Enhancing Supervisor Reporting of Behaviors of Concern

Leissa C. Nelson
Defense Personnel and Security Research Center
Office of People Analytics

James G. Beneda
Shannen M. McGrath
Daniel G. Youpa
Northrop Grumman Technology Services

Enhancing Supervisor Reporting of Behaviors of Concerns

Leissa C. Nelson
Defense Personnel and Security Research Center, Office of People Analytics,

James G. Beneda, Shannen M. McGrath, Daniel G. Youpa
Northrop Grumman Technology Services

Released by – Eric L. Lang

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.			
1. REPORT DATE:	2. REPORT TYPE: Technical Report		3. DATES COVERED:
4. TITLE: Enhancing Supervisor Reporting of Behaviors of Concern	5a. CONTRACT NUMBER:		
	5b. GRANT NUMBER:		
	5c. PROGRAM ELEMENT NUMBER:		
6. AUTHOR(S): Leissa C. Nelson, James G. Beneda, Shannen M. McGrath, Daniel G. Youpa	5d. PROJECT NUMBER:		
	5e. TASK NUMBER:		
	5f. WORK UNIT NUMBER:		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES): Defense Personnel and Security Research Center Office of People Analytics 400 Gigling Road Seaside, CA 93955	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC:		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES):	10. SPONSORING/MONITOR'S ACRONYM(S):		
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):		
12. DISTRIBUTION/AVAILABILITY STATEMENT:			
13. SUPPLEMENTARY NOTES:			

ABSTRACT: DoD personnel who pose a threat or experience personal problems may show early warning signs but supervisors do not always recognize indicators or report their concerns through proper channels. A literature review and subject matter expert (SME) interviews collected information about barriers to reporting, strategies for overcoming these barriers, and tools to assist with the reporting process. This study also evaluated the utility and feasibility of using the United Kingdom Centre for Protection of National Infrastructure Employee Assessment Tools to supplement automated continuous evaluation and to provide supervisors an early intervention channel for at-risk employees. Literature review findings suggest that a comprehensive approach to prevention and mitigation of misconduct may increase the likelihood of reporting, and vice versa. Increased reporting may be achieved by providing a clear, easily used, and trusted reporting system, along with a positive organizational culture that makes felt responsibility to report stronger than the psychosocial impediments. SMEs interviewed for this study recommended clarifying reporting policy, providing additional scenario-based training, and improving relationships between supervisors and security managers. Some SMEs also emphasized the importance of holding personnel accountable for reporting security concerns. They suggested that accountability is currently inadequate, which may contribute to underreporting. The researchers concluded that the Employee Assessment Tools are not appropriate for the entire DoD cleared population, but are an excellent example of a reporting tool for individuals in high-risk positions.

14. SUBJECT TERMS:				
15. SECURITY CLASSIFICATION OF: Unclassified		16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 62	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT:	b. ABSTRACT:	c. THIS PAGE: FOUO			19b. TELEPHONE NUMBER (Include area code): 831-583-2846

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

The Office of the Under Secretary of Defense for Intelligence funded the Defense Personnel and Security Research Center, a division of the Office of People Analytics, to examine reporting obstacles and methods for increasing supervisor reporting of personnel issues, security concerns, and insider threats. Findings from this effort highlight the impediments to reporting and potential tools to assist with the reporting process. The authors offer strategies for addressing these impediments to help policy makers better understand reporting behavior and identify ways to enhance reporting. Enhanced reporting mechanisms will help supervisors proactively address concerning behavior by reporting their concerns to appropriate officials.

Eric L. Lang
Director, PERSEREC

EXECUTIVE SUMMARY

DoD personnel who pose a threat or experience personal problems may show early warning signs, but supervisors do not always recognize indicators or report their concerns through proper channels. Therefore, the Office of the Under Secretary of Defense for Intelligence requested that the Office of People Analytics' Defense Personnel and Security Research Center assess reporting obstacles and methods for increasing supervisor reporting of personnel issues, security concerns, and insider threats. This study collected information about barriers to reporting, strategies for overcoming these barriers, and tools to assist with the reporting process.

Researchers conducted this study in two parts. First, researchers identified known barriers to reporting in organizational settings as well as methods to increase felt responsibility and autonomous motivation to report. This analysis included a systematic review of academic literature as well as a subject matter expert (SME) data call and follow-up interviews. Next, researchers evaluated the utility and feasibility of using periodic assessment tools, specifically the United Kingdom Centre for Protection of National Infrastructure Employee Assessment Tools (EAT), to supplement DoD's automated continuous evaluation program.

REPORTING BARRIERS AND POTENTIAL SOLUTIONS

Research points to individual reporting behavior as the result of preexisting psychosocial factors and more immediate contextual factors such as organizational practices or culture. The commonalities revealed across these studies suggest that most organizations face the same fundamental problem of underreporting. This literature makes clear that an organization should expect that most people, most of the time, will not report misconduct they observe. However, the variation in reporting behavior demonstrated in these studies points to the fact that an organization's policies, practices, and culture directly influence its members' propensity to both commit misconduct and to report it when observed. These findings suggest that an approach to prevention and mitigation of misconduct that takes into account a range of factors may increase the likelihood of reporting, and vice versa. The best strategies for increasing reporting may consist of providing a clear, easily used, and trusted reporting system along with creating a positive organizational culture that makes felt responsibility to report stronger than the psychosocial barriers against it.

Interviews with a convenience sample of SMEs, all current or former DoD personnel security practitioners, provided understanding and insight into the issues surrounding supervisor reporting. SMEs interviewed for this study recommended clarifying reporting policy, providing additional scenario-based training, and improving relationships between supervisors and security managers. Some SMEs also emphasized the importance of holding personnel accountable for reporting security concerns. They suggested that accountability is currently inadequate and that this contributes to underreporting. Participants generally agreed that a reporting procedure such as the Personal Acknowledgment of Staff Security (PASS), developed by the

Defense Personnel and Security Research Center, could increase accountability for reporting and clarify policy as well as improve relationships between supervisors and security personnel (e.g., the procedure might include required follow-up interactions to address concerns).

EAT EVALUATION

This study concluded that EAT is not appropriate for the entire DoD cleared population, but it is an excellent example of a reporting tool for individuals in high-risk positions. The information it collects can provide many useful insights into factors that may increase an individual's vulnerability. However, despite its many promising features, EAT is unsuitable for large-scale use by DoD as an off-the-shelf solution. The United Kingdom Centre for Protection of National Infrastructure developed it for U.K.-based organizations, and the process and content reflect cultural and legal limitations specific to the U.K. Moreover, EAT was not designed for an organization as large and operationally diverse as DoD.

The researchers believe that, although EAT and other resource-intensive personnel security assessments are impractical for the entire DoD cleared population, an abbreviated version of these procedures could enhance supervisor reporting of concerns. For example, the PASS procedure would require supervisors to submit only one annual certification for their subordinates as a group. The research literature also suggests that initiating such a procedure would help implement Security Executive Agent Directive 3 and related programs by increasing felt responsibility and accountability for reporting personnel security concerns. An organization could use a more comprehensive assessment like EAT on a limited basis to substantiate reported concerns.

RECOMMENDATIONS AND NEXT STEPS

This research will continue with a second phase with the following objectives:
- Finalize a version of PASS that focuses on personnel security;
- Develop a version of PASS that emphasizes employee assistance;
- Conduct a pilot test of one or both versions, and gathering information from participants about the usefulness of the tool(s); and
- Identify the resources required to implement an effective reporting mechanism.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

DoD employs an enormous workforce, all of whom undergo background vetting prior to employment and many of whom undergo periodic reinvestigation. Despite this vetting, behaviors of concern still occur. In some cases, these behaviors may indicate that an individual needs help. In other cases, these behaviors result in harm to DoD personnel and resources. When incidents of harm have occurred, after-action reviews frequently identified warning signs that, if properly reported and addressed, might have prevented the incident (e.g., the Washington Navy Yard shooting). The purpose of this study was to examine reporting research across domains and develop recommendations for improving reporting of personnel security and related concerns.

The timely reporting of concerning behavior to appropriate personnel (e.g., security, human resources) can help avert incidents and conserve DoD resources (in particular, DoD investment in personnel) by providing assistance or other interventions to resolve behaviors of concern. Policy requirements make reporting behaviors of concern every employee's responsibility. Military and civilian supervisors are key players in recognizing and reporting concerns at an early stage so that intervention will have a reasonable chance of success. Unfortunately, many people are reluctant to act on this responsibility. In addition, despite the requirement to report, supervisors receive little guidance on reporting and lack an efficient means for making reports.

The Defense Personnel and Security Research Center (PERSEREC), a division within the Office of People Analytics, conducted this study to examine reporting obstacles and methods for increasing supervisor reporting of personnel issues, security concerns, and insider threats through a comprehensive literature review of academic and applied research. Researchers also considered the potential utility of existing periodic security assessment tools to supplement automated continuous evaluation procedures.

REPORTING POLICY

As noted, supervisors receive little guidance for handling concerning behavior; available guidance comes from the personnel security process and applies directly to cleared personnel. More recently, on-going monitoring requirements, including reporting, were expanded to cover non-cleared personnel to include individuals in positions of public trust. Executive Order (E.O.) 12968 (August 2, 1995, as amended) established the expectation for all cleared personnel "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." Subsequently, E.O. 13467 (June 30, 2008, as amended) added a continuous evaluation (CE) requirement for ongoing monitoring of all individuals with eligibility to access classified information or to hold a sensitive position. The ongoing monitoring requirement was extended under E.O. 13764 (January 17, 2017) to most of the Federal workforce, including those not covered by personnel security policy.

The Security Executive Agent is responsible for oversight of Federal personnel security policy, including development of uniform guidance and procedures for reporting behaviors of concern. Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position*, (June 12, 2017) delineates reportable activities. It also directs covered individuals (as defined in the policy) to inform agency heads or designees of reportable activities for self (e.g., foreign travel and foreign contacts) and others (e.g., unexplained affluence, alcohol abuse, misuse of U.S. Government property). SEAD 4, *National Security Adjudicative Guidelines,* (June 8, 2017) established common criteria for determining initial or continued eligibility for access to classified information or to hold a sensitive position. Those criteria include 13 Adjudicative Guidelines that define behaviors by which eligibility is determined (e.g., drug use, criminal conduct).

Although E.O.s and Security Executive Agent policies apply to the entire Federal Government, agencies establish their own implementation policy. Current DoD reporting requirements are covered in a number of policy issuances. The DoD Personnel Security Program (DoD Instruction 5200.02, March 21, 2014, as amended) prescribes CE requirements and requires timely reporting of significant behaviors of concern, unfavorable administrative actions, and adverse actions to the appropriate personnel security, human resources, and counterintelligence officials.

Procedural guidance for the Personnel Security Program is provided in DoD Manual 5200.02 (April 3, 2017), including the requirement to continuously assess cleared personnel to ensure that they remain trustworthy; responsibility is assigned to all DoD personnel for reporting behaviors of security concern. Reporting mandates are also included in DoD insider threat (DoD Directive 5205.16, September 30, 2014, as amended) and counterintelligence programs (DoDD 5240.06, May 17, 2011, as amended). These policies include mandatory training requirements to provide awareness of individual reporting responsibilities.

PERSEREC RESEARCH ON SUPERVISOR AND COWORKER REPORTING

The problem of underreporting, specifically of security concerns, by government employees has been the subject of PERSEREC research for many years. Studies of espionage and other insider threats have consistently demonstrated that observations of suspicious behavior often go unreported or unaddressed by authorities (Herbig, 2008). Furthermore, studies of source productivity in background investigations and clearance revocations have shown that people who know the subject (e.g., coworkers, supervisors, and neighbors) often provide less relevant information than public records or subjects' self-disclosed information (Kramer, Crawford, Heuer, & Hagen, 2001; Fischer & Morgan, 2002). PERSEREC research on the willingness of government employees to report security concerns confirms the general pattern of underreporting by coworkers and supervisors and suggests a variety of potential causes.

Bosshardt, Dubois, & Crawford (1991)

Bosshardt, DuBois, and Crawford (1991) found that unit commanders, supervisors, security managers, and coworkers are often reluctant to report potential security concerns. Reasons for underreporting included inadequate training, lack of anonymity, few consequences for failing to report, unstructured information gathering, lack of accountability, reluctance to report on friends, and negative impacts on mission due to access suspensions. Their recommendations for improving reporting included improved security education, protections for reporters against retaliation, formal reporting and continuous monitoring requirements, and clear consequences for noncompliance. In addition, they recommended use of employee assistance programs as early intervention to help at-risk individuals resolve personal problems before they escalate.

Sarbin (Unpublished Manuscript)

In an unpublished manuscript prepared in 2001, Sarbin synthesized a diverse body of literature from the 1920s to the early 2000s and applied the findings to DoD policy for reporting security-relevant behavior. He found that reporting directives are based on the inaccurate premise that any evidence of unreliable, untrustworthy, or disloyal behavior represents a character flaw that predisposes a person to engage in espionage. Empirical research has repeatedly indicated otherwise; Sarbin found that individuals might behave in a morally unacceptable way in one situation but be morally circumspect in others. Furthermore, mandatory reporting policies fail to account for the positive organizational value of loyalty to peers, cultural norms against "snitching," and the perception that national security concerns are only tenuously related to reportable behaviors. The author concluded that it is unreasonable to expect employees to inform on their coworkers without a clearly defined nexus between reporting mandates and legitimate threats to national security.

Wood & Marshal-Mies (2003)

In an empirical study of Federal employees, Wood and Marshall-Mies (2003) found that supervisor and coworker reporting behavior conformed to Sarbin's hypotheses. Most Federal employees supported reporting obvious security concerns (e.g., bankruptcy, criminal conduct), but behaviors less clearly linked to security were rarely reported (e.g., alcohol abuse or late payments). In addition to confirming the need to implement earlier PERSEREC recommendations (Bosshardt, DuBois & Crawford, 1991), the findings of this study supported policy changes to make the personnel security program more accessible and transparent to employees by developing a list of reportable behaviors that pose a palpable threat to national security. A follow-up study (Wood, Crawford & Lang, 2005) provided a validated list of these behaviors that DoD should include in its counterintelligence reporting requirements.

Youpa & Smith-Pritchard (2013)

Youpa and Smith-Pritchard (2013) developed a concept of operations for a simple procedure called the Personal Acknowledgment of Staff Security (PASS) as a possible

strategy to encourage reporting. The purpose of the proposed procedure was to increase supervisor awareness, felt responsibility, accountability, and reporting of behaviors related to foreign intelligence entity threats in accordance with DoD's Counterintelligence Awareness and Reporting policies (DoDD 5240.06, May 17, 2011, as amended). The defining feature of PASS is a signed certification by supervisors that they understand and intend to comply with reporting policy.

The PASS concept is based on research showing that increasing autonomous motivation and felt responsibility encourages positive workplace behavioral change (Dose & Klimonski, 1995; Gagne & Deci, 2005; Fuller, Marler, & Hester, 2006). Felt responsibility is fostered when accountability results in clear expectations, perceived control of the situation, and the perception that the desired behavior is important. The PASS procedure would increase autonomous motivation and felt responsibility by clearly conveying the importance of reporting, helping supervisors feel competent to know when to report, acknowledging possible resistance to reporting, and reinforcing collective feelings of concern and respect for employees. A signed certification would function as a commitment that a supervisor is making to uphold her/his reporting responsibilities. Research indicates signing such a certification results in a higher likelihood that the signer will act in accordance with the commitment (Shu, Gino, & Bazerman, 2011).

Scalora, Bulling, DeKraai, Hoffman, and Avila (2014)

More recently, PERSEREC partnered with the University of Nebraska to examine reporting of workplace violence concerns. Scalora, Bulling, DeKraai, Hoffman, and Avila (2014) surveyed U.S. Marine Corps uniformed and civilian employees to ask how they would handle a range of behaviors potentially related to workplace violence. The survey included examples of violence indicators, and most respondents indicated they would report the more obvious concerning behaviors. However, many said they would attempt to intervene personally prior to reporting. The reasons subjects provided for not reporting workplace violence largely matched findings from personnel security reporting research (e.g., concerns about how officials would handle the reports). Notably, the study found significant differences between civilian and military attitudes regarding reportable behaviors and appropriate responses.

SUPERVISOR REPORTING TOOLS

Current standards have stressed the importance of ongoing assessment of the Federal workforce to protect against threats to national security and public trust (E.O. 13764, January 17, 2017). PERSEREC's prior research consistently shows that coworkers and supervisors often observe early indicators of potential threats, but face significant barriers to reporting that prevent authorities from intervening in many of these situations. Existing reporting channels within DoD may not be easily accessible or understood by supervisors, and few tools are available to encourage supervisors to fulfill their reporting responsibilities while also holding them accountable. Similarly,

existing CE programs do not yet include the systematic collection of concerning behavior observed in the workplace.

A few organizations have attempted to develop tools and systems that allow supervisors to conduct regular assessments of their subordinates. They designed these tools and systems to facilitate early intervention. The tools often include checklists of behaviors that could make the organization vulnerable. Because of the additional resources needed to perform these types of assessments, they are usually limited to personnel in sensitive positions.

In this study, researchers evaluated a tool to incorporate supervisor reporting into DoD's continuous evaluation program. The research team considered an existing procedure for enhancing supervisor reporting of employee misconduct that has received attention from a number of U.S. Government agencies: the Employee Assurance Tools (EAT). Developed in the United Kingdom (U.K.) by the Centre for the Protection of National Infrastructure (CPNI), EAT supplements employee risk management with an easy-to-use software package. The basic EAT leads supervisors through an employee evaluation and generates a risk assessment. If needed, a trained practitioner completes the second, more detailed, EAT for a more in-depth assessment. Dedicated human resources and personnel security specialists review assessments and intervene where necessary to assist troubled employees and prevent potential harm to the organization. A detailed description of EAT functions and features is provided in Appendix A.

STUDY RATIONALE AND OBJECTIVES

This study gathered information about barriers to reporting, strategies for overcoming such barriers, and possible tools to assist with the reporting process. The study had the following objectives:

- Characterize known reporting obstacles and identify methods for increasing felt responsibility and motivation of supervisors[1] for reporting concerning behavior; and
- Evaluate the utility and feasibility of using the EAT to supplement automated continuous evaluation and to provide supervisors an early intervention channel for at-risk employees (i.e., employees demonstrating behaviors of concern).

Researchers designed this study to provide recommendations for addressing known reporting impediments through policy and procedural changes, to include potentially implementing a procedure such as EAT. The sponsor for this report is the Office of the Under Secretary of Defense for Intelligence (OUSD[I]), and primary audiences include OUSD(I) and other Executive Branch agencies with similar reporting requirements.

---

[1] The literature review examined reporting behavior in general to gain a broad understanding of important factors. However, the primary focus of this study was to improve supervisor reporting.

METHOD

This study was conducted in two parts. First, known barriers to reporting as well as methods to increase felt responsibility and autonomous motivation to report were identified. This analysis included both a systematic review of academic literature and a subject matter expert (SME) data call with follow-up interviews. Second, the utility and feasibility of using periodic assessment tools, specifically EAT, to supplement DoD's automated continuous evaluation program were evaluated. The SME data call and interviews also contributed to the evaluation of assessment tools.

REPORTING BARRIERS AND POTENTIAL SOLUTIONS

Researchers conducted a two-step evaluation of known barriers to reporting and the closely related problem of felt responsibility. First, commonly recognized patterns of reporting behavior were identified through a comprehensive review of academic and applied research literature. These findings informed the second step, a data call and SME interviews conducted to determine if research findings aligned with personnel security practices in various DoD components.

Review Strategy

Google Scholar was used as the primary search engine to identify articles, and references listed in these articles were reviewed to expand the search. Key terms gleaned from previous PERSEREC reports were used in the search for relevant articles (e.g., employee reporting, felt responsibility). Additionally, Defense Technical Information Center and PERSEREC's report libraries were searched for technical reports not publicly available. In total, 143 academic and applied research articles were reviewed (see Appendix B).

A modified form of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis statement, a framework designed to improve the reporting of both systematic reviews and meta-analyses (Moher, Liberati, Tetzlaff, & Altman, 2009), was followed to select relevant research. These procedures helped ensure a logical and orderly approach to source identification, selection, and assessment. Specifically, the Preferred Reporting Items for Systematic Reviews and Meta-Analysis statement was used to direct data element extraction (e.g., key factors) and inform the iterative source inclusion process. As themes relevant to employee reporting and misconduct were identified, the search was expanded to settle on a selection of studies covering a broad range of reportable behavior and organizational contexts.

Because these studies used a number of different units of analysis and a wide range of a priori theoretical assumptions, direct comparison was difficult. It was not possible to generalize about individual, organizational, or cultural factors by imposing a single theoretical framework. Instead, empirically demonstrated measures, recommendations, and precautions for developing a successful supervisor reporting system were identified. The full literature review, which highlights important topics related to

complex social and psychological factors that may affect an individual's decision to report potential misconduct, is provided in Appendix B, along with a complete list of all sources reviewed.

SME Data Call and Interviews

SME data calls and interviews were conducted to (a) obtain input on obstacles to reporting employee misconduct and other security concerns, (b) identify best practices for supervisor reporting, (c) obtain input on existing personnel security training related to reporting, and (d) determine the utility and feasibility of periodic assessment tools to augment CE programs.

Procedure

A data call message was developed with the following three questions:

- What obstacles to supervisor reporting of personnel security concerns have you encountered?
- To what extent do supervisors report concerns as required by policy and why might they choose not to report?
- Are you aware of any practices that encourage or have improved supervisor reporting?

OUSD(I) Security Policy and Oversight Division distributed the data call via e-mail to their component points of contact. Respondents were instructed to send data call input to PERSEREC. Responses were received from eight security management and personnel security policy offices. The responses were analyzed to determine themes and follow-up questions. All respondents were asked to participate in a follow-up interview.

An interview guide covering the following topics was prepared:
- Supervisor reporting in general (e.g., How do supervisors know what to report?);
- Reporting obstacles (e.g., What are supervisors' concerns about reporting?);
- Reporting best practices (e.g., Are you aware of any practices that encourage or have improved supervisor reporting?); and
- EAT and other periodic supervisor assessment tools (e.g., What do you think are the advantages and disadvantages of this [type of] tool?).

Literature review results also informed interview guide development. The interview guide is provided in Appendix C.

SME interview participants included data call respondents and their staff. In total, seven SMEs from seven agencies participated in the interview portion of this study. SMEs were personnel security specialists, security managers, and policy personnel. Interviews were conducted by telephone, with an interviewer and a note taker present

for each interview. Each interview lasted from 1 to 2 hours and included up to six SME participants. The interview notes were then analyzed to identify relevant themes.

EAT EVALUATION

EAT was evaluated to determine if its tools adequately address known impediments to supervisor reporting, and can be used in their present form for employee assessments within DoD to supplement automated continuous evaluation. Information from the literature review and the SME discussions informed the EAT evaluation.

Additionally, EAT was independently evaluated by a U.S. security and counterintelligence expert who was employed as a consultant for this study. The consultant has over 30 years of experience performing security-related functions, including management positions, for DoD and the intelligence community. His feedback informed the evaluation.

Procedure

CPNI staff involved in developing and administering EAT were contacted by phone to discuss the system. CPNI participants included five SMEs with expertise in behavioral science, personnel security, vetting, and insider threat. CPNI provided recent versions of the tools to PERSEREC researchers, as well as testimony regarding their validity with U.K. employee populations. The tools and other documents provided by CPNI included:

- Annual Security Appraisal - Part 1 - Subject (n.d.);
- Annual Security Appraisal - Part 2 - Line Manager (n.d.);
- Security Appraisal Form NSV006 (09/2016);
- CPNI Employee Assurance Tools, Summary Plan and Guidance for Organizations (2012);
- Employee-assurance-tools-briefing-sheet.pdf (n.d.);
- Employee Assurance Tools - Networked Version, Operating Notes for the Assessors Module (2015);
- Employee Assurance Tools - Networked Version, Operating Notes for the Practitioners Module (2015); and
- EAT Example Reports (5).

These materials and CPNI discussion notes were used to describe the EAT process and training requirements. The security expert consultant provided an independent review of the same materials. A formal program evaluation framework (Milstein & Wetterhall, 1999) was used to examine EAT's utility and feasibility, including ways in which the tools mitigate known reporting impediments, as well as possible enhancements for use within the DoD environment.

RESULTS

The results for both the literature review and EAT evaluation are relatively extensive. For the sake of brevity, this section includes only a summary of these results. Appendices A and B contain more detailed information about each.

REPORTING BARRIERS AND POTENTIAL SOLUTIONS

This review defined reporting behavior as the individual decision to report or not report adverse information (e.g., misconduct) to an appropriate authority. Because there is little research that specifically addresses personnel security reporting, the review included academic and applied research from multiple domains, such as studies of "whistleblowing"[2] in public and private organizations, workplace safety incidents, and antecedents of school violence. These works also cover a broad range of reportable behavior, including actual or threatened law violations, unethical conduct or counterproductive work behavior, and simply reporting "bad news" to others. The researchers use the term "misconduct" to describe this broad range of reportable information.

Individual's Decision to Report Misconduct

Research into personal characteristics of the reporter has shown mixed results. The dominant position in the literature is that there are few personal characteristics that affect reporting behavior. Instead, most research views reporting behavior as the result of rational decision-making based on a cost-benefit calculation. For example, position in an organizational hierarchy plays a role in establishing an individual's sense of obligation to the organization, peers, and subordinates, which may influence likelihood of reporting. Other factors in these calculations include the seriousness of the observed misconduct, strength of available evidence, the observer's relationship to the wrongdoer, and potential consequences of the decision to report.

Organizational Influence on Reporting

There is a robust consensus in the literature that collective factors that make up the organizational setting heavily influence both misconduct and reporting. Various elements of an organization's culture may directly influence the likelihood of misconduct and the likelihood of reporting. Such factors include the ethical climate in which misconduct occurs as well as perceptions of the organization and its leaders as trustworthy. The broader professional culture organizations operate within may influence the organization and result in development of unique cultural barriers that put reporting at odds with other professional priorities. For example, members of many police organizations may adhere to a "blue code" that emphasizes group loyalty over responsibility to report misconduct; military organizations may share similar informal

---

[2] For some audiences, "whistleblowing" may have negative connotations suggesting potential insider threats. However, in the studies cited, it generally refers to positive, "prosocial" disclosure of "illegal, immoral or illegitimate practices" through channels within an organization (Dozier & Micelli, 1985).

norms against reporting. Just as important, however, are an organization's formal policies and practices, including effective reporting channels, protections against retaliation, and education programs that define misconduct and explain reporting mechanisms. Studies show that a well-implemented reporting and compliance program, aligned with a strong ethical culture, will both increase reporting likelihood and decrease the occurrence of misconduct.

Underlying Reasons for Nonreporting

Organizational influences clearly affect reporting behavior, but organizational efforts to improve reporting may have limits. Research consistently demonstrates the more fundamental problem that the norm is to not report, regardless of organization or type of misconduct. Two lines of research offer complementary explanations for the seeming universality of this phenomenon. First, socialization research has demonstrated that attitudes and behaviors related to reporting develop from early life experiences. Studies of "tattling" or "snitching" behavior among children indicate that norms against reporting become stronger as children age, and the formation of this behavior reflects children's relationships with adult authority figures, peer group dynamics, and broader cultural influences that define reportable misconduct and acceptable attitudes toward authority. Second, studies of "silence and voice" behaviors have focused on the more fundamental question of why individuals choose to speak up or remain silent in socially challenging circumstances. These studies suggest that nonreporting may be the result of a general reluctance to report bad news to authorities or, on a more personal level, anxiety about a potentially uncomfortable social interaction.

Felt Responsibility

Research indicates that one of the most effective ways to encourage behavioral change in the workplace is through increasing felt responsibility, that is, the individual's belief she or he has an obligation to guide positive change. Organizations can foster felt responsibility by creating accountability measures that result in clear behavioral expectations, the individual's perceived control of the situation, and the shared perception that the desired behavior is important. Research shows that a sense of responsibility toward an organization or coworkers is closely related to an individual's likelihood of exhibiting prosocial helping behavior, including reporting of misconduct.

An individual's formal acknowledgment of personal responsibility can lead to an active commitment to comply with regulations and expectations. This may result in more reporting because people want to be consistent in their values and actions and appear consistent to others. Personal consistency is valued within society and simplifies daily life by reducing information-processing requirements in recurring situations. Additionally, making a voluntary, active decision to do something may result in more commitment than making the same choice by doing nothing. Reading and signing something like an honor code can increase moral saliency and thereby reduce moral disengagement and unethical behavior. In contrast to persuasive appeals through

information campaigns, this kind of procedure may promote enduring attitude and behavior change as it involves the compelling influence of cognitive dissonance.[3]

SME Data Call and Interviews

Interviews with a convenience sample of SMEs, all current or former DoD personnel security practitioners, provided understanding and insight into the issues surrounding supervisor reporting in the participating DoD organizations. Topics addressed included personnel security policy and training, barriers to reporting, and recommendations to encourage reporting. Information provided by SMEs was consistent with literature review results and with previous PERSEREC research.

Security Policy and Training

All SMEs indicated that DoD has generally implemented required security awareness and training programs effectively. These programs include a combination of annual security trainings, briefings, forums, newsletters, and campaigns that highlight topics relevant to supervisor reporting (e.g., Operations Security, Personnel Security, Insider Threat, and CE).

A prominent theme throughout all interviews was that reporting policies and training requirements are sufficient, but deficiencies in implementation exist. For example, components may not present policy and training requirements consistently. Additionally, policy guidance often is unclear. For example, thresholds for determining when a behavior is reportable may be too ambiguous. Likewise, policies should more clearly define reportable behavior and reporting criteria to facilitate compliance with reporting policy.

Barriers to Reporting

The barriers to reporting most frequently cited by SMEs fall into three categories: (a) lack of understanding reporting procedures, (b) distrust of reporting processes and outcomes, and (c) military cultural norms related to unit loyalty and leader accountability. SMEs indicated that supervisors often are unfamiliar with security procedures and often lack training that focuses specifically on their personnel security responsibilities. Because personnel appointed as acting supervisors have up to 1 year to complete security training, some may not be sufficiently familiar with reporting requirements, even though this is an important aspect of their duties. More importantly, reporting policies are frequently misinterpreted or misunderstood despite regular security training. In many cases, supervisors may not recognize the nexus between reportable behavior and national security concerns.

---

[3] Cognitive dissonance is a state of psychological tension that occurs when attitudes are in conflict with behavior (Festinger, 1957). People are motivated to reduce dissonance and reestablish consistency as soon as they experience this type of unpleasant drive state. Dissonance-induced attitude and behavior change is effective because it involves an individual's self-concept.

Distrust of reporting policies and procedures appears linked to a persistent belief that reporting derogatory information will result in negative outcomes. For example, reporting to security managers may result in clearance revocation or suspension and potential loss of employment for the subject. Personnel often view reporting as a disciplinary process, and inexperienced supervisors may fail to recognize reporting as early intervention to assist troubled employees. They also may not realize that personnel security policy allows for mitigation of adverse information. In addition, some individuals may refrain from reporting because they are fearful of retaliation. Supervisors also may avoid reporting due to the potential impact an employee suspension or termination would have on their own workload and mission. SMEs also suggested that the emphasis on "incident" reporting in policy, training, and procedures creates a stigma around reporting.

Finally, military cultural norms that conflict with reporting requirements may exacerbate barriers. Unit loyalties and interpersonal trust form the basis of military culture, and those loyalties and trust could be jeopardized if personal information is shared externally. Long-held expectations that military leaders are personally accountable for the actions of their subordinates may create another barrier to reporting. In addition, commanders have historically had broad disciplinary discretion within their units, including the authority to decide some personnel security issues. Although current policies require reporting of all established security concerns to security managers, commanders too often "locally adjudicate" security issues themselves. Commanders are, indeed, best placed to intervene to support troubled subordinates; however, their failure to submit reports to security managers prevents long-term, systematic evaluation of potential threats. Furthermore, lack of coordination between commanders and security managers creates gaps in information available to DoD Consolidated Adjudications Facility adjudicators.

Recommendations to Encourage Reporting

SMEs provided recommendations to encourage supervisor reporting by improving policy, training, and relationships between supervisors and security managers. They discussed the need for clear guidance and training that is more consistent across components. Most suggestions related to how and when specific security concerns should be reported. Some SMEs recommended training that focuses on reportable information with relatively ambiguous connections to national security (e.g., personal financial difficulties, marital problems) as well as additional use of training scenarios to clarify what is covered by personnel security reporting requirements.

SMEs also commented that personnel security policy and training suffer from an overreliance on punitive language. For example, terms like "incident" and "insider threat" have negative connotations, and link reporting with punishment. These labels focus attention on reporting major incidents, while ignoring less recognizably harmful behavior. Negative labels also may create confusion for supervisors that undermines reporting as a positive early intervention to help troubled subordinates. Negative labels create a sense of antagonism between subordinates and supervisors, who may be able

to connect their employees with available resources. Negative labels may also make supervisors reluctant to report information that might reflect poorly on their own performance.

There was general agreement among SMEs that personnel security policy must better distinguish between immediate security threats, troubling behaviors that merit early intervention, and information necessary for continuous evaluation. One SME suggested modifying DoD's current personnel security incident reporting system by creating data entry options based on these distinctions and eliminating incident flags in most cases. By distinguishing the information, incident reporting could serve as a tool for continuous evaluation. Suggested modifications were as simple as having an option to change or update any low-threshold information previously provided (e.g., recent traffic ticket over $300.00) to serve as a real-time update to an individual's file.

Most SMEs expressed the need for greater transparency in personnel security reporting. Supervisors and employees at all levels need assurance that reporting does not automatically result in clearance revocation or employment termination. There must be a clear understanding that security managers have a stake in helping individuals maintain their access eligibility. Security managers should make it clear that they are approachable and available to guide and assist supervisors in performing their personnel security responsibilities. Supervisors and commanders must rely on security managers as advisors, rather than antagonists, when addressing personnel security concerns.

EAT EVALUATION

EAT's content and processes were evaluated through analysis of training materials provided by CPNI. The evaluation addressed EAT's design and function, background assumptions related to its development, and organizational considerations and training requirements for its implementation. Findings are presented in two sections, with additional detail in Appendix A. The first section provides a brief description of the tools. The second evaluates how EAT or similar procedures might mitigate known reporting barriers and enhance an organization's personnel security. It also identifies potential challenges to developing a supervisor reporting tool that effectively and efficiently captures actionable security concerns among employees.

Brief Description

The EAT system was intended to enhance asset protection and foster appropriate management support for employees in sensitive positions. CPNI designed it to improve an organization's ability to identify personnel requiring additional management support or attention, as well as to detect issues and enable intervention before misconduct becomes a serious threat. EAT is based on employee disaffection and insider activity research, and CPNI states that the tools have been thoroughly tested and validated.

EAT comprises two automated questionnaires: basic and detailed. Managers complete the basic questionnaire for initial screening. It contains 17 items and takes about 10 minutes to complete for each employee. Dedicated practitioners (human resources or security professionals) outside the employee's chain of command who oversee the process complete the more detailed follow-up questionnaire. The 62-item detailed questionnaire involves collecting additional information and takes approximately 30 minutes to complete. It addresses concerns identified through the basic tool and other developed sources. EAT automatically scores responses and compiles a report that includes guidance for addressing any identified concerns.

Mitigating Barriers to Detecting and Reporting Insider Threats

The EAT process appears to address several common behavioral and organizational barriers to reporting that have been identified in social science and security research (see Appendix B). For example, because EAT reporting emphasizes specific, observable workplace behaviors, the problem of recognizing the nexus between reporting requirements and security concerns is minimized. EAT's confidence-level ratings are intended to address concerns about strength of available evidence. Furthermore, it allows documentation of information that may only be hearsay and removes the supervisor's burden of having to decide if the information poses a genuine threat or of having to take direct action without sufficient evidence. EAT places that responsibility with trained security professionals outside the employee's chain of command who have the resources and expertise to further investigate and make an objective determination.

Use of EAT may also enhance role-based expectations of supervisor reporting responsibility by providing a clearly defined reporting channel that must be used regularly for evaluating covered employees. Supervisors' felt responsibility may improve because the system is not simply a disciplinary tool; rather, it is a way for organizations to help troubled employees before workplace behavior becomes high risk. This proactive use of the system may also help reduce negative attitudes about reporting related to cultural norms against informing on peers.

To be most effective, employees must view a program like EAT as a means to improve the workplace through organization and employee shared responsibility. The system must balance reducing organizational risk with positive early intervention to assist at-risk employees. The EAT process may contribute to increased levels of felt responsibility, which is fostered when accountability results in clear expectations, perceived control of the situation, and the perception that reporting is important. Because EAT requires supervisors to include potentially derogatory information in some cases, an effort must be made to establish trust in the assessment process. Important factors for establishing trust include communicating the assessment's effectiveness and reliability, appropriate organization response to the information provided, policies to ensure that accurate reporting will have no repercussions on the reporter's position in the organization, and assurances that reporting low-risk or low-confidence information will not unnecessarily undermine supervisors' relationships with employees.

DISCUSSION

The work described in this report reflects PERSEREC's ongoing interest in understanding factors that influence reporting behaviors of concern and efforts to establish an effective reporting process. This work can make an important contribution to DoD's efforts to better protect its workforce and national security, respond to insider threats, and implement prevention, assistance, and response capabilities at the installation level. As discussed in the introduction, personnel security, insider threat, and workplace violence incidents are often preceded by behaviors of concern that are not reported or, if reported, not handled effectively. The literature review provided insights into explanations for these deficiencies, and the evaluation of reporting tools contributed ideas for tool and process development.

CONCLUSIONS FROM THE RESEARCH LITERATURE

Literature review findings reflected four primary themes. The first theme focused on the individual decision to report. Although some studies have tried to identify personal characteristics that make reporting more or less likely, most see reporters as rational actors who must carefully weigh the costs and benefits of their decision. The second theme represented organizational factors that mediate patterns of both misconduct and reporting behavior. Such factors include formal organizational policies, informal norms and practices rooted in organizational culture, and broader professional influences that go beyond any single organization. The third theme considered broader psychosocial patterns of nonreporting. These include deeply socialized norms against reporting instilled in early childhood, as well as psychological and social barriers to communicating adverse information that may transcend an organizational context. Finally, studies of felt responsibility demonstrate that factors influencing an individual's sense of responsibility toward an organization and coworkers will also influence the likelihood of prosocial behavior (e.g., reporting or intervening to assist an at-risk employee).

Taken together, the research literature points to individual reporting behavior as the result of preexisting psychosocial factors and more immediate contextual factors such as organizational practices and culture. The commonalities revealed across these studies suggest that most organizations face the same fundamental problem of underreporting. This literature makes clear that an organization should expect that most people, most of the time, will not report misconduct they observe. However, the variation in reporting behavior demonstrated in these studies points to the fact that an organization's policies, practices, and culture directly influence its members' propensity to both commit misconduct and to report it when observed. These findings suggest that a comprehensive approach to misconduct, focused on prevention and early intervention through assistance to at-risk members, may also increase the likelihood of reporting. It may be that the best strategies to increase reporting consist of providing a clear, easily used, and trusted reporting system, and by fostering a

positive organizational culture that makes felt responsibility to report stronger than the psychosocial barriers against it.

EAT EVALUATION

EAT is an excellent example of a reporting tool for individuals in high-risk positions. The information it collects may provide useful insights into factors that increase an individual's vulnerability to adversaries and counterproductive workplace behavior. However, despite its many promising features, EAT is not appropriate for large-scale use by DoD as an off-the-shelf solution. It was developed to address problematic insider behavior in U.K.-based organizations, and its process and content reflect cultural and legal limitations specific to the U.K. (e.g., linguistic and privacy concerns).

EAT was also not designed for an organization as large and operationally diverse as DoD. Ultimately, EAT is tailored to a single group of reporters and organizational relationships (i.e., supervisors of employees in high-risk, sensitive positions), which makes it impractical for large-scale DoD implementation. While the basic tool may only take 10 minutes to complete per employee, any concerns require a follow-up assessment. Not only does the follow-up assessment take much longer to complete, a trained practitioner must be available. Meeting these requirements is not practical given the size of the DoD population. However, a tool like EAT could be effective for assessing personnel in the most sensitive positions.

Effective implementation of EAT requires support from dedicated practitioners. Dedicated security or human resources experts outside the employee's chain of command are necessary to evaluate and respond to reports; this is a critical element that differentiates EAT from other reporting processes. Effective implementation requires clear definition of the dedicated practitioner role and adequate resources. The advantage of dedicated practitioners is the ready availability of trained personnel who can address immediate threats and early intervention needs.

EAT offers the benefit of automated risk scoring, which introduces a level of objectivity into an otherwise highly subjective process. Review of all reports by trained dedicated practitioners removes the burden from first-line supervisors to directly address risky behavior and provides the organization with a clearer picture of its overall security. Over time, regular and consistent use of EAT may have a positive impact on organizational culture and ethical climate by instilling positive attitudes toward reporting, and the expectation of regular monitoring may help reduce employee misconduct.

These features make EAT an encouraging concept to improve reporting of what CPNI calls "counter-productive work behaviors," and to provide appropriate follow-up with trained practitioners. Most importantly, the tools provide a channel for supervisors to identify and help employees before they become disaffected and cause harm to themselves, others, and the organization. Additionally, such a system could provide security managers a mechanism for evaluating security practices across an

organization in order to address more systemic threats. While EAT is not appropriate for large-scale use by DoD, it provides an excellent point of comparison for assessing how an automated supervisor reporting and risk management tool might be developed for use in the DoD environment.

CONSIDERATIONS FOR DEVELOPING A DOD REPORTING TOOL

Given the wide range of factors that mediate reporting behavior, the research literature strongly supports the conclusion that a well-designed reporting system, as part of a broader strategy to create a more positive organizational culture, may reduce organizational risk and help mitigate threats posed by insiders. SMEs interviewed for this study recommended clarifying reporting policy, providing additional scenario-based training, and improving relationships between supervisors and security managers. Some SMEs also emphasized the importance of holding personnel accountable for reporting security concerns. They suggested that accountability is currently inadequate and that this contributes to underreporting. The majority of participants agreed that a reporting procedure such as PASS (Youpa & Smith-Pritchard, 2013) would increase accountability for reporting and could clarify policy as well as improve relationships between supervisors and security personnel (e.g., the procedure could include required follow-up interactions to address concerns; see Appendix D for more information).

The researchers believe that, although EAT and other resource-intensive personnel security assessments are impractical for the entire DoD cleared population, an abbreviated version of these procedures could enhance supervisor reporting of concerns. For example, the PASS procedure would require supervisors to submit only a single annual certification for their subordinates as a group (i.e., instead of for every individual subordinate). The research literature also suggests that such a tool would help implement SEAD 3 and related programs by increasing felt responsibility and accountability for reporting personnel security concerns. The procedure would require DoD military and civilian supervisors to acknowledge familiarity with the reporting requirements in DoDM 5200.02, as well as their intent to report behaviors that cause a concern. The procedure could include additional information about reporting requirements as well as ways to support personnel in need of assistance. Based on the strengths and weaknesses of the approaches considered (e.g., making PASS part of annual performance appraisals), the researchers recommend linking PASS with annual security refresher training. The PASS approach also has the benefit of reinforcing training through immediate application to supervisory duties. Additionally, DoD could use a more comprehensive assessment like EAT on a limited basis to substantiate reported concerns.

Based on the review of the EAT process, an important part of developing a DoD supervisor reporting procedure would be identification of relevant legal and privacy issues. These concerns would require coordination between key stakeholders, including intelligence, personnel, and insider threat policy makers, each of whom may

have different mission priorities and legal limitations. Legal staff would have to provide guidance in addressing employee grievances, especially if a manager acted arbitrarily and capriciously in the tool's application. In addition, policy makers would need to address several practical concerns prior to implementation, such as determining how information is collected, stored, used, and retained. Successful implementation might begin by using the tool to assess personnel in high-risk positions and individuals with a documented history of security concerns. This aligns with the DoD model of focusing CE on individuals in high-risk assignments.

POTENTIAL UTILITY OF PASS

The PASS procedure would address the main principles of increasing autonomous motivation and felt responsibility by clearly conveying the importance of reporting, helping supervisors feel competent to know when to report, acknowledging possible resistance to the behavior, and reinforcing collective feelings of concern and respect for employees. Manipulating perceived accountability may affect people differently; however, the procedure could result in more felt responsibility overall and potentially lead to increased reporting of concerns.

Standard security training and awareness programs for DoD employees are usually information-based persuasive campaigns to help recognize and appropriately address potential concerns. However, the effectiveness of these campaigns is unclear. Typically, DoD employees are relatively passive recipients of information even when follow-up questions are part of the training. This is especially true with respect to intent to comply with reporting policy. The proposed PASS procedure would require supervisors to actively acknowledge their understanding and intent to comply with reporting requirements by signing a certification. A signed certification would function as the supervisor's commitment to uphold their responsibilities for reporting and, based on research reviewed, would indicate a higher likelihood to act.

Several SMEs who have reviewed the proposed PASS tool and procedure expressed interest in the accountability that PASS would create and believed the procedure would encourage supervisors to report more security concerns. Additionally, there is value in PASS as a means of documenting acknowledgment of individual supervisor reporting responsibilities. Some SMEs expect that this accountability will increase rates of reporting by reinforcing reporting expectations, eliminating ignorance as an excuse for underreporting, and by creating a clear expectation for the consequences of not reporting. In addition, if the supervisor signs a certificate in association with annual security training, PASS would provide a channel for supervisors to connect with security managers while they are thinking about reporting obligations and reportable behavior.

SME feedback suggests that supervisor accountability is currently weak in personnel security policy and practice, and there is near consensus that PASS may help address this need. However, stakeholders should address a few potential concerns prior to implementation. Human resources policy differs for military, civilian, and contractor

employees, and the PASS procedure might need to be customized for each population. In addition, implementation that focuses too heavily on accountability could perpetuate negative beliefs about personnel security reporting. It also would be important to demonstrate that PASS actually increases supervisor reporting as opposed to unnecessary paperwork.

RECOMMENDATIONS AND NEXT STEPS

This research will continue with a second phase with the following objectives:

- Finalize a version of PASS that focuses on personnel security;
- Develop a version of PASS that emphasizes employee assistance;
- Conduct a pilot test of one or both versions, and gathering information from participants about the usefulness of the tool(s); and
- Identify the resources required to implement an effective reporting mechanism.

REFERENCES

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). *Continuing assessment of cleared personnel in the military services: Report 1--A conceptual analysis and literature review* (TR 91-01). Monterey, CA: Defense Personnel Security Research and Education Center.

Department of Defense. (2011, May 17). *Counterintelligence awareness and reporting (CIAR)* (DoD Directive 5240.06). Washington, DC: Author.

Department of Defense. (2014, March 21). *DoD personnel security program (PSP)* (DoD Instruction 5200.02). Washington, DC: Author.

Department of Defense. (2014, September 30). *The DoD insider threat program* (DoD Directive 5205.16). Washington, DC: Author.

Department of Defense. (2017, April 3). *Procedures for the DoD personnel security program (PSP)* (DoD Manual 5200.02). Washington, DC: Author.

Dose, J., & Klimoski, R. (1995). Doing the right thing in the workplace: Responsibility in the face of accountability. *Employee Responsibilities and Rights Journal, 8*(1), 35-56.

Dozier, J.B., & Micelli, M.P. (1985). Potential predictors of whistle-blowing: A prosocial behavior perspective. *Academy of Management Review, 10*(4), 823-36.

Exec. Order No. 12968, 3 C.F.R. 40245 (1995).

Exec. Order No. 13467, 3 C.F.R. 38101 (2008).

Exec. Order No. 13764, 3 C.F.R. 8115 (2017).

Festinger, L. (1957). *A Theory of Cognitive Dissonance.* Stanford: Stanford University Press.

Fischer, L.F., & Morgan, R.W. (2002). *Sources of information and issues leading to clearance revocations* (TR 02-01). Monterey, CA: Defense Personnel Security Research Center. DTIC: ADA411037

Fuller, J. B., Marler, L. E., & Hester, K. (2006). Promoting felt responsibility for constructive change and proactive behavior: Exploring aspects of an elaborated model of work design. *Journal of Organizational Behavior, 27*, 1089-1120.

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior, 26*, 331-362.

Herbig, K.L. (2008). *Changes in espionage by Americans: 1947-2007* (TR 08-05). Monterey, CA: Defense Personnel Security Research Center.

Kramer, L.A., Crawford, K.S., Heuer, Jr., R.J., & Hagen, R.R. (2001). *SSBI-PR source yield: An examination of sources contacted during the SSBI-PR* (TR 01-05). Monterey, CA: Defense Personnel Security Research Center. DTIC: ADA403829

Milstein, B., & Wetterhall, S. F. (1999). Framework for program evaluation in public health. *Morbidity and Mortality Weekly Report, 48*(RR-11).

Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009). *Preferred Reporting Items for Systematic Reviews and Meta-Analyses:* The PRISMA Statement. PLoS Med 6(7): e1000097. doi:10.1371/journal.pmed1000097

Office of the Director of National Intelligence. (2017, June 8). Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*. Washington, DC: Author.

Office of the Director of National Intelligence. (2017, June 12). Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position*. Washington, DC: Author.

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

Scalora, M., Bulling, D., DeKraai, M., Hoffman, S. & Avila A. (2014). *Barriers to reporting threatening behaviors in a military context*. Lincoln, NE: University of Nebraska Public Policy Center.

Shu, L. L., Gino, F., & Bazerman, M. H. (2011). Dishonest deed, clear conscience: When cheating leads to moral disengagement and motivated forgetting. *Personality and Social Psychology Bulletin, 37*(3), 330-349.

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

Wood, S., Crawford, K. S., & Lang, E. L. (2005). *Reporting of counterintelligence and security indicators by supervisors and coworkers* (Tech. Rep. 05-6). Monterey, CA: Defense Personnel Security Research Center.

Youpa, D.G. & Smith-Pritchard, S.A. (2013). *Development of a procedure to increase awareness and reporting of counterintelligence and terrorism indicators: Personal Acknowledgment of Staff Security (PASS)* (TR 13-02). Monterey, CA: Defense Personnel Security Research Center. DTIC: ADA624588

APPENDIX A: EMPLOYEE ASSURANCE TOOLS (EAT) EVALUATION SUPPLEMENT

SCOPE AND PURPOSE

The development of EAT was based on the Centre for the Protection of National Infrastructure's (CPNI) extensive research into known insider threats. In addition to identifying characteristics of individual wrongdoers, this research found a number of organizational factors associated with insider threat activity, including:

- Poor management practices that permitted observed misconduct to go unresolved;

- Poor security culture, including general failure to follow security policies and management ambivalence to security practices and violations;

- Inadequate role-based risk assessment and failure to identify employee suitability concerns that lead to vulnerability to exploitation or compromise;

- Poor communication and failure to share information across organizational units, resulting in delays to mitigating known employee misconduct; and

- Lack of awareness among senior leaders of potential risks, resulting in security policy gaps, lack of accountability, and inadequate resources to quickly mitigate threats.

The EAT process was designed to address each of these organizational factors as part of a broader security strategy. By identifying potential threats among employees, EAT provides an opportunity for the organization to identify and evaluate personnel security policies and practices before risks are exploited and significant damage is done.

Critically, EAT is intended to provide managers a mechanism to identify subordinates who may require additional management attention, support, or assistance in order to respond proactively to behaviors of concern. Research shows that insider threats may display behavioral indicators that can be acted upon before causing significant damage to the organization. Additionally, CPNI's research shows that early intervention in such situations promotes quicker resolution for the employee and organization and can prevent minor problems from escalating to major security concerns. As a prevention tool, EAT should be coupled with policies and resources to support at-risk employees and should not be used simply for investigatory or disciplinary purposes.

When properly implemented, the EAT process becomes a management practice to monitor behaviors of concern and provides supervisors the means to regularly evaluate employee risk. Regular use of EAT and employee awareness of increased monitoring could contribute to a more positive security culture. Review of all Basic assessments by dedicated practitioners is intended to provide formal accountability for reporting as well as establish a clear channel to communicate potential risks to senior leaders.

BACKGROUND AND ASSUMPTIONS

According to CPNI, EAT was developed based on research into indicators of employee disaffection and insider activity. EAT has been thoroughly tested and validated (CPNI, personal communication, November 9, 2017). Face validity was established based on feedback from assessors during initial trials. Content validity was based on a comprehensive literature review and a card-sorting exercise to identify the tools' dimensions. Items were written to ensure proper coverage of the domain. CPNI was able to establish partial construct validity (proper coverage of all facets of interest) using factor analysis. Factor solutions were cross-validated on two additional data sets and the tools' generalizability was demonstrated by finding the same factor structure as a U.S. survey. Concurrent criterion validity was based on assessments made at the same time against baseline data and employees of concern. In addition, the initial study on the validation of the tools was based on a CPNI database of insider cases for which they had case files. There were only a small number of cases in the initial study; however, over time, a data set of approximately 120 cases was assembled and compared with the initial study results to estimate post-predictive criterion validity.

CPNI documentation explains that the effectiveness of EAT depends on the accuracy of information provided by the assessor. EAT should be implemented as part of an organization's broader personnel security monitoring program for staff in high-risk, sensitive positions. EAT evaluates employee welfare and possible disaffection to protect against specific risks and is used independent of employee performance appraisals. It is a resource to help identify the risk an employee poses to the organization, although it is not designed to predict specific types of counterproductive work behavior. Policies governing EAT use should clearly define circumstances under which it may be used, the frequency and duration of the assessment, and how the policy will be maintained and reviewed. Use of EAT should be based on clear ethical guidelines for both the organization and individual users. The guidelines provided by CPNI for EAT use are based on: Code of Ethics and Conduct of the British Psychological Society (August 2009), International Guidelines for Test Use (2000), and Code of Good Practice for Psychological Testing (2007).

STAKEHOLDERS

EAT was designed based on assumptions that specific stakeholder groups have a role in successful implementation and that each group has unique concerns. However, stakeholder contexts will vary based on the internal and external environments of an implementing organization. Identifying the full range of active stakeholder groups and addressing stakeholder concerns should be an ongoing part of using the tools. Table 1 lists the stakeholders and concerns identified by CPNI for implementation of EAT among their core customers.

Table 1
EAT Stakeholders and Concerns Identified by CPNI

Stakeholder	Concerns
Organizational Leadership	• Return on investment • Reputation • Data protection • Employee engagement
Human Resources & Security Professionals	• How to implement & govern • How to investigate & escalate
Immediate Supervisors	• How to deal with resistance • How to escalate
Employees	• Invasion of privacy • Fairness of the tools/ potential for misuse • Impact on performance appraisal
Employee Unions	• Protect members' interests
Employee Representative Bodies	• Invasion of privacy • Fairness of EAT & potential for misuse • Protect staff

PRE-IMPLEMENTATION PROCESSES AND TRAINING

CPNI recommends that organizations take the following steps prior to implementing EAT.

1. Conduct an assessment of EAT's suitability for use within the organization. The assessment should identify the specific risk that EAT is intended to address, evaluate the potential for EAT to address this risk as well as the extent to which EAT use is justified by the risk.
2. Assess the potential impact EAT may have on organizational processes, policies, and technology; employee engagement and performance management; compliance with applicable laws; and organizational culture.
3. Implement a framework of policies and training to ensure that using EAT is compliant with relevant laws, appropriate to the organization's intent, and is secure.
4. Implement procedures to monitor and evaluate program effectiveness.

The aims and objectives of EAT should be communicated to relevant stakeholders to enlist their support and ensure organizational readiness. There should be training and support programs to ensure that users have the necessary skills, knowledge, and support for effective use of EAT. Users must be trained in program functions, policies, and procedures prior to use and should receive regular refresher training.

ASSESSMENT PROCESS

EAT is composed of two software-based screening tools: the Basic tool and the Detailed tool. The basic level assessment is an initial screening questionnaire completed by an employee's direct supervisor in accordance with the organization's policies. The assessment is based on day-to-day observations of the employee's actions in the workplace. It does not require the supervisor to interview the employee. The Basic tool contains 17 items and takes approximately 10 minutes to complete. The items fall into the following categories:

- **Organizational climate**: Focuses on the employee's suitability to the work environment, particularly in relation to organizational change and coping skills.

- **Lifestyle changes**: Observation of an employee's personal issues that negatively impact work or that lead to disaffection from work.

- **Circumstantial vulnerabilities**: An employee's potentially exploitable weaknesses or experience of a major negative life event.

- **Personality**: Individual personality traits related to sociability that impact the employee's work.

- **Adversarial mindset**: Employee's personal beliefs that are significantly at variance with those of other employees or that impede loyalty to the organization.

- **Suspicious work activities**: Observation of activities in the workplace that fall outside the norm for the individual or for the position.

- **Unauthorized work activities**: Observation of activities in the workplace that are not authorized for the position.

Supervisors rate each item based on their level of concern (No, Minor, Moderate, Significant, Not Known) and confidence in the rating (Low, Moderate, High, Not Known). They also are required to provide evidence to support their ratings. The Basic tool's effectiveness depends on its honest, accurate, clear, objective, fair, and consistent application by supervisors of all assessed employees.

After submission, EAT software calculates the employee's level of risk: Very Low, Low, Moderate, or High. In addition to the overall score, the Basic level results flag particular items of concern and suggest a recommended course of action. Results of the Basic level assessment are reviewed by a "dedicated practitioner" (typically a human resources or security professional). Results are not provided to the employee's supervisor. The dedicated practitioner determines whether further action is required. Suggested actions for cases scored as "Very Low" risk include standard/annual review. "Low" risk cases may require more frequent review. "Moderate" and "High Risk" cases should be independently assessed by a dedicated practitioner using the Detailed tool.

A Detailed level assessment will be initiated and completed by the dedicated practitioner when:

- The Basic tool indicates moderate or high risk;

- The dedicated practitioner concurs with the Basic level assessment; and

- There is sufficient supporting evidence that is accurate, clear, objective, fair and relevant.

The Detailed tool covers the same behavior categories as the Basic tool, but in more depth. For example, where the Basic tool assesses 8 items in the "Personality" section, the Detailed tool includes 27 items in that section. In total, the Detailed assessment contains 62 items and takes about 30 minutes to complete after gathering necessary information. Prior to completing the Detailed tool, the dedicated practitioner must gather and review additional evidence related to the risks indicated in the initial assessment. This may include the employee's personnel record, interview with the employee, and interviews with the employee's supervisors or coworkers.

Results of the Detailed level assessment are provided in the same format as the Basic level assessment. The results include recommendations for whether specific risk areas require intervention or follow-up with the employee or if it is necessary to obtain additional evidence. Based on results of the Detailed tool, the dedicated practitioner determines whether action is taken to mitigate risks posed by the employee in accordance with the organization's established security and personnel policies.

ADDITIONAL CONSIDERATIONS

This study's evaluation of EAT raised several points that must be accounted for in the development of a reporting system to augment continuous evaluation procedures. The content of the questionnaire must be carefully designed to balance the relevance of reportable behaviors against the ability to accurately assess the level of concern for these behaviors. Some managers may be able to identify reportable behavior but still be challenged to understand how to report their level of concern. Managers may also be reluctant to report information or they may categorize the behavior as "not known" on the level of concern to avoid future problematic confrontation with employees. Other managers may still believe there is no reason to report particular behaviors if the employee is otherwise productive and the organization is operating successfully. This belief may result in underreporting of the observable behaviors to avoid getting employees in trouble through follow-up investigation by dedicated practitioners. Despite the concept of "personality" having relevance for personnel security, managers may be either reticent or ill equipped to make the assessments on personality characteristics. Minimizing rater bias in the calculation of the overall risk score would require careful testing and validation of questionnaire content both during development and in an ongoing evaluation system.

APPENDIX B: LITERATURE REVIEW SUPPLEMENT

This appendix provides a systematic review of previous research characterizing known obstacles to supervisor and coworker reporting in order to identify methods for increasing felt responsibility and motivation for reporting concerning behaviors. The findings of this review are summarized in the Results section of the main report.

This review defines reporting behavior as the individual decision to report or not report adverse information (e.g., misconduct) to an appropriate authority. Because there is little research that specifically addresses personnel security reporting, the review included academic and applied research from multiple domains, such as studies of "whistleblowing" in public and private organizations, workplace safety incidents, and antecedents of school violence. These works also cover a broad range of reportable behavior, including actual or threatened law violations, unethical conduct or counterproductive work behavior, and simply reporting "bad news" to others. The present report uses the term "misconduct" to describe this broad range of reportable information.

This systematic literature review examined 142 academic and applied research articles. The methods used to select and analyze relevant research are described in the Method section of the main report. This literature review highlighted important topics related to complex social and psychological factors that may affect an individual's decision to report potential misconduct. This appendix provides an overview of empirically demonstrated measures, recommendations, and precautions for developing a successful supervisor reporting system.

Findings are presented in four sections and reflect the primary themes and subthemes identified in the review. The first section summarizes research findings that focus on the individual decision to report, including personal characteristics that influence the propensity to report and factors that may be involved in cost-benefit calculations.

The second section covers organizational factors that may mediate patterns of both misconduct and reporting behavior. It focuses on three related findings:

- Various elements of an organization's culture may directly influence both propensity to misconduct and reporting;
- Professions may develop unique cultural barriers that put reporting at odds with other professional priorities, a finding of particular relevance to military organizations; and
- More positively, an organization's development of effective reporting systems can reduce the likelihood of misconduct.

The third section considers broader psychosocial patterns of nonreporting to demonstrate the fundamental barriers that any effort to increase reporting behavior must face: there are deeply socialized norms against reporting that are instilled in early childhood and there are psychological and social barriers to communicating adverse information that may transcend any organizational context.

Research on reporting behavior is closely related to studies of felt responsibility and autonomous motivation. The fourth section looks at studies demonstrating that factors influencing an individual's sense of responsibility toward an organization and coworkers will also influence the likelihood of prosocial behavior such as reporting or intervening to assist an at-risk employee.

DECISION TO REPORT MISCONDUCT

Research into personal characteristics of the reporter has shown mixed results. The dominant position in the literature appears to be that there are few a priori characteristics that contribute to the propensity of individuals to report. Situational factors, however, may lead individuals to calculate the costs and benefits of the reporting decision.

Individual Propensity to Report

A small number of studies have attempted to identify individual characteristics such as personality traits that may determine reporting likelihood. Personality traits may be important antecedents to reporting. For example, individuals exhibiting traits of extraversion, dominance, and lower levels of agreeableness may be more likely to report (Bjørkelo, Einarsen, & Matthiesen, 2010). An individual's moral beliefs may also predict reporting behavior, as idealistic attitudes are positively related to reporting (Batson, Klein, Highberger, & Shaw, 1995; Sims & Keenan, 1998; Campbell, Stylianou, & Shropshire, 2016). In government organizations, reporting is more likely by individuals displaying higher levels of altruism and "public service motivation" (Caillier, 2016b). Other studies, however, have found no a priori psychological or ideological profile of those more or less likely to report (Detert & Edmondson, 2011; Henik, 2014), and, given how few studies have focused on individual-level predictors, this position seems to be the dominant assumption in the literature.

On the other hand, the specific role of the reporter within the organization is among the more widely recognized indicators of individual propensity. More powerful individuals are more likely to intervene when they witness misconduct (Hershcovis, Neville, Reich, Christie, Cortina, & Shan, 2017). This may reflect how perceptions of one's "psychological safety" to report are reduced by the "power distance" between an organization's low and high status members (Appelbaum, Dow, Mazmanian, Jundt, & Appelbaum, 2016). Unfortunately, leaders are less likely to report observed misconduct when they believe reporting a particular event falls outside their organizational role, when concerned about their own poor work performance, or when employed in more highly bureaucratized organizations (Miceli, Near, & Schwenk, 1991). For low-level managers, a sense of obligation to report is related to knowledge of reporting mechanisms and potential reporting outcomes, knowledge that generally comes with greater experience in the organization (Keenan, 1995).

Cost-Benefit Calculation

The significant difference in the literature between the few studies of individual traits compared to the regular emphasis on organizational roles reflects the common assumption that reporting is a rational, almost economic, judgment of self-interest. There is strong evidence supporting arguments that reporting behavior depends on the individual's careful weighing of costs and benefits (Miceli & Near, 1985; Caillier, 2016b). In some cases, reporting may depend on a purely economic assessment. For example, a study of safety violation reporting found that workers report accidents at a much lower rate when they perceive employment to be insecure (Probst, Barbaranelli, & Petitta, 2013). In other cases, reporting may depend on more complex moral calculations. For example, it is unsurprising that peer reporting is diminished by fear of retaliation; however, it is also influenced by the reporter's sense of responsibility for the wrongdoer's punishment (De Graaf, 2010). When reporters judge misconduct to be unintentional, they are more likely to confront the wrongdoer directly rather than report to management (King, 2001). Internal auditors are more likely to report fraudulent activity they discover when they believe the wrongdoer personally benefits (Sonnier, 2013). A study of campus violence found that pre-incident reporting behavior correlated with the reporter's evaluation of immediacy of danger and likelihood of harm to self or others (Hodges, Low, Viñas-Racionero, Hollister, & Scalora, 2016).

Reporting may also include social calculation. Studies commonly attempt to account for the personal relationship between the observer and the wrongdoer (Rehg, Miceli, Near, & Van Scotter, 2008). A study of mass shootings on college campuses found that pre-incident behaviors were not reported due to relationship factors of the potential reporter to the perpetrator, including personal victimization or perceptions of danger (Hollister & Scalora, 2015). Finally, differences between willingness to report and actual reporting may depend on the reporter's interest in the outcome (Micelli, Near & Schwenk, 1991; Brink, Lowe & Victoravich, 2013). This may be the simple result of fear of consequences (Cortina & Magley 2003) or a more complex moral judgment, such as the reporter's desire for procedural fairness or retributive justice (Victor, Trevino, & Shapiro, 1993).

ORGANIZATIONAL INFLUENCE ON REPORTING

Even where studies work from an individual unit of analysis, there is a robust consensus in the literature that the organizational setting heavily influences both misconduct and reporting. Such factors include the organization's ethical climate as well as perceptions of the organization and its leaders as trustworthy. Critically, some organizations may develop cultural practices and values at odds with their own reporting requirements. Just as important, however, are an organization's formal policies and practices, including effective reporting channels, protections against retaliation, and education programs that define misconduct and explain reporting mechanisms. Studies show that a well-implemented reporting and compliance program, aligned with a strong ethical culture, will both increase reporting likelihood and decrease the occurrence of misconduct (Ethics Resource Center, 2008).

Organizational Climate

A number of factors controllable by the organization directly influence reporting behavior. For example, a major barrier to reporting may be the simple failure of an organization to recognize that reporting requires an available label for both the act of misconduct and the wrongdoer (Westmarland & Rowe, 2016; Taylor & Taylor, 2017). Unsurprisingly, inconsistent enforcement of organizational policies by managers is a strong indicator of underreporting (Probst & Estrada, 2010), and even a manager's likeability influences willingness to report (Kaplan, Pope, & Samuels, 2015). More significantly, perceptions of managers as being ethical increases employees' sense of psychological safety, individual commitment to the organization, and therefore willingness to report (Walumbwa & Schaubroeck, 2009; Hassan, Wright, & Yukl, 2014). At the same time, an employee's dependence on a peer or superior reduces willingness to report that person's misconduct (McIntosh, et al., 2017).

Unrealistic corporate expectations are perhaps the greatest influence on unethical behavior within business organizations (Lagan, 2006), and the pressure of those expectations undermines willingness to report (Probst & Graso, 2013). Nonreporting due to employees' moral disengagement has been correlated with specific organizational characteristics. For instance, reporting is less likely in technocratic organizations that prioritize immediate results and encourage internal competition and more likely in bureaucratic cultures with well-defined reporting roles and expectations (Petitta, Probst, & Barbaranelli, 2017). Nonreporting may also be an inevitable consequence of unclear or competing organizational demands that force employees to make value judgments of their own and their coworkers' behavior, a pattern that actually increases as employees gain job experience (Mansbach, Kushnir, Ziedenberg, & Bachner, 2014). Peer reporting is enhanced in organizations that encourage a participatory culture and instill confidence in upward communication (Richardson, Wheeless, & Cunningham, 2008). In addition, organizations must also consider the changing external environment in which they operate, such as changing norms around gender roles and sexual harassment (Keenan, 1995; McDonald, 2012).

Cultures of Misconduct and Reporting

Certain professions may develop unique barriers to reporting. For example, construction workers may underreport workplace injuries because of the negative consequences for job security, but this may also result from an industry culture that sees injuries as "part of the job" (Moore, Cigularov, Sampson, Rosecrance, & Chen, 2013). Some organizational cultures expect members to be "good sports" and not complain about problems (Podsakoff, Whiting, Podsakoff & Blume, 2009), a form of "citizenship behavior" that is critical in establishing trust between military leaders and their subordinates (Deluga, 1995; Guburz 2009). Other cultures enforce an informal "code of silence" in which expectations of peer loyalty outweigh formal mandates to report misconduct (Westmarland & Rowe, 2016; Magal, 2017). For example, a number of studies have considered the unique culture of law enforcement organizations that frequently share belief in a "blue code" against peer reporting. In such cultures, certain

behaviors might be "trivialized" so that complaining about those behaviors becomes taboo (Geoffrion, Goncalves, Boyer, Marchand, & Guay, 2017). Peer reporting of police misconduct depends on evaluation of the seriousness of misconduct in relation to internal norms rather than the letter of the law, and willingness to report in these organizations is less likely without some recognizable benefit to the reporter or an easily predictable outcome (Westmarland, 2005; Long, Cross, Shelley, & Kutnjak Ivković, 2013). These informal codes are quickly socialized among new police officers, although more experienced officers are more likely to report even serious misconduct than new officers (Westmarland & Rowe, 2016; Rothwell & Baldwin, 2007).

A similar pattern may exist in military organizations. Pershing (2002; 2003) studied students at the U.S. Naval Academy and found that institutional expectations of professional self-regulation in adherence with a code of conduct were less influential than informal norms of peer loyalty. The conflict between these institutional norms results in the social marginalization of both those reported for misconduct and those who rigidly enforce the code of conduct; because of this, successful peer intervention in misconduct requires "neutralizing" conflicting loyalties to peers and the institution. The unique character of military culture is also highlighted in a survey comparing reporting attitudes between U.S. Military and DoD civilian personnel (Scalora, Bullig, DeKraai, Hoffman, & Avila, 2014). Although the study found consistently high willingness to intervene when observing potentially violent threats, military personnel significantly favored direct intervention over simply reporting to an appropriate authority. The authors attribute the differences to cultural factors, including the normalization of violence and norms of problem resolution based on self-regulation and unit loyalty. Modern military institutions around the world operate on this same general "culture of silence" (Magal 2017). The self-regulation of military members is related to cultural norms that give great value to unit loyalty, unquestioning patriotic service, and the unique character of a military's role in society. However, contextual factors that create a chilling effect on reporting may be the same as those that influence wrongdoing in the first place, so that efforts to create a more professional culture that values reporting should also reduce cultural incentives for misconduct.

Reporting System

It seems certain that the combination of a well-implemented reporting program and a strong ethical culture will increase reporting behavior and decrease misconduct (Ethics Resource Center, 2008). Of course, the availability and accessibility of reporting mechanisms is critical to reporting decisions (Avery & Quinones, 2002). However, a poorly designed or implemented system may impede reporting (Bunn & Sagan, 2014). Reporting systems may take many forms and may rely on both formal and informal reports through either internal or external channels. Reporters may use different reporting channels depending on the direct effects of misconduct. For example, a study of workplace violence (Arnetz et al., 2015) found that formal reporting channels are rarely used except when the victim lost time from work. College students are most likely to report pre-incident indicators of violence through formal reporting channels

when they are already aware of available resources; those who turn to informal channels are influenced by their relationship to the potentially dangerous individual or their belief that formal reporting might escalate the situation (Hodges, Low, Viñas-Racionero, Hollister, & Scalora, 2016).

Internal reporting systems range from direct reporting to supervisors to formal reporting positions or departments within the organization. External channels may include third-party hotlines, regulatory agencies, or even reporting to news and media outlets. Organizations usually prefer internal channels because they allow better management of reporting consequences. To be successful, however, managers must consistently build trust in internal reporting by carefully and transparently investigating alleged misconduct, minimizing the possibility of retaliation, and taking positive corrective actions (Near & Miceli, 2016). Employees who unsuccessfully confront peers about misconduct are more likely to report the misconduct to an immediate supervisor rather than an official internal reporting channel (Kaplan, Pope, & Samuels, 2010). Unfortunately, management "open door" policies are often improperly implemented and employees do not trust their effectiveness (Miceli, Near, & Dworkin, 2008). Concerns about appearing disloyal may influence higher rates of internal reporting, even where formal external channels exist (Sonnier, 2013). Organizations may rely on external reporting channels either to provide employees a reporting option that appears more safe and objective than internal channels or because such channels are imposed by regulators. Reporting intention of low-level employees is higher when channels are administered externally (Gao, Greenberg, & Wong-On-Wing, 2015), while managers turn to external reporting mechanisms when they perceive a direct threat to coworkers or the public, when there are few observers, and when the organization is externally regulated (Miceli, Near, & Schwenk, 1991). Employee willingness to use a particular reporting mechanism may also reflect their level of trust in the organization. Internal reporting is more likely where there is a strongly ethical organizational culture, and external reporting is more common where the organization's ethical character is questionable (Miceli & Near 1985; Kaptein, 2011).

This complexity may require organizations to develop multiple reporting channels to account for the range of reporters' positions and propensities to report (Kaptein, 2011). Codes of conduct and reporting systems are only as effective as the organization's commitment to preventing misconduct. For example, organizations that implement whistleblowing education programs increase the likelihood of reporting and decrease retaliation against reporters (Caillier, 2016a); however, failure to change the broader climate is likely to perpetuate members' moral disengagement by instilling cynical attitudes in low-level managers and undermining employees' sense of empowerment to report misconduct of their peers (Nair & Kamalanabhan, 2011). Reporting likelihood may decrease if organizational definitions of misconduct and responsibility do not align with members' definitions (Saunders, Huynh & Goodman-Delahunty, 2007). In highly competitive, individualist cultures, poorly designed reporting systems may be manipulated by ill-intentioned employees to the detriment of both peers and the

organization as a whole (Loyens, 2013). In addition, procedural safeguards against retaliation may have little effect on, or actually inhibit, willingness to report if not properly designed and implemented (Cortina & Magley, 2003; Kaplan, Pany, Samuels, & Zhang, 2009; Kaplan, Pope, & Samuels, 2015).

UNDERLYING REASONS FOR NONREPORTING

Organizational influences clearly affect reporting behavior, but the different patterns emphasize the underlying problem that nonreporting is the norm across organizations and forms of misconduct. Two lines of research offer complementary explanations for the seeming universality of this phenomenon. One line has demonstrated that attitudes and behaviors related to reporting develop from early life experiences. Studies of "tattling" or "snitching" behavior among children indicate that norms against reporting become stronger as children age, and the formation of this behavior reflects children's relationships with adult authority figures, peer group dynamics, and broader cultural influences that define reportable misconduct and acceptable attitudes toward authority. Other researchers have focused on the more fundamental question of voice and silence behaviors, that is, why individuals choose to speak up or remain silent in socially challenging circumstances. These studies suggest that nonreporting may be the result of a general reluctance to report bad news to authorities or, on a more personal level, anxiety about a potentially uncomfortable social interaction.

Socialized Norms against Reporting

Studies of reporting behavior in children point to deeply socialized norms against reporting, which become stronger as children age. The formation of these behaviors reflects children's relationships to adult authority figures, dynamics within the more immediate social environment of peer groups, and broader cultural influences that define reportable misconduct and acceptable attitudes toward authority. This line of research suggests that, although organizations may create incentives or disincentives to report, negative attitudes toward reporting the misconduct of others is well established in most people before they reach adulthood.

Among preschool children, "tattling" may account for the majority of communication about peers by young children to adults. While more commonly displayed by socially dominant children, preschooler reports are highly truthful and usually align with teachers' assessments of the reported misconduct (Ingram & Bering, 2010). This sort of tattling is shaped by adult responses, and the consequences of tattling help establish children's understanding of moral standards and evaluation (Bak & Ross, 1996). Among elementary school students, older students are less likely to report minor transgressions, suggesting that reporting behaviors are influenced by both cognitive development and changing relationships among peers, which impose high social costs for violations of peer group loyalty (Chiu Loke, Heyman, Forgie, McCarthy, & Lee, 2011). A comparison of American and Japanese schoolchildren found cultural differences in reporting for older elementary students, suggesting that socialization of

reporting behavior might be influenced by cultural patterns of respect for authority and social interdependence (Chiu, Loke, Heymany, Itakura, Toriyama, & Lee, 2014).

Reporting becomes more situationally contingent as children reach adolescence. For example, willingness of middle school students to report on peers is affected by the specific reporting context, such as the reporter's trust in adults or a school's policies to protect anonymity (Brank et al, 2007). Reporting context is also strongly influenced by peer socialization. A large-scale study of middle school students across the United States found that individual teens who perceive aggressive behaviors as a source of social status also express attitudes against reporting threats and that attitudes about aggression and social status are a better indicator of the general reporting attitudes within a school than other demographic measures (Millspaugh, Cornell, Huang, & Datta, 2015). In general, reporting behaviors are negatively associated with social status, with socially rejected teens perceived as more likely to snitch by both their peers and adults (Friman, et al., 2004).

High school students are significantly less likely to report or intervene directly in a peer's misconduct than middle school students, although willingness to report depends on the individual's trust in the authority of the school and its leaders (Syvertsen, Flanagan & Stout, 2009). Moreover, school efforts to encourage students' use of official channels are hampered by broader community "anti-snitching" attitudes based in cultural distrust of formal authority (Morris, 2010), and adherence to an anti-snitching "street code" is among the strongest predictors against peer reporting (Slocum, Esbensen, & Taylor, 2017). Older students also become more tolerant of transgressions as they learn to recognize differences between decreed moral principles and socially tolerated behavior (Wang, Zhang, & Kou, 2015). Given these social pressures against reporting, efforts by educators in recent years to encourage peer reporting to prevent mass violence have been largely ineffective (Madfis, 2014).

Silence and Voice Behavior

For the most part, the research presented in the previous sections begins with an assumption that reporting and nonreporting are opposite sides of the same coin, emphasizing the individual decision to report misconduct when another's actions are recognized as such. A smaller but equally compelling body of research argues for the complex nature of "silence" and "voice" behaviors (Morrison & Milliken, 2000; Detert & Edmondson, 2011), that is, the reasons individuals withhold or express information to others. Accounting for this complexity is necessary to accurately attribute the motives of reporters and nonreporters. Misunderstanding individual reporting actions may result in organizational responses that do not correct underlying problems (Dyne, Ang & Botero, 2003).

There is strong evidence that most people are generally reluctant to communicate "bad news" with others, regardless of prior social influences, positive incentives to speak up, or consequences for remaining silent (Rosen & Tesser, 1970). Although studies of silence and voice disagree whether these behaviors are rooted in basic emotions or

rational decision-making (Detert & Edmondson, 2011), this reluctance to speak up in itself seems sufficient to explain the tendency to nonreporting. It also suggests a more fundamental problem to overcome than simply encouraging people to report misconduct. That is, remaining silent due to reluctance appears to be a different behavior than choosing to report others' misconduct in accordance with social norms or organizational pressures. This difference can be seen in studies of the "bystander effect" in which isolated individuals are more likely to intervene in observed misconduct than in cases where there are multiple observers and responsibility to intervene is "diffused" across the group. Here, social isolation creates an urgency to act that is stronger than personal reluctance and independent of preexisting social roles or constraints (Darley & Latané, 1968).

Reluctance to share bad news and the bystander effect have been validated in subsequent research (Keil, Smith, Pawlowski, & Jin, 2004; Bowes-Sperry & O'Leary-Kelly, 2005; Richardson, Wheeless, & Cunningham, 2008; Nickerson, Aloe, Livingston & Feeley, 2014). These works have also contributed to findings that silence and voice, and by extension reporting and nonreporting, are distinct and multidimensional behaviors and not simply opposites (Dyne, Ang & Botero, 2003). In this model, voice and silence may each be "acquiescent" (the passive response to a situation due to moral disengagement), "defensive" (a proactive response motivated by self-protection), or "prosocial" (a proactive response motivated by concern for others). While the model provides a framework for explaining individual behavior, it also raises the question of how observers interpret silence and voice behaviors. For example, a completely unintentional behavior could be interpreted as silence or voice by an observer, for instance when an individual is not aware that another person's behavior constitutes misconduct or when someone speaks up without knowing there are norms against it. This research is particularly relevant to developing new reporting requirements. If an organization misattributes the causes of nonreporting, any fix based on these assumptions may be flawed.

FELT RESPONSIBILITY TO REPORT

Silence and voice theories have influenced research on "prosocial" behavior, including reporting, in organizational contexts (Dozier & Micelli, 1985). Prosocial behaviors are those actions intended to benefit others, whether the action is motivated purely by altruism or in part by self-interest (Staub, 1978). These studies show that positive prosocial behavioral changes in the workplace can be achieved through fostering employees' sense of felt responsibility to the organization and its members, that is, the individual's belief that they are directly obligated to guide positive change (Dose & Klimonski, 1995; Gagne & Deci, 2005; Fuller, Marler, & Hester, 2006).

If an individual feels a sense of responsibility toward an organization or coworkers, they may be more likely to exhibit helping behavior, including reporting of misconduct (Pearce & Gregersen, 1991; Hershcovis et al., 2017). This sense of personal obligation plays a crucial role in various aspects of job performance, from individual behaviors

such as timeliness or absenteeism to measures of collective productivity and effectiveness (Morrison & Phelps, 1999). Felt responsibility is fostered when accountability results in clear expectations, perceived control of the situation, and the perception that the behavior is important (Dose & Klimoski, 1995; Poile, 2017). Organizational efforts to improve felt responsibility must also educate individuals on when and how to act on their responsibilities, account for possible resistance to behavioral change, and reinforce collective feelings of concern and respect for others (Gagne & Deci, 2005).

Formal Acknowledgment of Personal Responsibility

Information-based, persuasive educational campaigns to help employees recognize and appropriately address potential concerns may have limited effectiveness (Dickerson, Thibodeau, Aronson, & Miller, 1992). Most people are relatively passive recipients of information even when there are follow-up questions as part of the training, and this may be especially true with respect to compliance with reporting policies. An active commitment to comply with regulations may result in more reporting because people want to be consistent in their values and actions and appear consistent to others (Cialdini, 2009). Personal consistency is valued within society and simplifies daily life by reducing information-processing requirements in recurring situations. Additionally, making a voluntary, active decision to do something may result in more commitment than making the same choice by doing nothing (Cioffi & Garner, 1996; Shu, Gino, & Bazerman, 2011).

Psychological research suggests that the additional step of requiring a signed acknowledgment of personal responsibility may make training more salient and improve compliance (Shu et al., 2011; Mazar, Amir, & Ariely, 2008). Ordinary people may justify their unethical behavior through moral disengagement, and the likelihood of unscrupulous behavior is increased due to motivated forgetting (selective memory) of moral rules. This phenomenon probably is common, and it is more likely to occur in permissive environments. However, reading and signing something like an honor code can increase moral saliency and thereby reduce moral disengagement and unethical behavior (Shu et al., 2011; Mazar et al., 2008). For example, research has found that the action of signing one's name resulted in more compliance with the honor code than simply reading it (Shu et al., 2011). When people make a commitment to do something, they usually want to behave in ways that are consistent with that commitment (Cialdini, 2009). A signed certification functions as a commitment to uphold personal responsibilities, resulting in a higher likelihood that the signer will act in accordance with this commitment. Although manipulating perceived accountability may affect people differently, it may also promote enduring attitude and behavior change because it involves the compelling influence of cognitive dissonance (Festinger, 1957; Aronson, 1992; Dickerson, Thibodeau, Aronson, & Miller 1992; Frink & Ferris, 1999).

CONCLUSIONS

Taken together, this research points to individual reporting behavior as the result of immediate contextual factors (e.g., the reporter's relation to misconduct or the organizational setting) and preexisting psychosocial factors (e.g., socialized norms or silence and voice behaviors). Most context-focused studies, whether focused on the reporter or the organization, generally have an underlying presumption of reporters as rational actors and see reporting behavior as the result of careful cost-benefit analyses influenced by competing incentives and possible outcomes. Socialization research also may presume rational action but generally sees normative behavior as responses learned early in life to conform to social and cultural expectations of appropriate conduct. If context theories are the best explanation of reporting behavior, then increasing reporting is possible by carefully establishing a set of reporting incentives that are stronger than organizational disincentives. If socialization theories or silence and voice models are correct, increasing reporting is much more difficult because an organization's efforts must account for attitudes and behaviors it had no hand in instilling.

The commonalities revealed across these studies suggest that most organizations face the same fundamental problem of underreporting. This literature makes clear that an organization should expect that most people, most of the time, will not report misconduct they observe. However, the variation in reporting behavior demonstrated in these studies points to the fact that an organization's policies, practices, and culture directly influence its members' propensity to both commit misconduct and to report it when observed. These findings suggest that a comprehensive approach to prevention and mitigation of misconduct may also increase the likelihood of reporting, and vice versa. Efforts to increase reporting may be best achieved by providing a clear, easily used, and trusted reporting system along with a positive organizational culture that makes felt responsibility to report stronger than the psychosocial barriers against it.

APPENDIX B REFERENCES

NOTE: This section includes all sources reviewed for this study. Sources consulted, but not cited, are prefaced by a "*".

Appelbaum, N. P., Dow, A., Mazmanian, P. E., Jundt, D. K., & Appelbaum, E. N. (2016). The effects of power, leadership and psychological safety on resident event reporting. *Medical Education, 50*(3), 343-350.

Arnetz, J. E., Hamblin, L., Ager, J., Luborsky, M., Upfal, M. J., Russell, J., & Essenmacher, L. (2015). Underreporting of workplace violence: Comparison of self-report and actual documentation of hospital incidents. *Workplace Health & Safety, 63*(5), 200-210.

Aronson, E. (1992). The return of the repressed: Dissonance theory makes a comeback. *Psychological Inquiry, 3* (4), 303-311.

Avery, D. R., & Quiñones, M. A. (2002). Disentangling the effects of voice: the incremental roles of opportunity, behavior, and instrumentality in predicting procedural fairness. *Journal of Applied Psychology, 87*(1), 81-86.

Baillien, E., Neyens, I., & De Witte, H. (2008). Organizational, team related and job related risk factors for workplace bullying, violence and sexual harassment in the workplace: A qualitative study. *International Journal of Organisational Behaviour, 13*(2), 132-146.

Bak, I. M., & Ross, H. S. (1996). I'm telling! The content, context, and consequences of children's tattling on their siblings. *Social Development, 5*(3), 292-309.

* Barnett, T., Bass, K., & Brown, G. (1996). Religiosity, ethical ideology, and intentions to report a peer's wrongdoing. *Journal of Business Ethics, 15*(11), 1161-1174.

Batson, C., Klein, T., Highberger, L., & Shaw, L. (1995). Immorality from empathy-induced altruism: When compassion and justice conflict. *Journal of Personality and Social Psychology, 68*(6), 1042-1054.

* Becker, T. E. (1998). Integrity in organizations: Beyond honesty and conscientiousness. *The Academy of Management Review, 23*(1), 154-161. doi:10.2307/259104

Bjørkelo, B., Einarsen, S., & Matthiesen, S. B. (2010). Predicting proactive behaviour at work: Exploring the role of personality as an antecedent of whistleblowing behaviour. *Journal of Occupational and Organizational Psychology, 83*(2), 371-394.

* Blakely, G. L., Andrews, M. C., & Moorman, R. H. (2005). The moderating effects of equity sensitivity on the relationship between organizational justice and organizational citizenship behaviors. *Journal of Business and Psychology, 20*(2), 259-273.

* Blando, J., Ridenour, M., Hartley, D., & Casteel, C. (2015). Barriers to effective implementation of programs for the prevention of workplace violence in hospitals. *Online Journal of Issues in Nursing, 20*(1).

* Booth-Kewley, S. (1995). *Factors affecting the reporting of sexual harassment in the Navy* (NPRDC-TN-95-9). San Diego, CA: Navy Personnel Research and Development Center.

Bowes-Sperry, L., & O'Leary-Kelly, A. M. (2005). To act or not to act: the dilemma faced by sexual harassment observers. *Academy of Management Review, 30*(2), 288-306.

Brank, E. M., Woolard, J. L., Brown, V. E., Fondacaro, M., Luescher, J. L., Chinn, R. G., & Miller, S. A. (2007). Will they tell? Weapons reporting by middle-school youth. *Youth Violence and Juvenile Justice, 5*, 125–146.

* Brass, D.J., Butterfield, K.D., & Skaggs, B.C. (1998). Relationships and unethical behavior: A social network perspective. *Academy of Management Review, 23*(1), 14-31.

Brink, A. G., Lowe, D. J., & Victoravich, L. M. (2013). The effect of evidence strength and internal rewards on intentions to report fraud in the Dodd-Frank regulatory environment. *Auditing: A Journal of Practice & Theory, 32*(3), 87-104.

* Britt, T.W. (1999). Engaging the self in the field: Testing the triangle model of responsibility. *Personality and Social Psychology Bulletin, 25*(6), 698-708.

* Buckley, L., & Chapman, R. L. (2016). Characteristics of adolescents who intervene to stop the risky and dangerous behavior of their friends. *Accident Analysis & Prevention, 88*, 187-193.

Bunn, M., & Sagan, S. D. (2014). *A worst practices guide to insider threats: lessons from past mistakes*. Cambridge, MA: American Academy of Arts and Sciences.

Caillier, J. G. (2016a). An examination of the role whistle-blowing education plays in the whistle-blowing process. *The Social Science Journal, 54*(1), 4-12

Caillier, J. G. (2016b). Public service motivation and decisions to report wrongdoing in US federal agencies: Is this relationship mediated by the seriousness of the wrongdoing. *The American Review of Public Administration, 47*(7), 810-825.

Campbell, M., Stylianou, A. C., & Shropshire, J. (2016). The impact of attitudinal factors on intention to report workplace Internet abuse. *Journal of Information Privacy and Security, 12*(2), 68-83.

* Carter, M., Thompson, N., Crampton, P., Morrow, G., Burford, B., Gray, C., & Illing, J. (2013). Workplace bullying in the UK NHS: A questionnaire and interview study on prevalence, impact and barriers to reporting. *BMJ Open, 3*. doi:10.1136/bmjopen-2013-002628

Chiu Loke, I., Heyman, G. D., Forgie, J., McCarthy, A., & Lee, K. (2011). Children's moral evaluations of reporting the transgressions of peers: age differences in evaluations of tattling. *Developmental Psychology, 47*(6), 1757.

Chiu Loke, I., Heyman, G. D., Itakura, S., Toriyama, R., & Lee, K. (2014). Japanese and American children's moral evaluations of reporting on transgressions. *Developmental Psychology, 50*(5), 1520.

* Choi, J. N. (2007). Change-oriented organizational citizenship behavior: Effects of work environment characteristics and intervening psychological processes. *Journal of Organizational Behavior, 28*(4), 467-484. doi:10.1002/job.433

Cialdini, R. B. (2009). *Influence: Science and Practice* (5th ed.). Boston: Allyn & Bacon.

Cioffi, D., & Garner, R. (1996). On doing the decision: Effects of active versus passive choice on commitment and self-perception. *Personality and Social Psychology Bulletin, 22* (2), 133-147.

* Clarke, H.M. (2014). Predicting the decision to report sexual harassment: Organizational influences and the theory of planned behavior. *Journal of Organizational Psychology 14*(2), 52-65.

Cortina, L. M., & Magley, V. J. (2003). Raising voice, risking retaliation: Events following interpersonal mistreatment in the workplace. *Journal of Occupational Health Psychology, 8*(4), 247-265.

Darley, J.M., & Latané, B. (1968).Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4), 377-383.

De Graaf, G. (2010). A report on reporting: Why peers report integrity and law violations in public organizations. *Public Administration Review, 70*(5), 767-779.

* Deisinger, E.R.D., Scalora, M.J. (2016). Threat assessment and management in higher education in the United States: A review of the 10 years since the mass casualty incident at Virginia Tech. *Journal of Threat Assessment and Management, 3*(3-4), 186-199.

Deluga, R. J. (1995). The relation between trust in the supervisor and subordinate organizational citizenship behavior. *Military Psychology, 7*(1), 1.

Detert, J.R., & Edmondson, A.C. (2011). Implicit voice theories: Taken-for-granted rules of self-censorship at work. *Academy of Management Journal, 54*(3), 461-488.

Dickerson, C. A., Thibodeau, R., Aronson, E., & Miller, D. (1992). Using cognitive dissonance to encourage water conservation. *Journal of Applied Social Psychology*, 22 (11), 841-854.

Dose, J., & Klimoski, R. (1995). Doing the right thing in the workplace: Responsibility in the face of accountability. *Employee Responsibilities and Rights Journal, 8*(1), 35-56.

Dozier, J.B., & Micelli, M.P. (1985). Potential predictors of whistle-blowing: A prosocial behavior perspective. *Academy of Management Review, 10*(4), 823-36.

* Duval, S., Duval, V. H., & Neely, R. (1979). Self-focus, felt responsibility, and helping behavior. *Journal of Personality and Social Psychology, 37*(10), 1769-1778. doi:10.1037/0022-3514.37.10.1769

Dyne, L. V., Ang, S., & Botero, I. C. (2003). Conceptualizing employee silence and employee voice as multidimensional constructs. *Journal of Management Studies, 40*(6), 1359-1392.

* Einarsen, S., Hoel, H., Zapf, D., & Cooper, C. (2003). *Bullying and emotional abuse in the workplace: International perspectives in research and practice.* London: Taylor & Francis.

Ethics Resource Center (2008). *National government ethics survey: An inside view of public sector ethics.* Arlington, VA: Ethics Resource Center. http://www.ethics.org/files/u5/The_National_Government_Ethics_Survey.pdf

Festinger, L. (1957). *A theory of cognitive dissonance.* Stanford: Stanford University Press.

* Fitzgerald, L. F., Swan, S., & Fischer, K. (1995). Why didn't she just report him? The psychological and legal implications of women's responses to sexual harassment. *Journal of Social Issues, 51*(1), 117-138.

Friman, P. C., Woods, D. W., Freeman, K. A., Gilman, R., Short, M., McGrath, A. M., & Handwerk, M. L. (2004). Relationships between tattling, likeability, and social classification: A preliminary investigation of adolescents in residential care. *Behavior Modification, 28*(3), 331-348.

Frink, D. D., & Ferris, G. R. (1999). The moderating effects of accountability on the conscientiousness-performance relationship. *Journal of Business and Psychology, 13* (4), 515-524.

Fuller, J. B., Marler, L. E., & Hester, K. (2006). Promoting felt responsibility for constructive change and proactive behavior: Exploring aspects of an elaborated model of work design. *Journal of Organizational Behavior, 27*, 1089-1120.

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior, 26*, 331-362.

Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing intentions of lower-level employees: The effect of reporting channel, bystanders, and wrongdoer power status. *Journal of Business Ethics, 126*(1), 85-99.

Geoffrion, S., Goncalves, J., Boyer, R., Marchand, A., & Guay, S. (2017). The effects of trivialization of workplace violence on its victims: profession and sex differences in a cross-sectional study among healthcare and law enforcement workers. *Annals of Work Exposures and Health, 61*(3), 369-382.

* Giacalone, R.A. (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, April 2001. Monterey, CA: Defense Personnel Security Research Center.

* Gurbuz, S. (2009). Some possible antecedents of military personnel organizational * citizenship behavior. *Military Psychology, 21*(2), 200.

Hassan, S., Wright, B.E., and Yukl, G. (2014) Does ethical leadership matter in government? Effects on organizational commitment, absenteeism, and

willingness to report ethical problems. *Public Administration Review, 74*(3), 333-343.

Henik, E. (2014). Understanding whistle-blowing: a set-theoretic approach. *Journal of Business Research, 68*(2), 442-450.

* Henriksen, K., & Dayton, E. (2006). Organizational silence and hidden threats to public safety. *Health Services Research, 41*(4), 1539-1554.

Hershcovis, M., Neville, L., Reich, T., Christie, A., Cortina, L., & Shan, J. (2017). Witnessing wrongdoing: The effects of observer power on incivility intervention in the workplace. *Organizational Behavior and Human Decision Processes, 142*, 45-57. doi:http://dx.doi.org.library2.csumb.edu:2048/10.1016/j.obhdp.2017.07.006

Hodges, H. J., Low, E. C., Viñas-Racionero, M. R., Hollister, B. A., & Scalora, M. J. (2016). Examining the reasons for student responses to threatening behaviors on a college campus. *Journal of Threat Assessment and Management, 3*(3-4), 129-142.

Hollister, B. A., & Scalora, M. J. (2015). Broadening campus threat assessment beyond mass shootings. *Aggression and Violent Behavior, 25*(Part A), 43 – 55.

* Hollister, B. A., Scalora, M.J., Hoff, S., & Marquez, A. (2014). Exposure to preincident behavior and reporting in college students. *Journal of Threat Assessment and Management, 1*(2), 129-143.

* Hollister, B.A., Scalora, M.J., Hoff, S.M., Hodges, H.J., & Marquez, A. (2016). College student reporting responses to hypothetical and actual safety concerns. *Journal of School Violence, 15*, 1-18.

Ingram, G. P., & Bering, J. M. (2010). Children's tattling: The reporting of everyday norm violations in preschool settings. *Child Development, 81*(3), 945-957.

* Jeon, S. H. (2017). Where to report wrongdoings? Exploring the determinants of internal versus external whistleblowing. *International Review of Public Administration, 22*(2), 153-171.

Kaplan, S. E., Pany, K., Samuels, J. A., & Zhang, J. (2009). An examination of the effects of procedural safeguards on intentions to anonymously report fraud. *Auditing: A Journal of Practice & Theory, 28*(2), 273-288.

Kaplan, S. E., Pope, K. R., & Samuels, J. A. (2010). The effect of social confrontation on individuals' intentions to internally report fraud. *Behavioral Research in Accounting, 22*(2), 51-67.

Kaplan, S. E., Pope, K. R., & Samuels, J. A. (2015). An examination of the effects of managerial procedural safeguards, managerial likeability, and type of fraudulent act on intentions to report fraud to a manager. *Behavioral Research in Accounting, 27*(2), 77-94.

Kaptein, M. (2011). From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing. *Journal of Business Ethics, 98*(3), 513-530.

Keenan, J. P. (1995). Whistleblowing and the first-level manager: Determinants of feeling obliged to blow the whistle. *Journal of Social Behavior and Personality, 10*(3), 571.

Keil, M., Smith, H. J., Pawlowski, S., & Jin, L. (2004). 'Why didn't somebody tell me?': climate, information asymmetry, and bad news about troubled projects. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 35*(2), 65-84.

King, G. (2001). Perceptions of intentional wrongdoing and peer reporting behavior among registered nurses. *Journal of Business Ethics, 34*(1), 1-13.

* King, G., & Hermodson, A. (2000). Peer reporting of coworker wrongdoing: A qualitative analysis of observer attitudes in the decision to report versus not report unethical behavior. *Journal of Applied Communication Research, 28*(4), 309-329.

* Lagan, A. (2006). When good people do bad things. *In The Black, 76*(7), 75.

* Lanaj, K., Johnson, R. E., & Wang, M. (2016). When lending a hand depletes the will: The daily costs and benefits of helping. *Journal of Applied Psychology, 101*(8), 1097-1110. doi:10.1037/apl0000118

* LaVan, H., & Martin, W.M. (2008). Bullying in the U.S. workplace: Normative and process-oriented ethical approaches. *Journal of Business Ethics, 83*(2), 147-165.

* Law, C.L. (2011). *Sexual harassment and organization outcomes* (TR 99-11). Defense Equal Opportunity Management Institute, Directorate of Research.

* Lee, J. Y., Heilmann, S. G., & Near, J. P. (2004). Blowing the whistle on sexual harassment: Test of a model of predictors and outcomes. *Human Relations, 57*(3), 297-322.

* Lim, S., & Cortina, L.M. (2005). Interpersonal mistreatment in the workplace: The interface and impact of general incivility and sexual harassment. *Journal of Applied Psychology, 90*(3), 483-496.

Long, M. A., Cross, J. E., Shelley, T. O. C., & Kutnjak Ivković, S. (2013). The normative order of reporting police misconduct: Examining the roles of offense seriousness, legitimacy, and fairness. *Social Psychology Quarterly, 76*(3), 242-267.

Loyens, K. (2013). Towards a custom-made whistleblowing policy. Using grid-group cultural theory to match policy measures to different styles of peer reporting. *Journal of Business Ethics, 114*(2), 239-249.

* MacNab, B. R., & Worthley, R. (2008). Self-efficacy as an intrapersonal predictor for internal whistleblowing: A US and Canada examination. *Journal of Business Ethics, 79*(4), 407-421.

Madfis, E. (2014). Averting school rampage: Student intervention amid a persistent code of silence. *Youth Violence and Juvenile Justice, 12*(3), 229-249.

Magal, T. (2017). Self-censorship in military institutions. In D. Bar-Tal, R. Nets-Zehngut, & K. Sharvit (Eds.), *Self-censorship in contexts of conflict* (pp. 139-156). Cham, Switzerland: Springer International.

Mansbach, A., Kushnir, T., Ziedenberg, H., & Bachner, Y. G. (2014). Reporting misconduct of a coworker to protect a patient: a comparison between experienced nurses and nursing students. *The Scientific World Journal, 2014*, 1-6. http://dx.doi.org/10.1155/2014/413926

Mazar, N., Amir, O., & Ariely, D. (2008). The dishonesty of honest people: A theory of self-concept maintenance. *Journal of Marketing Research, XLV*, 633-644.

* McCabe, M.P., & Hardman, L. (2005). Attitudes and perceptions of workers to sexual harassment. *The Journal of Social Psychology, 145*(6), 719-740.

McDonald, P. (2012). Workplace sexual harassment 30 years on: A review of the literature. *International Journal of Management Reviews, 14*(1), 1-17.

McIntosh, T., Higgs, C., Turner, M., Partlow, P., Steele, L., MacDougall, A. E., ... & Mumford, M. D. (2017). To whistleblow or not to whistleblow: Affective and cognitive differences in reporting peers and advisors. *Science and Engineering Ethics*, 1-40. https://doi.org/10.1007/s11948-017-9974-3

Miceli, M. P., & Near, J. P. (1985). Characteristics of organizational climate and perceived wrongdoing associated with whistle-blowing decisions. *Personnel Psychology, 38*(3), 525-544.

Miceli, M. P., Near, J. P., & Dworkin, T. (2008). A word to the wise: How managers and policy-makers can encourage employees to report wrongdoing. *Journal of Business Ethics, 86*, 379-396.

Miceli, M. P., Near, J. P., & Schwenk, C. R. (1991). Who blows the whistle and why? *ILR Review, 45*(1), 113-130.

Millspaugh, S. B., Cornell, D. G., Huang, F. L., & Datta, P. (2015). Prevalence of aggressive attitudes and willingness to report threats in middle school. *Journal of Threat Assessment and Management, 2*(1), 11-22.

Moore, J. T., Cigularov, K. P., Sampson, J. M., Rosecrance, J. C., & Chen, P. Y. (2013). Construction workers' reasons for not reporting work-related injuries: an exploratory study. *International Journal of Occupational Safety and Ergonomics, 19*(1), 97-105.

Morris, E. W. (2010). "Snitches end up in ditches" and other cautionary tales. *Journal of Contemporary Criminal Justice, 26*(3), 254-272.

Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review, 25*(4), 706-725.

Morrison, E., & Phelps, C. (1999). Taking charge at work: Extrarole efforts to initiate workplace change. *The Academy of Management Journal, 42*(4), 403-149.

Nair, P., & Kamalanabhan, T. (2011). Predicting unwillingness to report ethical infractions of peers: A moderated mediation approach. *IIMB Management Review (Elsevier Science), 23*(2), 81-90. doi:10.1016/j.iimb.2011.02.001

* Namie, G. (2007). The challenge of workplace bullying. *Employment Relations Today, 34*(2), 43-51.

Near, J. P., & Miceli, M. P. (2016). After the wrongdoing: What managers should know about whistleblowing. *Business Horizons, 59*(1), 105-114.

Nickerson, A. B., Aloe, A. M., Livingston, J. A., & Feeley, T. H. (2014). Measurement of the bystander intervention model for bullying and sexual harassment. *Journal of Adolescence, 37*(4), 391-400.

Pearce, J. L., & Gregersen, H. B. (1991). Task interdependence and extrarole behavior: A test of the mediating effects of felt responsibility. *Journal of Applied Psychology, 76*(6), 838-844. doi:10.1037/0021-9010.76.6.838

Pershing, J. L. (2002). Whom to betray? Self-regulation of occupational misconduct at the United States Naval Academy. *Deviant Behavior, 23*(2), 149-175.

Pershing, J. L. (2003). To snitch or not to snitch? Applying the concept of neutralization techniques to the enforcement of occupational misconduct. *Sociological Perspectives, 46*(2), 149-178.

* Pershing, J.L. (2003). Why women don't report sexual harassment: A case study of an elite military institution. *Gender Issues 21*(4), 3-30.

Petitta, L., Probst, T. M., & Barbaranelli, C. (2017). Safety culture, moral disengagement, and accident underreporting. *Journal of Business Ethics, 141*(3), 489-504.

Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., & Blume, B. D. (2009). Individual- and organizational-level consequences of organizational citizenship behaviors: A meta-analysis. *Journal of Applied Psychology, 94*(1), 122.

Poile, C. (2017). Why would I help my coworker? Exploring asymmetric task dependence and the self-determination theory internalization process. *Journal of Experimental Psychology: Applied, 23*(3), 354-368. doi:10.1037/xap0000128

Probst, T. M., Barbaranelli, C., & Petitta, L. (2013). The relationship between job insecurity and accident under-reporting: A test in two countries. *Work & Stress, 27*(4), 383-402.

Probst, T. M., & Estrada, A. X. (2010). Accident under-reporting among employees: Testing the moderating influence of psychological safety climate and supervisor enforcement of safety practices. *Accident Analysis & Prevention, 42*(5), 1438-1444.

Probst, T. M., & Graso, M. (2013). Pressure to produce=pressure to reduce accident reporting? *Accident Analysis & Prevention, 59*, 580-587.

Rehg, M. T., Miceli, M. P., Near, J. P., & Van Scotter, J. R. (2008). Antecedents and outcomes of retaliation against whistleblowers: Gender differences and power relationships. *Organization Science, 19*(2), 221-240.

Richardson, B. K., Wheeless, L. R., & Cunningham, C. (2008). Tattling on the teacher: A study of factors influencing peer reporting of teachers who violate standardized testing protocol. *Communication Studies, 59*(3), 202-219.

Robinson, S. N., Robertson, J. C., & Curtis, M. B. (2012). The effects of contextual and wrongdoing attributes on organizational employees' whistleblowing intentions following fraud. *Journal of Business Ethics, 106*(2), 213-227.

Rosen, S., & Tesser, A. (1970). On reluctance to communicate undesirable information: The MUM effect. *Sociometry*, 253-263.

* Rosenfeld, R., Jacobs, B. A., & Wright, R. (2003). Snitching and the code of the street. *British Journal of Criminology, 43*(2), 291-309.

* Rotemberg, J. (1994). Human relations in the workplace. *Journal of Political Economy, 102*(4), 684-717.

Rothwell, G. R., & Baldwin, J. N. (2007). Ethical climate theory, whistle-blowing, and the code of silence in police agencies in the state of Georgia. *Journal of Business Ethics, 70*(4), 341-361.

Saunders, P., Huynh, A., & Goodman-Delahunty, J. (2007). Defining workplace bullying behaviour professional lay definitions of workplace bullying. *International Journal of Law and Psychiatry, 30*(4-5), 340-354.

Scalora, M., Bulling, D., DeKraai, M., Hoffman, S. & Avila A. (2014). *Barriers to reporting threatening behaviors in a military context.* Lincoln, NE: University of Nebraska Public Policy Center.

* Shaffer, D. R., Rogel, M., & Hendrick, C. (1975). Intervention in the library: The effect of increased responsibility on bystanders' willingness to prevent a theft. *Journal of Applied Social Psychology, 5*(4), 303-319. doi:10.1111/j.1559-1816.1975.tb00683.x

Shu, L. L., Gino, F., & Bazerman, M. H. (2011). Dishonest deed, clear conscience: When cheating leads to moral disengagement and motivated forgetting. *Personality and Social Psychology Bulletin, 37*(3), 330-349.

* Simons, T. (2002). Behavioral integrity: The perceived alignment between managers' words and deeds as a research focus. *Organization Science, 13*(1), 18-35. doi:10.1287/orsc.13.1.18.543

Sims, R. L., & Keenan, J. P. (1998). Predictors of external whistleblowing: Organizational and intrapersonal variables. *Journal of Business Ethics, 17*(4), 411-421.

Slocum, L. A., Esbensen, F. A., & Taylor, T. J. (2017). The code of silence in schools: An assessment of a socio-ecological model of youth's willingness to report school misbehavior. *Youth & Society, 49*(2), 123-149.

Sonnier, B. M. (2013). The effects of wrongdoer motivation and internal versus external reporting channel on the intention to report fraud. *Journal of Forensic & Investigative Accounting, 5*(2), 77-113.

* Souder, W.C. (2017). *Risk factors for sexual violence in the military: An analysis of sexual assault and sexual harassment incidents and reporting* (Master's Thesis). Monterey, CA: Naval Postgraduate School.

* Spector, P. & Fox, S. (2002). An emotion-centered model of voluntary work behavior some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource Management Review, 12*, 269-292.

* Stueve, A., Dash, K., O'Donnell, L., Tehranifar, P., Wilson-Simmons, R., Slaby, R. G., & Link, B. G. (2006). Rethinking the bystander role in school violence prevention. *Health Promotion Practice, 7*(1), 117-124.

* Sulkowski, M. L. (2011). An investigation of students' willingness to report threats of violence in campus communities. *Psychology of Violence, 1*(1), 53.

Syvertsen, A. K., Flanagan, C. A., & Stout, M. D. (2009). Code of silence: Students' perceptions of school climate and willingness to intervene in a peer's dangerous plan. *Journal of Educational Psychology, 101*(1), 219.

Taylor, R. A., & Taylor, S. S. (2017). Enactors of Horizontal Violence: The Pathological Bully, the Self-Justified Bully, and the Unprofessional Co-Worker. *Journal of Advanced Nursing, 2017*, 1-8. http://dx.doi.org/10.1111/jan.13382

* Teo, A.R., Holley, S.R., Leary, M., & McNiel, D.E. (2012). The relationship between level of training and accuracy of violence risk assessment. *Psychiatric Services, 63*(11), 1089-1094.

* Thoms, P., Dose, J., & Scott, K. (2002). Relationships between accountability, job satisfaction, and trust. *Human Resource Development Quarterly, 13*(3), 307-323.

* Trevino, L.K., & Brown, M.E. (2004). Managing to be ethical: Debunking five business ethics myths. *Academy of Management Executive, 18*(2), 69-81.

* Trevino, L. K., & Youngblood, S. A. (1990). Bad apples in bad barrels: A causal analysis of ethical decision-making behavior. *Journal of Applied Psychology, 75*(4), 378-385.

Victor, B., Trevino, L. K., & Shapiro, D. L. (1993). Peer reporting of unethical behavior: The influence of justice evaluations and social context factors. *Journal of Business Ethics, 12,* 253-263.

Walumbwa, F. O., & Schaubroeck, J. (2009). Leader personality traits and employee voice behavior: mediating roles of ethical leadership and work group psychological safety. *Journal of Applied Psychology, 94*(5), 1275.

Wang, J., Fu, X., Zhang, L., & Kou, Y. (2015). The impacts of moral evaluations and descriptive norms on children's and adolescents' tolerance of transgression. *Journal of Pacific Rim Psychology, 9*(2), 86-96.

* Weaver, G. R. (2004). Ethics and employees: Making the connection. Academy of *Management Executive, 18*(2), 121-125. doi:10.5465/AME.2004.13836241

Westmarland, L. (2005). Police ethics and integrity: Breaking the blue code of silence. *Policing and Society, 15*(2), 145-165.

Westmarland, L., & Rowe, M. (2016). Police ethics and integrity: can a new code overturn the blue code? *Policing and Society*, 1-17.

* Willness, C.R., Steel, P., & Lee, K. (2007). A meta-analysis of the antecedents and consequences of workplace sexual harassment. *Personnel Psychology, 60*, 127-162.

* Worchel, S., & Brand, J. (1972). Role of responsibility and violated expectancy in the arousal of dissonance. *Journal of Personality and Social Psychology 22*(1), 87-97.

APPENDIX C: SUBJECT MATTER EXPERT (SME) INTERVIEW GUIDE

Task 2.7 Supervisor Reporting
SME Interview Guide

Interviewer(s):	
SME(s):	
Date:	
Location:	

The purpose of this interview is to (1) obtain input on obstacles to reporting employee misconduct and other security concerns, (2) identify best practices for supervisor reporting, (3) obtain input on existing personnel security training related to reporting, and (4) get feedback on the Centre for the Protection of National Infrastructure (CPNI) Employee Assurance Tools (EAT) and the Personal Acknowledgment of Staff Security (PASS) as possible solutions.

Background

How does supervisor reporting work at your agency/component?

How do supervisors know what to report?

What is the system(s) for reporting (e.g., anonymous call line, JPAS, etc.)?

Are there different procedures and systems for reporting different types of concerns?

How often are incident or similar reports submitted?

What types of issues are most often reported?

What doesn't usually get reported that should be reported?

How is follow-up handled? Are follow-up strategies communicated to the workforce?

Does your organization take any steps to reassure people about the handling of reports (e.g., to minimize concerns about negative consequences for both reporter and reported)?

Reporting Obstacles

What are the obstacles to supervisor reporting of employee misconduct and other security concerns?

Why don't supervisors always report concerns in accordance with policy?

Are supervisors reluctant to report their colleagues? If so, why?

What are supervisors' attitudes about reporting?

Do supervisors know what to report and to whom?

What are supervisors' concerns about reporting?

What are some of the potential negative consequences of reporting?

Is it a violation of trust to report somebody? How does that affect the mission?

Reporting Best Practices

Are you aware of any practices that encourage or have improved supervisor reporting?

How can supervisor reporting be improved?

Are you aware of any initiatives to improve reporting?

Does anonymous reporting seem to help?

Do training and awareness programs seem useful?

Are you aware of any annual employee evaluation programs that encourage reporting of security concerns?

CPNI EAT and Related Tools

"The EAT are two software-based screening tools, designed to complement existing measures for managing employee risk: (1) a basic tool for initial screening, and (2) a more detailed tool for following up concerns identified through the basic tool or other channels. Questionnaires are completed by managers (basic level) and by the dedicated practitioner overseeing the process (detailed level). The software then scores the responses and provides a report, accompanied by interpretive guidance, which indicates where to focus attention and how to follow up with the people concerned in order to establish what the issues are."

Are you familiar with the EAT and/or ASA? Please explain.

What do you think are the advantages and disadvantages of this [type of] tool?

Could something like this be used within DoD? Please explain.

What would have to be done differently to use a tool like EAT within DoD?

Would you support pilot testing this type of reporting tool? Please explain.

What are the potential legal or policy obstacles (eg, employment or privacy regulations) to implementing a program like EAT?

EAT relies on review of submitted supervisor reports by a "dedicated practitioner" outside the employee's chain of command. Would that be appropriate in DoD? In DoD who might fill that role?

Are there cultural barriers in DoD that would impact the implementation or effectiveness of a program like EAT?

Could the same system be used for both military and civilian personnel in DoD?

To the best of your knowledge do you feel DoD has the resources to implement a tool like the EAT (e.g., adequate staffing and time allotted)

Currently, can you think of another way in which employee indicators or insider activity is being annually assessed in DoD?

PASS

Do you feel the PASS tool would be useful and effective? What are your thoughts?

Interview Notes:

APPENDIX D: PERSONAL ACKNOWLEDGMENT OF STAFF SECURITY (PASS)

BASIC PROCEDURE

Personnel security training is the most appropriate context for administering the Personal Acknowledgment of Staff Security (PASS) procedure at this time. There are two predominant methods of personnel security awareness training: computer-based training and in-person training by experienced security professionals. The proposed PASS procedure would have to work in both computer-based and in-person contexts because components implement training requirements differently (i.e., some use computer-based training while others provide training in-person). Components could deploy PASS as a stand-alone web application or paper form in conjunction with in-person security awareness training. The PASS procedure could also be made part of an annual, online security training application or some other annual requirement. Figure 1 shows three options for administering the procedure with different training scenarios.
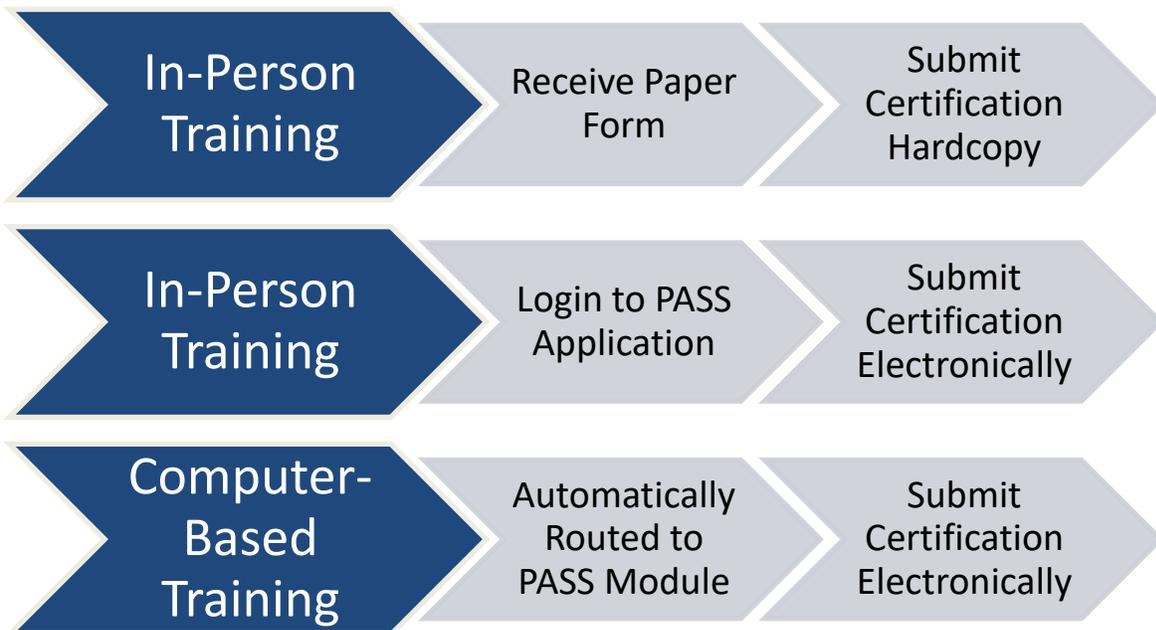
In-Person Training	Receive Paper Form	Submit Certification Hardcopy
In-Person Training	Login to PASS Application	Submit Certification Electronically
Computer-Based Training	Automatically Routed to PASS Module	Submit Certification Electronically

Figure 1 Overview of Options for Proposed Procedure With Different Training Scenarios

After completing security awareness training, supervisors[4] are directed to another computer-based module, or the instructor gives them a paper form, that reiterates their reporting responsibilities. Supervisors are asked to respond to the following three items (True/False) regardless of administration format:

---

[4] Personnel are considered supervisors if they complete official annual performance appraisals for one or more subordinates.

1. I am familiar with Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines and I understand my reporting responsibilities per SEAD 3 and DoDM 5200.02.
2. I am *unaware* of reportable contacts, activities, indicators, or behaviors listed in SEAD 4 for any of my subordinates.
3. If I become aware of reportable contacts, activities, indicators, or behaviors listed in SEAD 4, I will report them in accordance with policy.

Supervisors who select 'False' for any of the items are required to perform the following corresponding actions:

1. Review SEAD 4 and DoDM 5200.02, Section 11, and become familiar with your reporting responsibilities.
2. Discuss your observations with local security personnel who will contact you.
3. Prior to submitting the certification, explain why you do not intend to report contacts, activities, indicators, or behaviors listed in SEAD 4 as required.

After making a selection for each statement, supervisors are asked to certify their responses by entering full name, identification number, grade/rank, affiliation, and contact information. Supervisors then submit the signed and dated PASS certification either electronically (with digital signature) or as hardcopy. Completed forms are forwarded to counterintelligence elements or security managers for follow-up, as necessary, based on the information provided. Figure 1 shows the hardcopy version of the PASS form.

**PERSONAL ACKNOWLEDGMENT OF
STAFF SECURITY (PASS)**

Instructions. Executive Order 12968, Security Executive Agent Directive (SEAD) 3, DoD Manual (DoDM) 5200.02, and DoD Component policies establish requirements for reporting behaviors of personnel security concern that fall under SEAD 4, National Security Adjudicative Guidelines.

Please respond to the following three items concerning the requirement to report behaviors of personnel security concern. Sign and date the form, provide contact information, and submit the completed form to your security management office or as instructed.

I certify the following:	True	False
1. I am familiar with SEAD 4, National Security Adjudicative Guidelines and I understand my reporting responsibilities per SEAD 3 and DoDM 5200.02.	☐	☐
➢ If you selected 'False' for item number 1, please review SEAD 4 and DoDM 5200.02, Section 11 and become familiar with your reporting responsibilities. ○ SEAD 4: https://www.dni.gov/files/NCSC/documents/Regulations/ ○ DoDM 5200.02: http://www.esd.whs.mil/DD/DoD-Issuances/		
2. I am *unaware* of reportable contacts, activities, indicators, or behaviors listed in SEAD 4 for any of my subordinates.	☐	☐
➢ If you selected 'False' for item number 2, local security personnel will contact you to discuss your observations.		
3. If I become aware of reportable contacts, activities, indicators, or behaviors listed in SEAD 4, I will report them in accordance with policy.	☐	☐
➢ If you selected 'False' for item number 3, please explain below why you do not intend to report contacts, activities, indicators, or behaviors listed in SEAD 4 as required.		

3.a. Explanation (continue on other side if necessary):
Click here to enter text.

4. Signature	5. Date Click here to enter text.

6. Printed Name Click here to enter text.	7. Grade/Rank Click here to enter text.

8. Affiliation Click here to enter text.	9. Work Telephone Click here to enter text.	10. Email Address Click here to enter text.

Figure 2 Hardcopy Version of the PASS Form