are less understanding and willing to report behaviors that are not directly linked to national security. Typically, they try to protect their employees by handling internally suitability-type behaviors that they perceive as not clearly linked to national security. If they need assistance dealing with an employee who has personal issues, they may turn to Human Resources managers, who appear to have more choices than security managers.

Supervisors feel as if they lose control and that the case goes out of their hands when they report a person to the security manager; they would like to see closer coordination and feedback between security managers and themselves. They see the need for more clarity and transparency in the security system. They want clear-cut rules that they can explain to their subordinates and more information from the Security Office for employees in terms of what should be reported.

Supervisors regret the passing of the old, theater-style briefings that have long since been replaced in some agencies by Internet training. They recommend refresher courses on the subject of reporting requirements; these should be given by a single presenter, and in person. Computer training, despite its cost-effectiveness, is less meaningful than a real live human being speaking directly to an audience.

Coworker Focus Group Themes

Major themes from the coworker focus groups concerned the requirement to report, lack of clarity of the security system, and security awareness and training. Participants discussed coworkers' knowledge of exactly what to report, to whom to report, and the ramifications for the person reporting and the person reported. "At the moment it is all just confusing," said one participant.

Eyes and Ears of the Government. The participating coworkers understand and accept their responsibility to report behaviors that may potentially jeopardize national security. "Yes, reporting is our responsibility. If we don't do it, who will? The requirement is reasonable. And the government needs to have eyes and ears." "I have no problems with reporting something, and most people agree that they will mention it if they see something. If something was amiss somewhere, we'd have no problem about reporting it." Although they seem to have no problem with this, they questioned others' knowledge and willingness to comply. "A lot of people don't remember that [they should report] or say that they don't know that they are supposed to report."

The coworkers acknowledged that the eyes-and-ears arrangement was not effective in the cases of Ames and Hanssen, both convicted spies. They also acknowledged that keeping an eye open is not always effective in their work

environment. Most were confident of their ability to report, especially if the behaviors were really serious, e.g., an obvious security violation or violence in the workplace. "I always bring up the issue about things that are going on. [I tell my coworkers] to pick up the telephone, and call. I have a responsibility to protect your [coworker's] confidentiality." Others had reservations about their ability to truly perform this role, especially if the behaviors were in the more personal realm where the link to security is not quite so obvious. "I err on the side of being conservative [not reporting] when dealing with mental health or marital problems. If it comes to me, I always say let's talk to the people who are professionals. It can become very destructive and nobody knows what to do." "We are the eyes and ears of the government, but it is difficult to do. The task is not defined well."

The Reporting System is Unclear. The participants emphasized that the security system and reporting procedures are unclear. Areas needing clarification include what is reportable, to whom to report, what happens to those who report or are reported, and the security process itself.

- **What is reportable and reported?**

  Coworkers want to know exactly what is reportable. Some actions are obvious, but there are many gray-area behaviors. The system is very unclear, very nebulous.

  Participants acknowledged a hierarchy of reportable behaviors. "I think that security violations are the most important to report. Physical things that you can see that are out of place, things you can do something about. Next come the things that someone can be compromised for, like alcohol, drugs, gambling. Then you get to the more private things. I wouldn't report unless I worked with the person and knew the behavior was linked to security. And I'd have to be able to prove it."

  As with supervisors, coworkers wondered where to draw the line between obviously reportable behaviors and more personal problems. "What is it you are supposed to be looking for and what is your responsibility to report? If it is concrete, then it's understandable. Someone walks out of work because they are upset or there is a violent incident. That you can understand. I don't want to cause trouble for people. All of us have had our own problems, personal and family problems. As a human being I understand that. But we also want to be safe and we don't want to experience backlash from colleagues or supervisors."

  Coworkers want to know precisely what to report, to whom to report it, and the precise consequences to the person reported and, also, to themselves. "You can't ask people to do something if you don't define it." "Not everyone has the 13 adjudicative guidelines on their desk. We need more definitions." "How do we know which behaviors are OK and which are not? And how do we know what happens in the end? There is no feedback loop. If we really understood what

Security does, that would make me feel comfortable. Security should identify what they expect of me. They shouldn't be nebulous about it. I need to know their expectations. Serious infractions are clear to us, but all the rest isn't at all clear." Not knowing the resolution to a situation is a huge problem. "What was the outcome? Nothing could be proved? Nothing happened? And that then becomes a morale problem for us."

It was clear that many behaviors are not reported. "You have to be very sure of your facts before you report because the person can land up in great trouble. We have to protect other coworkers. Reporting can become very destructive and nobody knows what to do." One participant, describing a coworker, said, "When he gets in the elevator, he reeks of alcohol. His behavior is known and he has been disciplined. But the drinking is still occurring and it is known to everyone." Another said that she had smelled alcohol on a coworker at lunchtime, but that his behavior was not "funky." "I have never witnessed this individual doing anything wrong on his job." The coworkers indicated that, while serious, alcohol and drugs are seen as personal, not security, issues.

"These are changing times. I guess you have to weigh everything. Where do you make the judgment calls? I don't think that is clearly explained."

- **To whom should you report?**

There were differences of opinion as to whom to report—to the supervisor or to the security manager. Some workers only see their supervisors once a year; and others were unaware that the security manager even exists. Frequently it is a matter of trust—who you know (supervisor or a trusted contact in Security). Some were adamant that they would report to their supervisor. "I wouldn't want to report somebody's problem to a stranger. I would go to my supervisor because I am more comfortable talking to him. I don't know Security and the last thing I would do would go to them to report. It's a trust issue." Others would bypass the supervisor and go directly to the security manager. "I have a lot of relationships with people in Security. And I wouldn't go to my supervisor if it were a security issue."

"There is more of an emphasis on physical security because of terrorism. It is this other stuff...!" The participants feel uncomfortable about the "other stuff," the personal, often very private information they either observe or hear about over the half-walls of their office cubicles.

"When you report it to Security, you don't know the agenda of the person you are reporting the behavior to. What rules is Security going to use when handling the problem? It isn't the rules but what the person who is looking at the rules will do with the report. You could ruin someone. That would make you shy away from reporting."

- **What are the consequences of reporting?**

People fear telling supervisors or security managers because they don't know what the outcome will be. Perhaps the supervisor does nothing about the report; perhaps the security manager comes down like a ton of bricks on the reported person who then loses his job; perhaps the reporter will suffer retaliation if it becomes known he or she did the reporting. "I want to make sure that I am certain before I report something serious. Somehow people find out that you have reported and it comes back on you."

"We need some education on personnel security, not just what to report but what happens afterwards. It's a gray area. I don't know. You don't want anything really bad to happen [when you report]. We need some education about what Security does. At present it's a fuzzy mess that we don't really understand."

"Where are the guidelines? What are some of the parameters? How are we supposed to know what we are supposed to report? There are no boundaries. If the government wants us to be its eyes and ears, they should define the rules and explain to us what the processes are and what we are risking by reporting." Like several other participants, this person believes there is no feedback. "This seems to be the nature of Security. For us, you need to know in advance what the system is going to do."

One major impediment to reporting is not knowing how the report will affect the person being reported. "The problem with reporting is the possible damage to someone's career. You don't want to hurt people." Another impediment is confusion about how the reporter will be received. "You tell your supervisor and it doesn't go anywhere. But people somehow find out that you reported it and they are down on you. Especially in the close quarters that we are in. It is bad. Going to the supervisor didn't help anything." In spite of this, one coworker said, "There's a stigma to being labeled [as someone who reports]. But I am a loner and I don't care what people think of me. I will report security violations."

Some coworkers indicated that there are two levels of discipline: one for lower-level and one for higher-level employees. They believe that rank-and-file employees are swiftly disciplined and often lose their jobs; whereas, upper management seems to "get away with things." "The higher-ups don't like to discipline each other. It [inappropriate behavior] gets swept under the rug. I guess they don't want to be known as trouble. The higher-ups are immune from discipline." Sometimes, these individuals are moved around within the agency, rather than higher management dealing with the problem head-on. In frustration, one participant said, "When people see that kind of thing going on, they just say to themselves, 'Why even bother?'"

"Security should show us the processes and procedures of how they handle something. I have to have some level of confidence that the security people are following consistent processes and procedures and protecting people's rights before I am going to open my mouth. Trust is important. And there's no feedback. A letter or even an e-mail from Security saying that they have taken the information you gave them and everything is OK would be good."

Security Awareness and Training. Coworkers would like better security education. They don't like getting their security awareness education on the computer or via mass meetings of employees in a large auditorium. They recommended training within small groups, where they could hear about and discuss real-live scenarios and examples. "I believe in training and having effectiveness training for adults. I know it would cost more money and take more time, but then we could do scenarios. Otherwise, the briefings do not explain things in real terms. In the large briefings, the materials are read to us and we, the audience, don't get an opportunity to talk. Also, we don't necessarily want to see scenarios of extreme cases, like the spies. We want to hear about examples of ordinary people. We know that there is a lot of gray area in all this that never gets addressed. We want to be told how you make the boundaries clearer. I don't really know the answer. Times change, enemies change. When you have hot-topic problems like sexual harassment or terrorism, they do the briefings very well. Why not give the same treatment to briefings on reporting requirements?"

To explain the procedures to new and old employees, the coworkers suggested a small-group indoctrination that could be set up where you mix new hires and old-timers and explain the rules to both sets of people. "Break security briefings down into smaller groups. We need to know. When things are kept in the dark, you feel alone. In small groups you can talk to people and it helps to know where to go to report."

Another solution to the problem is, "Have Security go around and talk individually to people and get to know people. Security should get out more. They could talk to us either one-on-one or in small groups of, say, no more than 15. These small groups [e.g., the present focus group] really help."

Summary of Recommendations by Coworkers. Coworkers are presently confused by the security system and the coworker-reporting requirement. They want clearer guidance on the boundary between egregious behaviors and the other, more personal, gray-area behaviors that are also required by DoD Directive 5200.2-R to be reported. They want a system that tells them clearly what to report and to whom to report it. They want to reduce any caprice in the system. They want security managers to show them "the processes and procedures of how they handle something." In this way, they believe they will develop "some level of confidence that the security people are following consistent processes and procedures," which will make them more inclined to report. Coworkers recommend that receipt of their reports be acknowledged by letter or e-mail and that security managers eventually inform them concerning the disposition of the case reported.

Like the supervisors, coworkers do not like getting their security awareness briefings on the computer. Nor do they like mass briefings in large auditoria. They recommend mixing new and old employees into small-group indoctrination sessions where "you can talk to people."

Conclusions

The authors of this report conclude that there will always be some tension between the rules associated with supervisor and coworker reporting and cultural values not to inform on colleagues. This is especially likely in cases where the "infraction" is not perceived to be an illegal activity or security violation but a common, and often transient, personal problem. Yet, provided they understand the nexus, study participants have no objection to being the eyes and ears of the government. They believe that transient personal problems may be better handled in a different manner, perhaps by the supervisor through referral to employee assistance programs or other kinds of monitored treatment programs.

This study points to the need to increase the reporting of critical and obvious security-related behaviors, which employees say they are willing to report. It suggests drawing a clearer distinction between the reporting and consequences of these egregious security-related behaviors and suitability-type behaviors of a more personal nature that realistically are not likely to be reported. By clearly communicating these distinctions to supervisors and coworkers and by encouraging supervisors to become more proactive in addressing suitability issues, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence (ASD [C3I]) may be able to increase reporting of truly serious security infractions.

Recommendations

1. **ASD (C3I) change the DoD Directive 5200.2-R to make reporting security-relevant behavior a priority and to provide anonymity for people who report.**

   DoD Directive 5200.2-R acknowledges in Chapter IX that people will only meet their security responsibilities if they understand them, thus emphasizing the importance of security education. Supervisor and coworker reporting is not mentioned in descriptions of the various types of security education briefings (initial, refresher, foreign travel, and termination) in Section 2 of Chapter IX. It is recommended that the directive be amended to include supervisor and coworker reporting requirements as a priority.

   There is also no provision in DoD Directive 5200.2-R for ensuring the reporter's anonymity. Since many interviewees in this study expressed their hesitancy to report because they feared possible adverse consequences for themselves, wording should be inserted into the directive that assures that the confidentiality of reporters will be protected and guaranteed, if requested, and that only security managers will

know the identity of the reporter. Safeguarding the reporter should also be a topic in security education briefings.

2. **PERSEREC develop a list of behaviors of national security concern that must be reported if observed.**

This study's findings show that supervisors and coworkers are willing to report egregious behaviors that pose a palpable threat to national security. Because supervisors and coworkers also say they are unclear as to exactly what these behaviors are, PERSEREC should develop a list of these behaviors. The list would not include behaviors of a suitability and reliability nature since the research has shown that people are hesitant to report such matters anyway. If the list is limited to truly egregious and critical behavior, then the rate of reporting will likely increase.

The list should be developed with the help of CI and security personnel, with a final draft being submitted for review to a sample of rank-and-file supervisors and employees in the field. Each item in the list will be accompanied by scenarios and behavioral examples to make clear to employees exactly what the security and CI world considers egregious and critical. Subsequently, the final list should be communicated to the components by policy memorandum.

Supervisors would be accountable for reporting serious security-related behaviors and for ensuring that their cleared employees understand the behaviors that must be reported. They would be responsible for referring people with less-critical issues (from a national security standpoint) to employee assistance programs or other remedial programs. Cleared employees will also be required to report serious security-related behaviors.

3. **ASD (C3I) issue a security policy memorandum advising that certain changes must be made in the government's approach to supervisor and coworker reporting.**

A major, unstated policy issue concerning the role of security managers underlies this report. What is their responsibility for continuing evaluation? Is it only to decide when some adverse action needs to be taken relating to a person's clearance? Or does it also include being proactive and ensuring that people's personal problems get addressed before they become security problems? The authors recommend that the DoD make more explicit its security policy to, first and foremost, protect national security, particularly in cases where there are indications of potential CI activity. It should also clarify the circumstances under which supervisors should refer troubled employees to employee assistance programs or other remedial programs before their problems become a security concern.

ASD (C3I) should issue a memorandum making it explicit that security managers and supervisors have a proactive role to play in preventing security problems due to suitability issues. The statement should outline policies regarding how and under

what circumstance security managers should refer personnel for assistance rather than punishment when their actions are reported. This memorandum should also clarify the relationship between Security, employee assistance programs, and other functions.

Related to the above, the memorandum should address the problem of making reporting policies and procedures as transparent as possible for all employees. There should be more clarity in the security system, with clearer-cut rules as to what to report. There should be closer coordination and feedback between security managers and employees. Security managers at the very least should acknowledge a report was received and, if appropriate, inform the reporter of the eventual outcome. The reporter's confidentiality must be honored and protected.

The memorandum should also re-emphasize the importance of training for both supervisors and coworkers. This training should regularly remind supervisors and coworkers of their reporting responsibility. It should provide practical guidance on indicators that may signal matters of security concern and should outline personnel security policies and procedures, including categories of behavior to be reported and provisions for helping troubled employees. Such training would be developed by the Joint Security Training Center (JSTC) and provided to the components for implementation. The training should be conducted in person, not via the Internet, and should allow ample time for participants to interact with the presenter and among themselves.

4. **Joint Personnel Adjudication System (JPAS) Program Office develop and implement a system for recording and tracking in JPAS supervisor and coworker reporting of security-related concerns.**

At the present time, data do not exist concerning the extent of reporting by supervisors and coworkers, to whom the information was reported, and the results of the reporting. Without a tracking system, it will not be possible to precisely describe the problem and to evaluate the impact of steps taken to increase reporting. Thus, it is recommended that the JPAS Program Office add data fields to the JPAS database so that the source (including supervisors and coworkers) and nature of the information can be captured and evaluated. Security managers will be provided with guidance on how to code and enter reporting data into the JPAS. At the same time, they will report the information to the CAFs. In this way, it will be possible for ASD (C3I) to track reporting behaviors and to evaluate and adjust policy and training as needed.

5. **PERSEREC develop and field a survey to establish trend data concerning security-related behaviors that are observed and reported.**

To address a related concern about behaviors that are not reported, it is recommended that PERSEREC conduct a periodic survey of supervisors and employees within the DoD. The survey would be similar to the Whistleblower Survey of fraud, waste, and abuse behaviors, in that it would take the pulse of the workplace (Erdreich, Parks, & Amador, 1993). It would identify behaviors related to the

adjudicative guidelines that are observed in the workplace, the extent to which these behaviors are reported, and the results for both the person reported and the person who reported. It would also elicit reasons why supervisors and coworkers do not report the overwhelming majority of the behaviors they observe.

The first three recommendations will clarify and explain reporting policy. The JPAS tracking data, in combination with the survey data, could result in an effective feedback mechanism whereby reporting policies are evaluated and, if need be, altered. Combined, these recommendations have the potential to increase the rate of reporting and to encourage employees to obtain assistance before their problems become a security issue.

References

Barron, J. (1987). *Breaking the ring: The rise and fall of the Walker family spy network.* New York: Houghton Mifflin.

Blitzer, W. (1989). *Territory of lies: The rise, fall, and betrayal of Jonathan Jay Pollard.* New York: Harper & Row.

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). *Continuing assessment of cleared personnel in the military services, Reports 1-4* (PERS-TR-91-1 through 4). Monterey, CA: Defense Personnel Security Research Center.

Director of Central Intelligence 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information,* Jul. 2, 1998.

DoD Security Review Commission. (1985). *Keeping the nation's secrets: A report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices* (known as the Stilwell Commission). Washington, DC: Office of the Secretary of Defense.

DoD Directive 5200.2, *DoD Personnel Security Program* (April 9, 1999).

DoD Directive 5200.2-R, *Personnel Security Program* (January, 1987, revised Feb. 23, 1996).

Erdreich, B.L., Parks, J.L., & Amador, A.C. (1993). *Whistleblowing in the federal government: An update.* Washington, DC: U.S. Merit Systems Protection Board.

Executive Order 12564, *Drug-free Federal Workplace* (Sep. 15, 1986).

Executive Order 12968, *Access to Classified Information* (Aug. 2, 1995).

Federal Employee Substance Abuse Education and Treatment Act (P.L. 99-570) of 1986.

Fischer, L.F. & Morgan, R.W. (2002). *Sources of information and issues leading to clearance revocations.* Monterey, CA: Defense Personnel Security Research Center.

Giacalone, R.A. (April, 2001). *Coworker and supervisor disclosure of reportable behavior: A review of proxy literature and programs.* Paper presented at a colloquium on Obtaining Information from the Workplace: Supervisor and Coworker Reporting. Monterey, CA: Defense Personnel Security Research Center.

Joint Security Commission (1994). *Redefining security: A report to the Secretary of Defense and the Director of Central Intelligence.* Washington, DC: Author.

Joint Security Commission (1999). *A report by the Joint Security Commission II.* Washington, DC: Author.

Kramer, L.A., Crawford, K.S., Heuer, R.J., & Hagen, R.R. (2001). *Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) source yield: An examination of sources conducted during the SSBI-PR* (TR-01-5). Monterey, CA: Defense Personnel Security Research Center.

Manning, P.H. (1996). Drama of Control. In Sarbin, T.R. (Ed.). *Vision 2021: Security issues for the next quarter century*. Monterey, CA: Defense Personnel Security Research Center.

Manning, P.H. (1999). Reflection: The Visual as a Mode of Social Control. In Ferrell, J., & Websdale, N. (Eds.). *Making trouble*. New York: Aldine.

National Imagery and Mapping Agency (Producer). *Security awareness 2000.* Reston, VA: NIMA.

Sarbin. T.R. (April, 2001). *Moral resistance to informing on coworkers*. Paper presented at a colloquium on Obtaining Information from the Workplace: Coworker and Supervisor Reporting. Monterey, CA: Defense Personnel Security Research Center.

Wood, S. (2001). *Public opinion of selected national security issues: 1994-2000* (MR-01-04). Monterey, CA: Defense Personnel Security Research Center.

Appendix A

Analysis of Security Agency Policies as Translated into Military Service and Agency Requirements for Reporting Adverse Information

Analysis of Security Agency Policies as Translated into Military Service and Agency Requirements for Reporting Adverse Information

The military services have their own policy regulations that are modeled on DoD Directive 5200.2-R.

Department of the Army

AR 380-67, *Personnel Security Program*, dated September 9, 1988, describes in Chapter 9, Continuing Security Responsibilities, the responsibilities of management, supervisors, individuals, and coworkers for reporting to authorities behavior that might jeopardize national security. Commanders are required to ensure that employees are periodically instructed after their indoctrination on the national security implications of their duties and individual responsibilities. Commanders are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives.

Supervisors should be made aware of their special responsibilities and receive training in such matters, especially in terms of when and how they are to report information about their subordinates.

Individuals must make themselves aware of the standards of conduct required. They must also be instructed in what to report and to whom. The regulation lists various types of reportable actions, e.g., any form of contact with a citizen of a designated country, attempts at cultivation by citizens of designated countries, etc.

Lastly, coworkers must advise their supervisors when they become aware of information with potentially serious security significance regarding someone in a sensitive position.

Department of the Navy

The Navy's instruction is SECNATINST 5510.30A, *Department of the Navy Personnel Security Program,* dated March 10, 1999. Chapter 10 discusses continuous evaluation (CE).

The instruction states that CE is required to ensure that everyone who has access to classified information remain eligible for a clearance. Commanding officers must establish and administer a program for CE, a program that relies on all people in the command to report questionable or unfavorable information.

While the ultimate responsibility for maintaining eligibility to access to classified information is said to rest with the individual, coworkers also have an obligation to advise their supervisor or security officer of any information of potential security significance. Supervisors and managers also play a critical role, says the instruction, in assuring the success of a CE program. Supervisors must try to balance the needs of the

individual and the requirements of national security. Keys to an active CE program are security education and positive reinforcement of reporting requirements in the form of management support, assurances of confidentiality, and employee assistance referrals.

The instruction goes on to explain that individuals must understand what is required of them as part of their security responsibilities, so an effective security education program is needed. Personnel must receive indoctrination and orientation training on the national security implications of their duties; they must also receive annual refresher briefings. These briefings should inform them of the avenues open to them should they require assistance or have difficulty in maintaining trustworthiness standards.

Each commanding officer must establish a program for cleared employees to educate them about personnel security responsibilities and to inform them about available guidance and assistance programs. Commands should identify individuals with personal issues at an early stage and guide them to programs designed to counsel and assist them.

Employee fitness ratings must include an evaluation of how the employee manages. The intent is to encourage supervisors to refer security concerns as soon as they become apparent, and to provide supervisors an opportunity to annually assess their employees regarding continued eligibility to access classified information.

Chapter 10 ends with a two-page continuing evaluation check list of what should be reported to the Department of the Navy Central Adjudication Facility (DON CAF), along with a series of factors associated with the "issue," i.e., nature and seriousness, circumstances surrounding, frequency and recency, age at the time, motivation, how command became aware, etc., that should also be reported.

Department of the Air Force

The Air Force's instruction is AFI31-501, *Personnel Security Program Management* (May 1994 and revised August 2000). Chapter 9 briefly discusses continuous responsibility for security and refers the reader to DoD Directive 5200.2-R. It describes supervisors' responsibilities. Supervisors are not to review the security forms of anyone undergoing a periodic reinvestigation (PR); any behavior that needs to be reported should be observed directly by the supervisor. There is no mention of coworker reporting. Chapter 9, consisting of less than one page, also discusses initial, refresher, foreign travel, and termination briefings.

Appendix B

Study of Unique Sources of Issue Information in Periodic Reinvestigation Cases

Study of Unique Sources of Issue Information in Periodic Reinvestigation Cases.

As part of the current study, the research staff selected and conducted an in-depth review of a very small sample (N = 49) of periodic reinvestigation (PR) cases in which supervisors and coworkers provided information of a security nature. These cases were *not* intended to be representative of all PR cases; rather, they were selected to provide insights concerning the types of issues reported by supervisors and coworkers during PR investigations and the uniqueness of the information reported by these sources. It is important to note that the information provided in these cases did not result in revocation of the employees' clearances. It is also important to note that, due to the nature of the investigative reports, the researchers could not distinguish between information that the individuals being interviewed volunteered on their own and information that they provided in response to the investigator's direct questions.

With the exception of the Subject, all of the sources who provided information in these cases were supervisors or coworkers who were currently working with, or had worked with, the Subject. These supervisor and coworker sources were further identified as follows:

- Employment references (ERs) were the employee's current supervisors and coworkers;
- Listed references (LRs) were past or current supervisors and coworkers whose names were provided by the Subject on their *SF86*;
- Neighbors were current or past supervisors and coworkers who lived near the Subject; and
- Developed references (DRs) were present and past supervisors and coworkers whose names were identified during interviews with the Subject, ERs, LRs, or neighbors.

The objective of this case review was to determine the degree of uniqueness of the information provided by different sources during PR investigations. Unique information was defined as that provided by a *single* type of source (e.g., only the Subject or only ER/supervisors). From a cost-benefit perspective, unique sources of information were considered most valuable because, without these sources, potentially important issue information might not have been uncovered.

The most productive source of unique information was the Subject. In almost two-fifths of the cases, the Subject provided unique information covering 10 of the 13 guidelines. Most frequently revealed by the Subjects were financial problems, such as bad debts and credit card issues, and foreign connections, such as having relatives or acquaintances in foreign countries. Several Subjects revealed outside employment, alcohol-related issues (e.g., DUIs), emotional/mental/personality disorders, and personal conduct issues. Reported by one or two Subjects were issues dealing with security

violations, sexual conduct (e.g., alleged child sexual molestation), criminal behavior, and drug use.

The second most productive source, providing unique issue information in slightly less than one-third of the cases and covering seven of the 13 guidelines, was the Subject's current ER/supervisor. Behaviors most frequently mentioned by these supervisors related to emotional, mental, and personality disorders and outside activities. For example, supervisors reported that Subjects were participating in psychological counseling, had been prescribed medication for emotional problems such as depression, or had been required to attend anger management classes. They also reported criminal behavior (e.g., allegations of domestic violence, the fraudulent use of credit cards,), alcohol abuse, drug use, security violations, performance problems, and personal conduct issues (e.g., falsification of records).

DR/Coworkers and ER/Coworkers each provided unique information for about one-tenth of the cases and covering five of the 13 guidelines. Examples of behaviors uniquely noted by DR/Coworkers include poor work performance, paranoia, potential danger to others, downloading of pornography, and inappropriate physical contact. Examples of behaviors uniquely noted by ER/Coworkers include laxness in protection of classified documents, foreign contacts, and outside employment.

Least productive as a unique source of information were LR/Coworkers and Neighbor Coworkers. Examples provided by LR/Coworkers include alcohol counseling, contacts with foreign nationals, relatives in foreign countries, and bankruptcy. Neighbor Coworkers were infrequently interviewed and seldom provided unique information. However, in one case, the neighbor coworker had discovered a Subject in a potential attempted suicide and had obtained medical care for the Subject in this emergency. While not cognizant of the details, the supervisor had also mentioned that the Subject had been hospitalized.

Although these findings are based on an extremely small number of cases and cannot be generalized to all PR cases, they provide some understanding into the types of information reported by supervisors and coworkers and the degree to which such information adds value to the investigative results. This research found that Subjects and their supervisors can be valuable sources of unique information—information that was not revealed by other sources. It also found that ER/Coworkers and DR/Coworkers may provide unique information in a very small percentage of cases; and that LR/Coworkers and Neighbor/Coworkers generally cannot be expected to provide unique information. Most importantly, these findings suggest that, *when interviewed directly*, some supervisors and coworkers are willing to report issues they consider relevant to national security.

Appendix C

Agencies That Participated in the Security Manager Interviews

Agencies That Participated in the Security Manager Interviews

DoD Agencies	Other Federal Agencies
Headquarters, Department of the Army	Central Intelligence Agency
Naval Criminal Investigative Service	Customs Service
Headquarters, Air Force	Department of Energy
Headquarters, Marine Corps	Federal Bureau of Investigation
Defense Intelligence Agency	National Aeronautical and Space Agency
Defense Information Security Agency	National Reconnaissance Office
Defense Logistics Agency	Nuclear Regulatory Commission
DoD Inspector General	National Imagery and Mapping Agency
Defense Security Service	State Department
Washington Headquarters Service	United States Coast Guard

Appendix D

Protocol for Agency Security and Other Management Interviews

Protocol for Agency Security and Other Management Interviews

In-person _____ Via Telephone _____

Agency: _____

POC Name and Position Title: _____

Mailing Address: _____

E-mail Address: _____

Phone Number: _____ Fax Number: _____

Date of Interview: _____ Time Started: _____ Time Ended: _____

Introduction

Hello. My name is _____. Thanks for arranging to talk (or meet with me) about supervisor and coworker reporting at (agency name).

This interview will take about 30 minutes – somewhat shorter or longer depending upon the extent of supervisor and coworkers reporting in your agency. To ensure that we obtain consistent data from different Federal agencies, I'll be following a general outline of questions. Of course, if you are interested and have the time, we can discuss other related issues of particular importance to your agency.

During the course of the interview, please keep me abreast of your time constraints. That way, I can cover the most important questions first and leave others for a later time or discussion with others in your agency.

Section 1. Executive Orders, Regulations, Instructions Pertinent to Reporting

1. **Which are the major executive orders, regulations, and instructions covering supervisor and coworker reporting of security-related behaviors in your agency?** (Share handout and leave with POC to complete later if requested. Check or list those mentioned and request copies of those not listed be sent to PERSEREC)

   Handout: List other executive orders, directives, regulations, instructions, etc. Request that copies be sent to PERSEREC)

2. **Which of the executive orders, regulations, instructions, *etc.*, mentioned above are most relevant to supervisor and coworker reporting and how?**

3. **What other areas, if any, should policy and implementation documents cover?**

Section 2. Reporting Mechanisms, Including Hotlines

Our goal is to find out from each agency how many people report their supervisors and coworkers and the types of issues they report.

4. **Hotline: Does your agency have a hotline that supervisors and coworkers can use to report security concerns?** (Mention agency hotline, if known. If Yes, see Hotline Questions below.).

   _____ Yes _____ No _____ Don't know

   If Yes,

   a. Is the hotline? _____ Computerized? _____ Via Telephone?

b. How does this hotline work? (Probes: Who is responsible for maintaining it? How do employees find out about it?)

5. **Other Reporting Mechanisms: Does your agency have mechanisms other than hotlines that employees and supervisors can use to report security concerns?**

   _____ Yes _____ No

   If Yes, how does this mechanism work? (Probes: Phone? Computer?)

   Probes: Is the mechanism anonymous? What assurances are given to those who report that their identity will be kept confidential or that they will not suffer reprisals?

   Do you keep records of the following?

   _____ Yes _____ No Frequency of use?
   _____ Yes _____ No Types of issues reported?
   _____ Yes _____ No Whether coworkers or supervisors reported information?
   _____ Yes _____ No If so, could we review data for the years 1999 and 2000?

   Describe the format for keeping records?

   Who should we contact to find out the format and to review the data?

   Name: _____

   Phone Number: _____

a. If you do not keep records, what are your general impressions as to the types of issues reported and by whom?

Section 3. Security Education

6. **Security education materials: Does your agency have brochures, briefing materials, and other products or programs to tell supervisors and coworkers about their reporting responsibilities and procedures?**

   _____ Yes _____ No

   a. If Yes, could we have copies of these materials?

   b. If No, what types of educational content or materials do you think would be helpful?

Section 4. Problems and Successes with Reporting

7. **Problems and successes: Please describe major problems or successes your agency has experienced concerning reporting by supervisors or coworkers.**

   a. Do these problems or successes differ concerning Employee Assistance Program (EAP) issues (e.g., drugs, alcohol, financial problems) and Counterintelligence-related issues (e.g., foreign influence, foreign contacts, security violations)?

   _____ Yes _____ No

   b. If Yes, how do they differ?

Section 5. Recommendations

8. **Recommendations: Do you have any recommendations for encouraging supervisors and coworkers to value and take action on reporting of security-related issues?**

   a. Do these recommendations differ concerning Employee Assistance Program (EAP) issues (e.g., drugs, alcohol, financial problems) and Counterintelligence-related issues (e.g., foreign influence, foreign contacts, security violations)?

   _____ Yes _____ No

   b. If Yes, how do they differ?

Section 6. Other Comments

Do you have additional comments about the areas we've covered or comments on other areas of relevance to reporting?

Section 7. Other Contacts

9. **Ask for Other Agency Contacts.** Are there others within your agency whom you would suggest that I contact? If so, who are these individuals? Would you be willing to contact them to let them know that I'll be calling them? If this is not possible, may I use your name as the referral source?

Contact No. 1 Name and Position Title: _____

Phone Number: _____ E-mail Address: _____

Contact No. 2 Name and Position Title: _____

Phone Number: _____ E-mail Address: _____

Section 6. Feedback on Interview Questions

10. Are there other issues that you would suggest we address in our agency interviews?

11. Are there questions that you would suggest we not ask that were included?

Appendix E

Ground Rules for Focus Groups

Ground Rules for Focus Groups

Purpose of the Focus Group Session

The purpose of the focus group is to discuss issues related to supervisor and coworker reporting of behaviors that may raise questions about a cleared colleague's willingness and ability to protect classified information. We are requesting focus group participants' assistance to help us better understand problems related to supervisor and coworker reporting and to discuss possible solutions.

Ground Rules for the Session

Prior to the session, we encourage participants to discuss the topic with their colleagues. Participants' contributions to the session will then reflect a combination of their own personal experience as well as what they have learned from others.

To encourage participants to speak candidly, the following steps will be taken:

- During the sessions, participants will be asked to refer to coworkers, supervisors, and managers in general and to avoid naming individuals in their comments.

- Differences of opinion are acceptable and to be expected. Participants will be encouraged to say what they think and allow others to do the same. We request that only one person talk at a time.

- After the focus group, participants may talk generally about what was discussed, but should never associate comments with the individuals who made them.

- Facilitators will not share any participants' comments with anyone within the agency, including security personnel.

- The facilitators will take notes as the discussion proceeds. To ensure that no comments can be attributed to specific people, these notes will not include participants' names.

  In the final report, comments made by this focus group will be merged with the comments of people at other installations. The names of the participants as well as the installations will be kept confidential.

Focus Group Facilitation

The focus group will be facilitated by researchers from the Defense Personnel Security Research Center (known as PERSEREC), a small research group in Monterey, CA. PERSEREC is part of the Defense Human Resources Activity (DHRA) with policy oversight provided by the Assistant Secretary of Defense for Command, Control, Communication and Intelligence (OASD [C3I]). In existence since 1986, PERSEREC conducts research on the topic of personnel security in the following program areas: Automated Systems for Personnel Security, Trust Betrayal, Vetting Systems, and Continuing Evaluation. The present study, Supervisor and Coworker Reporting, falls under the research area, Continuing Evaluation. Joanne Marshall-Mies and Suzanne Wood will be conducting the focus groups.

Appendix F

Focus Group Protocol

Focus Group Protocol

Good morning [afternoon]. My name is Joanne Marshall-Mies and this is Suzanne Wood. We are researchers from the Defense Personnel Security Research Center and we are interested in talking to you about supervisor and coworker reporting. We want to thank you very much for volunteering to help us. You probably have received a one-page sheet describing the project and what we'd like to accomplish today. If not, we'll give you a copy of this now.

This is an opportunity for you to tell us what goes on around here in connection with supervisor and coworker reporting, and to do it in a confidential environment. Nothing you say will go back to your security manager or anyone in this organization and we'll never associate comments with individuals. In fact, no one will ever know which *organizations* we visited. So things are totally anonymous. Although Suzanne will be taking notes as we go along, she will not associate names with those who made the comments.

Initial Question:

1. **Let's start with a general question. This question concerns the requirement in DoD Directive 5200.2-R that supervisors [coworkers] are encouraged or required to report certain kinds of behaviors by their cleared colleagues to Security or other authorities. Are you aware of this requirement? What does the requirement mean to you? How well does it work around here?**

   Probe a: Has anyone you know ever reported a subordinate or coworker? If so, for what reason? Do you know what happened as a result of their report?

   Probe b: Studies have found that people are often aware of a person with problems but that, for various reasons, they don't report the problem to security managers. Why would a person be reluctant to report [impediments]?

   Probe c: Which types of behaviors are most likely to be reported? Least likely?

Final Questions:

2. **Do you think the government should even try to get people to report? Why? Why not?**

3. **Do you have any recommendations concerning the reporting requirements or the way in which reporting works or is handled here in your agency?**

   Probe: Should employees [supervisors or coworkers] be required to report their colleagues [subordinates]? If yes, which types of behaviors should they be required to report? If no, why not?

4. **What could the government do to encourage people to report subordinates [coworkers] who may be a Security risk? Would it make a difference if the requirement were to emphasize reporting as not only a way protect national security, but also as a way to help colleagues get the professional help they may need?**

5. **Are there ways that the reporting requirements could be explained more succinctly so that the rules and boundaries are clear? How best can this be done?**