PERSEREC

Technical Report 13-02
February 2013

Development of a Procedure to Increase Awareness and Reporting of Counterintelligence and Terrorism Indicators: Personal Acknowledgment of Staff Security (PASS)

Daniel G. Youpa
Samantha A. Smith-Pritchard
Northrop Grumman Technical Services

Approved for Public Distribution: Distribution Unlimited
Defense Personnel Security Research Center

Technical Report 13-02 **February 2013**

Development of a Procedure to Increase Awareness and Reporting of Counterintelligence and Terrorism Indicators: Personal Acknowledgment of Staff Security (PASS)

Daniel G. Youpa, Samantha A. Smith-Pritchard—*Northrop Grumman Technical Services*

Released by – Eric L. Lang

BACKGROUND

The potential damage caused by disaffected insiders and external adversaries, including espionage, terrorism, and malicious cyberspace activity, may be reduced by timely reporting of security concerns to appropriate personnel. While it is every employee's responsibility to report potential threats, military and civilian supervisors must ensure that threats are recognized and reported at an early stage so that intervention will have a reasonable chance of success. Nevertheless, previous research and anecdotal evidence indicates that there still may be obstacles to co-worker and supervisor reporting, and inadequate reporting can have devastating consequences. In addition, information-based persuasive campaigns may be insufficient for motivating personnel to report concerns about their colleagues.

HIGHLIGHTS

This report provides background information and a concept of operations for a simple procedure called the Personal Acknowledgment of Staff Security (PASS). The purpose of the proposed procedure is to increase supervisor awareness, felt responsibility, accountability, and reporting of behaviors related to foreign intelligence entity (FIE) threats in accordance with Department of Defense Directive (DoDD) 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, May 17, 2011. The defining feature of PASS is the requirement of a signed certification by supervisors that they understand and intend to comply with reporting policy. Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make training and reporting requirements more salient and improve compliance. The present report presents findings from field research on the PASS concept, as well as descriptions of paper and computer-based versions of the procedure.

Defense Personnel Security Research Center
20 Ryan Ranch Road, Suite 290
Monterey, CA 93940

REPORT DOCUMENTATION PAGE

<table>
<tr><td colspan="3">REPORT DOCUMENTATION PAGE</td><td colspan="3">Form Approved
OMB No. 0704-0188</td></tr>
<tr><td colspan="6">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.</td></tr>
<tr><td colspan="2">1. REPORT DATE: 20130227</td><td colspan="2">2. REPORT TYPE
Technical Report 13-02</td><td colspan="2">3. DATES COVERED (From – To)
October 2011 - February 2013</td></tr>
<tr><td colspan="2" rowspan="3">4. Development of a Procedure to Increase Awareness and Reporting of Counterintelligence and Terrorism Indicators: Personal Acknowledgment of Staff Security (PASS)</td><td colspan="4">5a. CONTRACT NUMBER:</td></tr>
<tr><td colspan="4">5b. GRANT NUMBER:</td></tr>
<tr><td colspan="4">5c. PROGRAM ELEMENT NUMBER:</td></tr>
<tr><td colspan="2" rowspan="3">6. AUTHOR(S):
Daniel G. Youpa, Samantha A. Smith-Pritchard</td><td colspan="4">5d. PROJECT NUMBER:</td></tr>
<tr><td colspan="4">5e. TASK NUMBER:</td></tr>
<tr><td colspan="4">5f. WORK UNIT NUMBER:</td></tr>
<tr><td colspan="2">7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Personnel Security Research Center
20 Ryan Ranch Road, Suite 290
Monterey, CA 93940</td><td colspan="4">8. PERFORMING ORGANIZATION REPORT NUMBER
PERSEREC: Technical Report 13-02</td></tr>
<tr><td colspan="2" rowspan="2">9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</td><td colspan="4">10. SPONSORING/MONITOR'S ACRONYM(S)</td></tr>
<tr><td colspan="4">11. SPONSORING/MONITOR'S REPORT NUMBER(S):</td></tr>
<tr><td colspan="6">12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited</td></tr>
<tr><td colspan="6">13. SUPPLEMENTARY NOTES:</td></tr>
<tr><td colspan="6">14. ABSTRACT: This report provides background information and a concept of operations for a simple procedure called the Personal Acknowledgment of Staff Security (PASS). The purpose of the proposed procedure is to increase supervisor awareness, felt responsibility, accountability, and reporting of behaviors related to foreign intelligence entity (FIE) threats in accordance with Department of Defense Directive (DoDD) 5240.06, Counterintelligence Awareness and Reporting (CIAR), May 17, 2011. The defining feature of PASS is the requirement of a signed certification by supervisors that they understand and intend to comply with reporting policy. Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make training and reporting requirements more salient and improve compliance. The present report presents findings from field research on the PASS concept, as well as descriptions of paper and computer-based versions of the procedure.</td></tr>
<tr><td colspan="6">15. SUBJECT TERMS: insider threat, counterintelligence indicators, terrorism indicators, threat reporting, accountability</td></tr>
<tr><td colspan="3" rowspan="2">16. SECURITY CLASSIFICATION OF: UNCLASSIFIED</td><td rowspan="2">17. LIMITATION OF ABSTRACT:</td><td rowspan="2">18. NUMBER OF PAGES: 79</td><td>19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director</td></tr>
<tr><td>a. REPORT: UNCLASSIFIED</td><td>b. ABSTRACT: UNCLASSIFIED</td><td>c. THIS PAGE: UNCLASSIFIED</td><td>19b. TELEPHONE NUMBER (Include area code): 831-583-2800</td></tr>
<tr><td colspan="6">Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18</td></tr>
</table>

PREFACE

The purpose of this report is to describe the Personal Acknowledgment of Staff Security (PASS) procedure for increasing awareness and reporting of indicators and activities related to espionage, terrorism, and malicious cyberspace activity within the Department of Defense (DoD). It was prepared by the Defense Personnel Security Research Center (PERSEREC) as part of an effort to design and pilot test the proposed system. This report was written for key stakeholders, subject matter experts, and potential end-users. The sponsor for this project was the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD [P&R]). This project also may be of interest to the Office of the Under Secretary of Defense for Intelligence (OUSD [I]). Ultimately, user agencies could include all Department of Defense (DoD) components, including military, civilian, and contractor personnel.

Eric L. Lang
Director

EXECUTIVE SUMMARY

The potential damage caused by disaffected insiders and external adversaries, including espionage, terrorism, and malicious cyberspace activity, may be reduced by timely reporting of security concerns to appropriate personnel. While it is every employee's responsibility to report potential threats, military and civilian supervisors must ensure that threats are recognized and reported at an early stage so that intervention will have a reasonable chance of success. Nevertheless, previous research and anecdotal evidence indicates that there still may be obstacles to co-worker and supervisor reporting, and inadequate reporting can have devastating consequences. In addition, information-based persuasive campaigns may be insufficient for motivating personnel to report concerns about their colleagues.

This report provides background information and a concept of operations for a simple procedure called the Personal Acknowledgment of Staff Security (PASS). The purpose of the proposed procedure is to increase supervisor awareness, responsibility, accountability, and reporting of behaviors related to foreign intelligence entity (FIE) threats in accordance with Department of Defense Directive (DoDD) 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, May 17, 2011. The defining feature of PASS is the requirement of a signed certification by supervisors that they understand and intend to comply with reporting policy. Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make training and reporting requirements more salient and improve compliance. The proposed procedure can be administered paper and pencil or computer-based, both of which are described in the report.

After completing security awareness training, supervisors would be directed to another computer-based module or given a paper form that reiterates their reporting responsibilities, and they would be asked to respond to the following three items (Yes/No) regardless of administration format:

(1) I am familiar with DoDD 5240.06, and I understand my reporting responsibilities per this directive.

(2) I am aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5 for one or more of my subordinates.

(3) If I become aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5, I will report them in accordance with policy.

After making a selection for each statement and responding to additional prompts (as necessary) based on their selections, supervisors would be asked to certify their responses by entering their full name, identification number, grade/rank, affiliation, and contact information. Supervisors would then submit the signed and dated PASS form either electronically or hardcopy. Completed forms would be

forwarded to counterintelligence elements or security managers for follow-up, as appropriate.

Initial interviews with counterintelligence and security personnel about the PASS concept resulted in positive feedback, but responses from a small sample of military and civilian supervisors indicated the need for more research to test and optimize the procedure. Stakeholders and subject matter experts were interested in the PASS concept, but some noted concerns about the utility of behavioral indicators for identifying potential threats, the effect of false positive reports on employees' careers, resistance to the procedure by supervisors, and legal/privacy concerns. Some military and civilian supervisors thought that the procedure was unique, straightforward, reasonable, and potentially effective. However, others felt that some of the materials needed revision to maximize effectiveness, and there were questions about the relative efficacy of paper versus computer-based administration. Another challenge noted by participants was that it would be necessary to distinguish the PASS procedure from a plethora of other requirements requiring supervisors' signatures.

The next phase of PASS research and development should include a pilot test to demonstrate its utility, determine the relative efficacy of paper and computer-based administration of the procedure, and inform implementation planning. Future research also could explore the differences between collective and individual certification of subordinates. This research could be done on a relatively small scale to minimize costs, but a well-designed pilot test would be essential for ensuring that DoD resources are used sensibly.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

BACKGROUND

The Department of Defense (DoD) employs an enormous workforce and relies on that workforce to secure and safeguard personnel, facilities, critical information, and other key aspects of its mission. Despite all of the measures taken by DoD to ensure the trustworthiness of the workforce, some individuals become vulnerable to adversaries and misuse that trust. The potential damage caused by disaffected insiders and external adversaries, including espionage, terrorism, and malicious cyberspace activity, may be reduced by timely reporting of security concerns to appropriate personnel. While it is every employee's responsibility to report potential threats, military and civilian supervisors must ensure that threats are recognized and reported at an early stage so that intervention will have a reasonable chance of success and minimize harm to national security. Unfortunately, threat indicators are not always reported as required by DoD policy.

The Defense Personnel Security Research Center (PERSEREC) developed a procedure called the Personal Acknowledgment of Staff Security (PASS) to increase supervisor[1] awareness, felt responsibility, accountability, and reporting of behaviors related to foreign intelligence entity (FIE) threats in accordance with Department of Defense Directive (DoDD) 5240.06, *Counterintelligence Awareness and Reporting (CIAR*), May 17, 2011 and component implementing policies (e.g., Army Regulation 381-12). The defining feature of the PASS procedure is the requirement of a signed certification by supervisors that they understand and intend to comply with reporting policy. Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make training and reporting requirements more salient and improve compliance (Shu, Gino, & Bazerman, 2011).

The present report provides background information and a concept of operations for the proposed PASS procedure. The first section discusses the significance of the insider threat, as well as underreporting of possible FIE threat indicators. The next major section provides an overview of training and reporting policy related to the proposed procedure. The third section explains the rationale for the procedure, to include underlying psychological concepts that are important for understanding how the procedure could be beneficial. Next, the research and development process is described with findings from stakeholder, subject matter expert, and supervisor interviews about the PASS concept. The fifth major section describes two different versions of the proposed procedure: paper and computer-based administration. Finally, the report concludes with a discussion of important considerations and recommendations.

[1] For the purposes of this document, "supervisors" are defined as personnel responsible for submitting official performance appraisals for one or more DoD military or civilian employees.

INSIDER THREAT

The proposed PASS procedure could be used to supplement existing awareness and reporting programs aimed at moderating the harm caused by current and former employees who threaten national security. DoDD 5240.06 defines a counterintelligence insider threat as "A person who uses their authorized access to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt operations, compromise DoD information or commit espionage on behalf of an FIE."[2] Most military, civilian, and contractor personnel with legitimate access to DoD facilities and information systems are trustworthy, reliable employees. However, there have been cases in which individuals have betrayed the trust that comes with government employment by committing acts of espionage, terrorism, or sabotage on behalf of FIEs. Others have committed similar acts in support of domestic entities or for personal reasons. These individuals may have been difficult to detect because they had authorized access to the information and other assets that were targeted for theft or harm. Trusted insiders motivated by greed, revenge, or divided loyalty, among other things, can be a significant threat to the department and its resources.

While trusted insiders are capable of causing serious damage and endangering lives, the scope of the problem is unclear based on available unclassified research. Respondents to the 2007 E-Crime Watch Survey (CSO Magazine, United States Secret Service, CERT® Coordination Center & Microsoft Corporation, 2007) reported that 51% of computer security incidents at their organizations were known or suspected to have been caused by insiders. However, a study by the Verizon RISK Team (2012) found that only 4% of corporate data thefts were perpetrated by employees in 2011. Nevertheless, the potential for causing significant harm is unparalleled among trusted insiders with bad intentions. Therefore, it is imperative that the DoD find ways to manage the risk.

UNDERREPORTING

While there are requirements for training and reporting, additional procedures are necessary to increase felt responsibility, accountability, and reporting of FIE and other serious threat indicators. DoD policy requires personnel to report to counterintelligence elements or other appropriate authority when a DoD employee exhibits behavior that could potentially harm national security or endanger lives (see DoDD 5240.06, 2011). However, previous research (Wood & Marshall-Mies, 2003) and anecdotal evidence indicates that there still may be obstacles to co-worker and supervisor reporting, and inadequate reporting can have devastating

[2] A more recent policy, Department of Defense Instruction (DoDI) 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat, May 4, 2012, defines an insider threat as "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities."

consequences. For example, the damage caused by the espionage activities of former Federal Bureau of Investigation (FBI) Supervisory Special Agent Robert Hanssen and the suspected perpetrator of the 2009 Fort Hood shootings may have been reduced had cognizant supervisors reported concerns to appropriate authorities (U.S. Department of Justice, 2003; Lieberman & Collins, 2011).

Reasons for not reporting include social norms against informing on co-workers, intrapersonal role conflict (Sims & Keon, 2000),[3] and a lack of transparency in the reporting process. For instance, co-workers and supervisors may not report security concerns as required because of a lack of clarity about the relationship between personal issues and personnel security (Wood & Marshall-Mies, 2003). Employees may believe it is not their responsibility to report "personal problems" to security or counterintelligence elements, and it is difficult to hold them accountable for failure to report undocumented concerns. The proposed procedure was designed to overcome some of these obstacles by raising awareness of behavioral indicators associated with FIE threats that may be exhibited by current and former employees, as well as by providing guidance about when and how to report relevant observations.[4] In addition, it was designed to encourage compliance with reporting policy by inducing cognitive dissonance (Festinger, 1957) in individuals who have observed but not reported FIE threat indicators. Cognitive dissonance is a state of psychological tension that occurs when attitudes are in conflict with behavior. 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.

TRAINING AND REPORTING

The DoD components conduct awareness training and employ a variety of reporting mechanisms to help counter FIE and other types of threats. The proposed PASS procedure is based on existing policy that requires training and reporting of observed threat indicators to appropriate authorities. This procedure could enhance current counterintelligence and force protection programs in a flexible, cost-effective manner. Policies and procedures that serve as the foundation for PASS are summarized in the following sections. First, key elements of DoDD 5240.06 are presented because the current version of the PASS procedure was designed to help implement this directive. Next, policy related to antiterrorism awareness training is summarized because the training could be used as a vehicle for administering the PASS procedure. Then, training and reporting methods are discussed to highlight important considerations related to PASS administration.

[3] Intrapersonal role conflict is the result of conflicting organizational expectations and employee values.

[4] The computer-based version of the procedure also could include a reporting mechanism to facilitate compliance.

BACKGROUND

DoDD 5240.06, Counterintelligence Awareness and Reporting

DoDD 5240.06 was issued based on the authority in DoDD 5143.01, *Under Secretary of Defense for Intelligence (USD[I])*, November 23, 2005. It determines policy, responsibilities, and procedures for CIAR in accordance with DoDD O-5240.02, *Counterintelligence*, December 30, 2010, and it applies to the DoD components, to include military, civilian, and appropriate contractor personnel. DoDD 5240.06 specifies reportable contacts, activities, indicators, and behaviors associated with FIE (see Tables 1 – 3 in Appendix A); it requires DoD personnel to report potential FIE threats; and it requires annual CIAR awareness training (Enclosure 3; see Appendix B).[5] DoD personnel must report threat information to their organization's counterintelligence element or supporting Military Department Counterintelligence Organization (MDCO). If counterintelligence support is not available, threats must be reported to a security officer, supervisor, or commander. Failure to report threat information as required in Enclosure 4 (see Appendix A) may result in judicial or administrative action, or both, pursuant to applicable law and regulations. Personnel subject to the Uniform Code of Military Justice (UCMJ) who violate the provisions of this directive may be subject to punitive action under Article 92, UCMJ. Civilian employees under their respective jurisdictions who violate these provisions may be subject to disciplinary action under regulations governing civilian employees.

Responsibility for CIAR is distributed to various components within the department. The USD(I) is responsible for monitoring implementation of DoDD 5240.06, as well as for providing direction and guidance as needed. The Deputy Undersecretary of Defense for Intelligence and Security (DUSD[I&S]) provides policy oversight of CIAR and recommends policy to the USD(I). Centralized management of CIAR and FIE threat analysis is the responsibility of the Director, Defense Intelligence Agency (DIA). Among other things, the Director, Defense Counterintelligence and Human Intelligence Center (DCHC) must coordinate, deconflict and centrally manage CIAR, and provide material support for DoD component CIAR training under the authority, direction, and control of the Director, DIA. The Director, Defense Security Service (DSS) responsibilities include providing CIAR assistance to cleared contractors. The heads of the DoD components must implement CIAR programs, provide material support to trainers, document participation in annual CIAR training, report FIE threats, and administer disciplinary action for failure to report FIE threats per this directive.

[5] CIAR training must be provided to DoD personnel by the components within 90 days of initial assignment/employment and annually thereafter. Training must be documented and the records maintained for 5 years, to include attendees, dates, and a summary of training content. This training should include instruction on FIE threats/methods, insider threat, and reporting requirements.

Antiterrorism Level I Awareness Training

DoDD 2000.12, *DoD Antiterrorism (AT) Program*, August 18, 2003 requires antiterrorism awareness training for all DoD personnel. Since there are existing computer-based antiterrorism awareness training modules, one option would be to administer the proposed PASS procedure in conjunction with online versions of this training requirement. Department of Defense Instruction (DoDI) 2000.16, *DoD Antiterrorism (AT) Standards*, October 2, 2006, Enclosure 3 prescribes a formal antiterrorism training program for the department. The most recent update was issued under the authority of DoDD 2000.12, to specify the minimum required elements of component antiterrorism programs, including risk management, planning, training, exercises, resource application, and program review. The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, under the Under Secretary of Defense for Policy is responsible for antiterrorism policy oversight and for monitoring compliance with this instruction. The DoD standard for formal antiterrorism training includes four levels: AT Awareness, AT Officer, Pre-Command AT, and AT Executive Seminar. The heads of the DoD components must ensure that all assigned personnel complete formal training as appropriate, and that completion is documented in individual records. In addition, they must ensure that all military, civilian, and other DoD direct-hire personnel complete Antiterrorism Level I Awareness Training at accession and annually post-accession.

Training and Reporting Methods

This section addresses some practical considerations related to how training and reporting requirements are implemented by the DoD components. Requirements from the Office of the Secretary of Defense are implemented by the DoD components, and implementation of DoDD 5240.06 may be based on component regulations that were written prior to the directive (i.e., they may be based on DoDI 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*, August 7, 2004). For instance, the Department of the Navy currently cites DoDI 5240.6 as the awareness training authority, and Secretary of the Navy (SECNAV) Instruction 3850.2C, *Department of the Navy Counterintelligence*, July 20, 2005, also may apply. Air Force Instruction 71-101 Volume 4, *Counterintelligence*, November 8, 2011 is the applicable Department of the Air Force policy, and Army Regulation 381-12, *Threat Awareness and Reporting Program*, 4 October 2010, is the associated implementing policy for the Department of the Army. Notably, threat indicators in component regulations may differ from those presented in DoDD 5240.06. However, this does not preclude implementation of the PASS procedure, as PASS could be modified to support similar programs within the DoD components. For example, the Army Threat Awareness and Reporting Program is a robust implementation with a slightly different set of behavioral indicators. Nevertheless, the PASS procedure could be tailored to support this program.

It also is noteworthy that CIAR and antiterrorism awareness training may be conducted in-person or online, and this has important implications for how the PASS procedure is designed and implemented within the components. DoDD 5240.06, Enclosure 3 requires the DoD components to provide CIAR training in a classroom environment by a person with counterintelligence experience. If experienced personnel are not available, a person familiar with CIAR may conduct the training, but the training materials must be reviewed by the organizational counterintelligence element or supporting MDCO. Nevertheless, CIAR training may be provided through other media when classroom training is not practicable. Similarly, annual Antiterrorism Level I Awareness Training may be provided by a qualified instructor or a DoD sponsored and certified computer-based program (e.g., https://atlevel1.dtic.mil/at/). Hence, the proposed PASS procedure probably would have to be developed for administration in both classroom and computer-based training environments.

A computer-based version of the PASS procedure could include functionality for reporting FIE threat indicators. Currently, threat information is reported by telephone, electronic mail, in-person, and online through component-specific suspicious activity reports. Examples include the

- Pentagon Force Protection Agency iWATCH online report (https://iwatchpfpa.org/page/iwatch/iwatchlogin.aspx?site=pfpa) and the Eagle Eyes program that employs email and telephonic reporting;
- Department of the Army iSALUTE counterintelligence reporting portal (https://www.inscom.army.mil/isalute/) and telephone hotline;
- Naval Criminal Investigative Service text, website (http://www.ncis.navy.mil/ContactUs/Pages/ReportaCrime.aspx), and smartphone application tip hotlines; as well as the
- Air Force Office of Special Investigations Eagle Eyes (http://www.osi.andrews.af.mil/eagleeyes/index.asp) and Crimebuster tips (http://www.osi.andrews.af.mil/library/factsheets/factsheet.asp?id=14522) programs.

The proposed procedure could include a separate reporting mechanism, or it could send information to an existing database(s).

CONCEPT DEVELOPMENT AND RESEARCH

The impetus for PASS came from relatively recent high-profile incidents that raised questions about accountability for reporting observable indicators of insider threats (e.g., the Fort Hood shootings and Wikileaks cases). Could these incidents have been avoided had the right people been notified ahead of time about the suspected perpetrators' questionable behavior? Even if the answer is "no" in these particular cases,[6] it is safe to assume that other trusted DoD insiders may be motivated to attack U.S. infrastructure, personnel, and sensitive information. Therefore, it is imperative that DoD personnel know their reporting responsibilities and make a commitment to report recognized indicators of FIE threats. Supervisors have additional responsibility for ensuring that threats are identified and reported in a timely manner, which is what the PASS procedure is designed to facilitate.

The PASS concept is related to procedures that some DoD components and foreign allies have used for periodic security assessments of employees in sensitive positions. These procedures typically require supervisors to conduct annual security appraisals for each of their subordinates. Their purpose is to enable identification and mitigation of security concerns before they become serious problems. Similarly, the original idea for PASS was to require supervisors to periodically evaluate each of their subordinates individually based on a list of behavioral indicators for a wide array of security and force protection concerns. However, even though they would have to consider each subordinate's behavior, the proposed PASS procedure would only require supervisors to submit a single annual certification for their subordinates as a group.

The domains of interest during the early stages of research included, among other things, espionage, terrorism, sabotage, self-radicalization, and workplace violence. The authors found adequate lists of indicators for most of the topics, but were convinced by subject matter experts to reduce the scope of concerns that the PASS procedure would address. Some experts felt that the proposed procedure could be more effective with a narrower focus. It also became apparent to the authors that the potential list(s) of indicators could become unreasonably large for supervisors to use as part of the procedure. Issuance of DoDD 5240.06 presented an opportunity to narrow the scope of PASS while still including some of the core concerns from the earlier concept. Moreover, DoDD 5240.06 included reasonable indicators and policy that the PASS procedure could help implement.

BEHAVIORAL INDICATORS AND PERIODIC SECURITY APPRAISALS

Initially, the authors conducted a literature review and spoke with subject matter experts to identify relevant policy, behavioral indicators, and initiatives designed to address insider threat detection and reporting. The original plan for PASS research

[6] Other factors surely contributed to these incidents, including improper or inadequate responses to reported concerns about the suspected perpetrators.

included discovery, generation, or improvement of behavioral indicators for conducting subordinate security appraisals. Lists of indicators were found for each of the original topics (e.g., espionage, terrorism, self radicalization, etc.), and then evaluated for use as part of the proposed procedure. The lists came from a variety of public and private unclassified sources. These sources included:

- Army Regulation 381-12, *Threat Awareness and Reporting Program*, 4 October 2010
- PERSEREC Technical Report 05-6, *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers*, May 2005
- DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*, August 7, 2004
- DoD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, May 17, 2011
- United States Department of Justice, Federal Bureau of Investigation (2002), *Workplace Violence: Issues in Response*
- Office of Personnel Management, *Dealing with Workplace Violence: A Guide for Agency Planners*, February 1998
- International Association of Chiefs of Police, *Combating Workplace Violence: Guidelines for Employers and Law Enforcement*, February 1, 1996.
- R.J. Heuer Jr., personal communication, (n.d.), *Preventing Violence.*
- R.J. Heuer Jr., personal communication, (n.d.), *List of Terrorism Indicators.*
- Sageman, M., *Behavioral Indicators of Concern: Radicalization and Terrorism*, April 1, 2011.
- New York Police Department, *Radicalization in the West: The Homegrown Threat*, 2007.

During the course of the study, several different approaches for implementing periodic security appraisals for military and civilian personnel also were considered. These included various approaches to violence risk assessment (Pressman, 2009; Campbell, French, & Gendreau, 2009; Storey, Gibas, Reeves, & Hart, 2011)[7] and employee screening tools designed to identify individuals who may engage in counterproductive work behavior or deception (developed by the United Kingdom [UK], Centre for the Protection of National Infrastructure). Most of these approaches require training and experience that may not be available to the majority of DoD supervisors, and they require more time to complete than what was envisioned for the PASS procedure. Nevertheless, some could be useful for secondary screening of personnel identified as potential threats, as well as with persons in sensitive

[7] There are several different approaches to violence risk assessment: unstructured clinical judgment, actuarial, and structured professional judgment. Most of the available assessment instruments were designed to be used in forensic mental health contexts (Storey et al., 2011). The Violent Extremist Risk Assessment (VERA; Pressman, 2009) is a structured professional judgment instrument that may be of interest to the DoD for evaluating potential insider threats.

positions (e.g., nuclear personnel reliability program, law enforcement, intelligence, etc.).

PSYCHOLOGICAL CONCEPTS FOR ENHANCING FELT RESPONSIBILITY AND ACCOUNTABILITY IN REPORTING

The proposed PASS procedure could enhance existing counterintelligence awareness and reporting programs by increasing felt responsibility[8] and accountability for reporting behaviors related to FIE threats in accordance with DoDD 5240.06. Research indicates that one of the most effective ways to encourage behavioral change in the workplace is through increasing autonomous motivation and felt responsibility (Gagné & Deci, 2005; Dose & Klimoski, 1995; Fuller, Marler, & Hester, 2006; Morrison & Phelps, 1999). Felt responsibility is fostered when accountability results in clear expectations, perceived control of the situation, and the perception that the desired behavior is important (Dose & Klimoski, 1995). 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 (Gagné & Deci, 2005). While manipulating perceived accountability will affect people differently, the procedure could result in more felt responsibility overall and potentially lead to increased reporting of threat indicators (Frink & Ferris, 1999).

Standard security training and awareness programs for DoD employees are usually information-based persuasive campaigns to help them recognize and appropriately address potential concerns. However, the effectiveness of these kinds of information campaigns is unclear (Dickerson, Thibodeau, Aronson, & Miller, 1992). Typically, DoD employees are relatively passive recipients of information even when there are follow-up questions as part of the training, and this is especially true with respect to their intent to comply with reporting policy. The proposed PASS procedure would require supervisors to actively acknowledge their understanding and intent to comply with the reporting requirements in DoDD 5240.06 by signing a certification. An active commitment to comply with regulations may result in more reporting because people want to be consistent and appear consistent to others (Cialdini, 2009). Personal consistency is valued within society, and being consistent 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 et al., 2011).

[8] Felt responsibility is when someone feels personally responsible for something as opposed to simply performing a role that entails that responsibility. For example, supervisory personnel may be expected to report certain things to counterintelligence elements, but a particular supervisor may not *feel* personally responsible for reporting his or her concerns.

Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make training and reporting requirements 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 when students in an experiment were required to sign their names after reading an honor code, dishonesty was virtually nonexistent in a task situation where cheating was possible. In contrast, some cheating still occurred when students were only asked to read the honor code (Shu et al., 2011). The action of signing one's name resulted in more compliance with the honor code than simply reading it. 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 would function as a commitment that a supervisor is making to uphold his/her responsibilities for reporting, and research indicates a higher likelihood that they will act in accordance with this commitment. 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 (Festinger, 1957; Aronson, 1992; Dickerson et al., 1992).

FIELD RESEARCH

Open-ended and semi-structured Interviews were conducted throughout the development process to gauge support for the PASS concept, identify related initiatives, and obtain feedback on the proposed procedure. The first round of interviews was conducted with potential stakeholders and subject matter experts for early conceptual development. The second set of interviews was done with a small sample of military and civilian supervisors to obtain feedback on key aspects of the procedure.

Stakeholder and Subject Matter Expert Interviews

The authors discussed different versions of the PASS concept with 46 subject matter experts and DoD policy personnel from the following United States and foreign organizations.[9] Initially, the authors contacted key stakeholders within OUSD(I) to discuss the project and to identify subject matter experts both within and outside the department. During the interviews, participants were asked to recommend other individuals with relevant expertise and/or potential interest in the proposed procedure. The authors then contacted these individuals and discussed the project with those who agreed to participate.

[9] Organizations are United States unless noted otherwise.

- Canadian Centre for Security and Intelligence Studies
- Centre for the Protection of National Infrastructure (UK)
- Defense Finance and Accounting Services
- Defense Intelligence Agency
- Department of Homeland Security
- DoD Insider Threat Working Group
- Federal Bureau of Investigation
- Foreign Policy Research Institute
- Global Skills X-Change
- Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs
- Office of the Under Secretary of Defense for Intelligence
- United States Air Force
- United States Army
- United States Marine Corps
- United States Navy

The purpose of the interviews varied to some extent depending on who was involved and at what point in the research process they were conducted. For instance, personnel at the FBI Behavioral Science Unit were interviewed relatively early in the study and at a time when one of the primary research tasks was to identify behavioral indicators and methods for detecting insider threats. Later in the study, security managers and counterintelligence special agents were interviewed to obtain feedback on different versions of the proposed procedure and recommendations for how it could be implemented. Some of the interviews were conducted as small group discussions of the proposed procedure, while others were done individually. Interviews were conducted in-person and by telephone. In most cases, the authors described the PASS concept and then asked participants for feedback and suggestions. Many of the discussions also addressed other related initiatives and procedures, especially in the early formative stages of the project. Typically, topics of discussion included reporting policy, reporting procedures, behavioral indicators, performance appraisal methods, accountability for reporting, security awareness training, and organizational culture. Interview notes were reviewed by the authors to identify relevant themes.

The overwhelming majority of participants were in favor of finding ways to improve awareness and reporting of potential threats. They also generally expressed interest in the proposed PASS procedure as a way to increase felt responsibility and accountability. Some of the challenges for PASS noted by participants were that behavioral indicators do not adequately capture the complexity of insider threat behavior; false positive reports by supervisors could harm employees' careers; there

may be resistance to the procedure by supervisors; and legal/privacy concerns will have to be addressed appropriately (e.g., data access restrictions, legal status of signatures, etc.).

Stakeholders and subject matter experts suggested additional considerations related to the proposed procedure. Several people mentioned that low base rates for espionage and terrorism may result in too many false positives. That is, there are so few spies and terrorists working for DoD that the vast majority of persons reported based on behavioral indicators actually would be innocent. Low base rates also make it difficult to develop empirically based actuarial prediction instruments for this type of threat assessment (Pressman, 2009). Therefore, it could adversely impact people who are reported, as well as overburden security and counterintelligence resources. Another suggestion was that unusual and suspicious behavior should be emphasized over specific behavioral indicators due to the complexity of human action (cf. Defense Science Board, 2012). This position advocates a more individualized, holistic approach to threat assessment to improve accuracy. On a related note, another group advised that other threat assessment methods may be useful in conjunction with the PASS procedure (e.g., structured professional judgment tools as follow-up to information reported by supervisors in the field). Also noteworthy, one participant proposed that awareness should be emphasized instead of compliance with reporting policy. Finally, there was some agreement that diffusion of responsibility is part of the problem with presumed underreporting.

Supervisor Interviews

Military and civilian supervisors were interviewed to obtain feedback on the DoDD 5240.06 version of the PASS procedure. The interviews were conducted at the Naval Postgraduate School (NPS) in Monterey, California. Participants were selected by the Chief of Staff, and the sample included 6 commissioned officers and 5 DoD civilian employees serving in faculty or staff positions at the school. The interviewer explained the proposed procedure and asked participants to review a paper and pencil version that consisted of a cover letter and a PASS certification form. The certification form consisted of brief instructions, three true/false statements, and a signature block.[10] Participants then were asked to provide their reactions (i.e., first impressions) to the materials and procedure. Lines of questioning were followed based on their initial responses. Additional questions asked of most participants included:

- What are the foreseeable benefits of the proposed procedure?
- What are some of your concerns about this procedure?
- How could the procedure be improved?
- Are you aware of other similar procedures? If so, how are they implemented?

[10] A more detailed description of PASS materials is presented in the next major section of this report.

The interviews were analyzed by identifying themes in the interviewer's field notes. As can be seen in Table 1, fourteen relevant themes were identified in the notes. Study participants are numbered from 1 to 11 in the table.[11]

Based on the explanation and materials provided by the interviewer, some study participants (55%) indicated that the PASS concept seemed similar to other procedures that require a signature (e.g., "Just another form to sign"), while other participants (36%) thought it was unique. A number of participants indicated that the proposed procedure seemed straightforward (36%), reasonable (18%), and potentially effective (36%). However, some felt that the potential impact of the procedure could be increased (45%) by either revising item number two (45%) or by providing real-world examples of incidents and their consequences (45%; e.g., "To get their attention," "Make them care"). It also was noted that the effectiveness of computer-based and paper versions of the procedure may be different (36%), and some participants thought that the paper version would be more effective (36%). In particular, signing a paper version of the certification form in the presence of others might have a bigger impact than signing it online (18%). Finally, some participants (45%) noted that individual differences, for example in conscientiousness, will affect the utility of the procedure, and others (18%) thought it might be advantageous to expand the proposed requirement to all employees (i.e., to encourage coworker reporting).

Table 1
Distribution of Themes from Supervisor Interviews

	Participant												
Theme	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Total**	**Percent**
Similar	1			1		1	1	1		1		6	55%
Unique		1			1				1		1	4	36%
Straightforward	1		1		1				1			4	36%
Reasonable	1	1										2	18%
Potentially effective	1	1	1		1							4	36%
Increase impact	1		1				1	1			1	5	45%
Revise item 2	1	1	1		1						1	5	45%
Real examples			1	1			1	1		1		5	45%
Versions different			1	1		1			1			4	36%
Paper more effective			1	1	1				1			4	36%
Signature context				1	1							2	18%
Individual differences			1		1			1	1	1		5	45%
Include coworkers									1		1	2	18%

[11] Note that stakeholder and subject matter expert interviews were not readily comparable because the interviews covered a wide range of topics at different points in the development process.

PROPOSED PASS PROCEDURE

The proposed PASS procedure will provide a mechanism to help implement DoDD 5240.06 and related programs by increasing felt responsibility and accountability for reporting potential FIE threats. The procedure would require DoD military and civilian supervisors to acknowledge familiarity with the reporting requirements in DoDD 5240.06, as well as their intent to report observed indicators. Based on the strengths and weaknesses of the approaches considered for this study, the authors recommend linking PASS with an annual security-training requirement (e.g., Antiterrorism Level I Awareness Training). It is likely that this approach can be adopted with less resistance than the others that were considered (e.g., making PASS part of annual performance appraisals), and it also has the benefit of reinforcing training through immediate application to supervisory duties. The remainder of this report will describe the PASS procedure in conjunction with security awareness training. However, this should not preclude making it part of some other process, if necessary.

Initially, the PASS concept required supervisors to complete separate certifications for each of their subordinates, and one idea was to make the procedure part of annual performance appraisals. This approach could potentially prompt supervisors to consider each of their subordinates individually with respect to the FIE indicators in DoDD 5240.06, and go on record as to whether or not they are aware of relevant security concerns. Whereas this is still a viable option, individual certification of subordinates as part of the performance appraisal process would be more laborious for supervisors than collective certification[12] in conjunction with annual security awareness training. Moreover, linking the PASS procedure with training might make certain aspects of the training more salient to participants (e.g., reporting observed indicators). Thus, the authors recommend testing collective certification in conjunction with the security training approach.

The PASS procedure could provide an additional mechanism for reporting threat information to appropriate authorities depending on the medium used for implementation (i.e., paper versus computer-based form submission). A paper and pencil version of the procedure would further encourage supervisors to report relevant observations by contacting a local counterintelligence element or security manager. Computer-based implementation, on the other hand, could provide encouragement as well as include a module for immediate online reporting. The pros and cons of these approaches will be discussed below. Note, however, that the relative efficacy of the two approaches has not been determined. It is unclear whether or not a digital signature would have the same effect as a hard signature, or if other aspects of the procedures would affect the desired outcomes. During the interviews, several supervisors suggested that there could be important differences

[12] One of the implementation options discussed below is to require supervisors to submit one PASS form annually for their subordinates as a group, instead of submitting a separate form for each individual.

between paper and pencil and computer-based administration. For example, one interviewee said that the proposed procedure might be more effective coupled with in-person training, and if supervisors were required to sign the certification with their superior or security manager present. Part of the solution may be to differentiate the PASS procedure from all of the other things that supervisors sign. Additional research is necessary to resolve this issue.

The proposed procedure is intended to be used with military and civilian supervisors, but it could be required of all DoD personnel. The original proposal was to limit the PASS requirement to supervisory personnel because the idea was for supervisors to submit a form for each subordinate indicating whether or not they have exhibited indicators of security concern (individual certification of subordinates is still an option). In addition, while all personnel are responsible for reporting the indicators in DoDD 5240.06, persons in supervisory positions have added responsibility for ensuring that subordinates comply with policy to safeguard national security. Supervisors should be accountable for reporting relevant information that comes to their attention even though they may not always be in the best position to directly observe behavioral indicators in their subordinates. Moreover, supervisors are in a position to encourage others to report per DoD policy. In any case, the PASS procedure could be expanded to additional personnel upon successful implementation with supervisors.

BASIC PROCEDURE

There are two predominant methods of security awareness training: computer-based training and in-person training by experienced counterintelligence instructors. The proposed procedure would have to work in both contexts because components implement training requirements differently (i.e., some use computer-based training while others provide training in-person). The PASS procedure could be part of an annual, online security training application or some other annual requirement, but it also could be deployed as a stand-alone web application or paper form in conjunction with in-person security awareness training. Figure 1 shows three options for administering the procedure with different training scenarios.

After completing the training, supervisors[13] would be directed to another computer-based module or given a paper form that reiterates their reporting responsibilities, and they would be asked to respond to the following three items (Yes/No)[14] regardless of administration format:

(1) I am familiar with DoDD 5240.06, and I understand my reporting responsibilities per this directive.

[13] Personnel are considered supervisors if they complete official annual performance appraisals for one or more subordinates.
[14] Item response options were changed from True/False to Yes/No based on reviewer feedback.

(2) I am aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5 for one or more of my subordinates.

(3) If I become aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5, I will report them in accordance with policy.

Supervisors who select 'No' for item 1, 'Yes' for item 2, or 'No' for item 3 would be required to perform the following corresponding actions:

(1) Review a copy of DoDD 5240.06 (or an official summary with indicators) and become familiar with its requirements prior to submitting the certification;

(2) Report relevant observations and concerns to the appropriate counterintelligence element or security manager;

(3) Prior to submitting the certification, explain why he/she does not intend to report in accordance with policy.

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

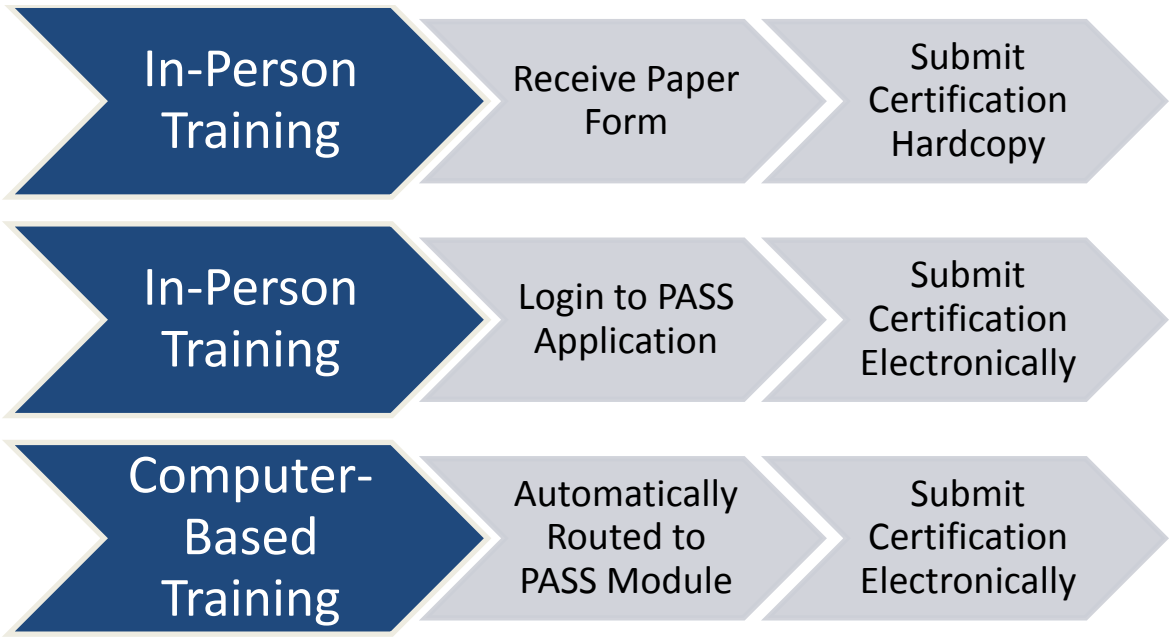

Figure 1 Overview of Options for Proposed Procedure with Different Training Scenarios

PAPER VERSION

A paper version of the PASS form and supporting materials could be used in conjunction with in-person security awareness training, as described below.

Materials

The paper and pencil version of this procedure should include a cover letter, copy of DoDD 5240.06 Enclosure 4, and certification form. The cover letter will be used to explain the procedure and to convey the importance of knowing and reporting behavioral indicators of espionage, terrorism, and malicious cyberspace activity. Based on interviews with supervisors, the cover letter should include an example(s) of a real incident that may have been prevented or moderated by timely reporting. The cover letter must get supervisors' attention and make them care about knowing their responsibilities and signing the form. A sample cover letter is shown in Appendix A. The cover letter could be based on a template and modified to suit local demands, or it could be a standard document from an Office of the Secretary of Defense (OSD) element (e.g., OUSD[I]). A modifiable template would enable local customization of elements such as senders' addresses, instructions for reporting, and local command authority.

Additionally, the procedure should include a copy of DoDD 5240.06, Enclosure 4 (see Appendix B). Inclusion of the enclosure would allow supervisors to complete the procedure without having to obtain the directive and read it in its entirety. Enclosure 4 specifies reporting requirements; consequences for failure to report observed indicators of FIE threats; and the indicators that must be reported. DoD

personnel are required to report potential FIE threats to their organization's counterintelligence element or supporting MDCO. If counterintelligence support is unavailable, they must report threats to their security officer, supervisor, or commander. Failure to report in accordance with this directive may result in judicial or administrative action, or both. Enclosure 4, tables 1 through 3 present reportable contacts, activities, indicators, and behaviors associated with FIEs. The information in these tables must be emphasized because the indicators are a fundamental part of the procedure.

The procedure also includes a paper certification form for supervisors to acknowledge their responsibilities and willingness to report relevant behavioral indicators. The paper version of the PASS certification is shown in Figure 2. As can be seen in the figure, the paper form consists of brief instructions, three Yes/No items, as well as a section for signature and contact information. Each Yes/No item is accompanied by instructions for certain responses. If 'No' is selected for the first item, the supervisor is instructed to become familiar with the reporting requirements in DoDD 5240.06. If a supervisor selects 'Yes' for the second item, he or she is informed that they will be contacted by counterintelligence or security personnel to discuss their observations. If 'No' is selected for the third item, the supervisor must explain in writing why he or she does not intend to comply with DoD policy. The certification form may be completed electronically, but the signature must be hand written.

DoD Form 00
Revised July 2012
U.S. Department of Defense
Policy Citation

PERSONAL ACKNOWLEDGMENT OF STAFF SECURITY (PASS)

Form approved:
OMB No. 0000 0000
NSN 0000-00 000-0000
00-000

Instructions. Please respond (Yes or No) to the following three items concerning Department of Defense Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, May 17, 2011, sign and date, provide contact information, and submit this form to your security management office. Note that failure to report foreign intelligence entity threats as identified in paragraph 3.a and section 5 of Enclosure 4 of this Directive may result in judicial or administrative action or both pursuant to applicable law or policy.

	I certify the following:	**Yes**	**No**
1.	I am familiar with DoDD 5240.06, and I understand my reporting responsibilities per this directive. ➢ If you selected 'No' for item number 1, please review DoDD 5240.06 (or an official summary with indicators) and become familiar with your reporting responsibilities. The directive is available in its entirety (19 pages) at www.dtic.mil/whs/directives/corres/pdf/524006p.pdf.	☐	☐
2.	I am aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5 for one or more of my subordinates. ➢ If you selected 'Yes' for item number 2, local counterintelligence or security personnel will contact you to discuss your observations.	☐	☐
3.	If I become aware of reportable contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5, I will report them in accordance with policy. ➢ If you selected 'No' for item number 3, please explain below why you do not intend to report contacts, activities, indicators, or behaviors listed in DoDD 5240.06, Enclosure 4, section 5 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. Work Telephone Click here to enter text.	**9. Email Address** Click here to enter text.

Figure 2 Paper Version of the PASS Form

Procedure

The paper version of the PASS procedure could accompany in-person Antiterrorism Level I Awareness Training or training associated with the Department of the Army Threat Awareness and Reporting Program (TARP), for example. Immediately following training, the PASS materials would be distributed to supervisors by the trainer, security manager, or superior in their chain of command. Supervisors would be asked to review the materials and to complete and sign the attached certification. Ideally, certifications would be signed in the presence of one of the aforementioned officials to help convey the importance of recognizing and reporting potential FIE threats. This also could strengthen the procedure by making the signature more of a public commitment.

Signed PASS certifications would be given to the command security manager for review and storage. Certifications with the "expected" response pattern (i.e., Yes, No, Yes) would be filed by the command security manager with no further action necessary. Copies of certifications with 'Yes' responses to item 2 would be forwarded to an appropriate counterintelligence element for further examination (e.g., contacting the supervisor to acquire additional information about his or her observations). The command security manager would follow-up with personnel who indicate 'No' for item 2 and 'No' for items 1 and/or 3 on the form to encourage awareness and compliance with DoD reporting policy. A flowchart of this process is shown in Figure 3.

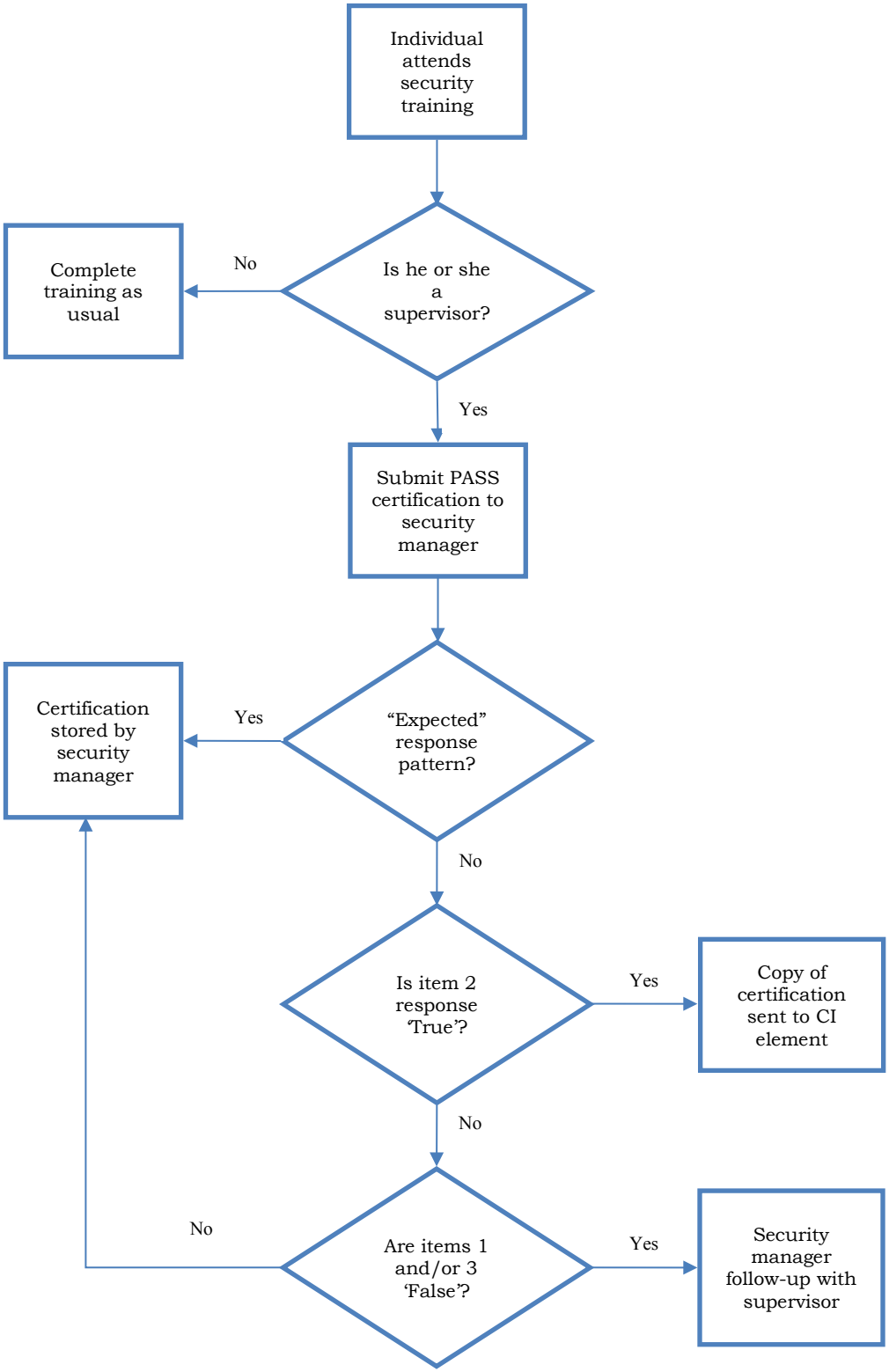

Figure 3 Flowchart Depicting Paper Version of the PASS Procedure

Pros and Cons

A paper and pencil version of the PASS procedure could be a relatively decentralized, flexible, low-tech approach. It may be less expensive and more effective than a computer-based approach, depending on how it is implemented in the field. It also may be possible to implement more quickly than a computer version of the procedure. However, this approach would not take full advantage of information technology resources for data collection and management. It also may be more of a burden for local security mangers to administer.

COMPUTER VERSION

Assuming the collected information is unclassified, the proposed PASS procedure could be incorporated as a module into existing online security awareness training (e.g., Antiterrorism Level I Awareness Training, https://atlevel1.dtic.mil/at/). It also could be operated as a standalone web application on a secure Non-classified Internet Protocol Router Network (NIPRNet)[15] server in conjunction with in-person security awareness training. The PASS procedure would be administered by command security managers. The web application could be operated and maintained by the host of the training application or another DoD element with web hosting capability.

Computer-Based Security Awareness Training Module

A PASS module could be deployed as part of an existing security awareness training application. In this scenario, command security managers would submit the names of personnel required to complete PASS certifications prior to annual online training. Command security managers would be responsible for ensuring that supervisors submit an annual certification that they are familiar with the directive and that they intend to comply with its reporting requirements. Supervisors would complete the training and then be routed automatically to the PASS module. In addition to submitting a certification, this version of the procedure could allow users to electronically report indicators of potential FIE threats directly to a counterintelligence database. Reporting functionality could be an integral part of the proposed system, or the PASS system could be designed to forward reports to an external counterintelligence system. Users would receive a certificate of completion for the training after they submit the PASS certification. The command security manager would have a PASS module account to monitor compliance and to address reported security concerns, as appropriate.

As shown in Figure 4, the basic steps for a module deployed with computer-based security awareness training are as follows:

[15] The NIPRNet is also known as the Sensitive But Unclassified IP Data service (see http://www.disa.mil/Services/Network-Services/Data/SBU-IP for more information).

(1) The command security manager submits a list of supervisors to the security awareness training application.

(2) Supervisors login and complete online security awareness training.

(3) Upon completion, the security awareness training application automatically routes supervisors to the PASS module where they submit a digitally signed certification. The module notifies the training application upon submission, and supervisors are routed to a confirmation page.

(4) Certifications that include reported FIE contacts, activities, indicators, or behaviors are automatically sent to a local counterintelligence (CI) element or other appropriate authority.

(5) The PASS module automatically notifies the security manager when certifications are submitted, and the security manager ensures procedural compliance.

(6) The completion certificate for security awareness training is available for the supervisor to download and save.

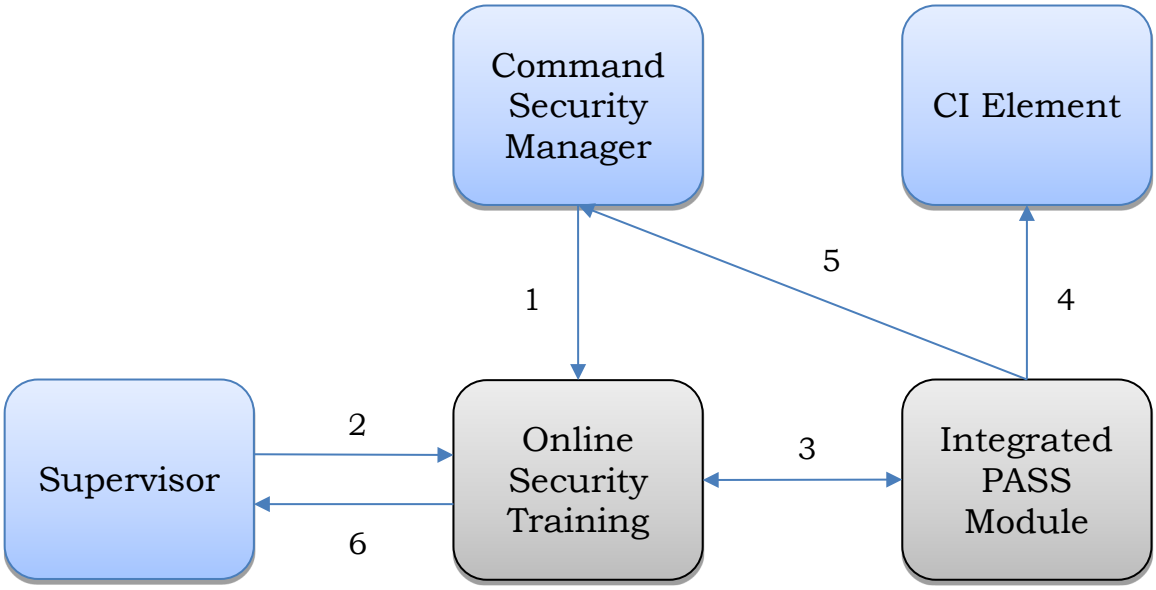

Figure 4 Proposed Computer-Based Training Module Procedure

Stand-Alone Web Application

The PASS procedure could be administered by command security managers through a stand-alone web application in conjunction with in-person security awareness training. An overview of the proposed procedure is shown in Figure 5. The security manager would have a PASS account to monitor compliance with this

requirement. In addition to submitting certifications, supervisors also would be able to report possible FIE threats as part of the proposed annual procedure and as they become aware of indicators at other times. Security managers will monitor compliance and ensure that reported security concerns are forwarded to counterintelligence elements. The basic steps for a stand-alone web application are as follows:

(1) The command security manager submits a list of supervisors to the PASS application.

(2) The application automatically notifies supervisors that they must submit a PASS certification upon completion of security awareness training.

(3) Supervisors receive security awareness training from an instructor.

(4) Supervisors login to the PASS application and submit a digitally signed certification.

(5) Certifications that include reported FIE contacts, activities, indicators, or behaviors are automatically sent to a local counterintelligence element or other appropriate authority.

(6) The PASS application automatically notifies the security manager when certifications are submitted, and the security manager ensures procedural compliance.

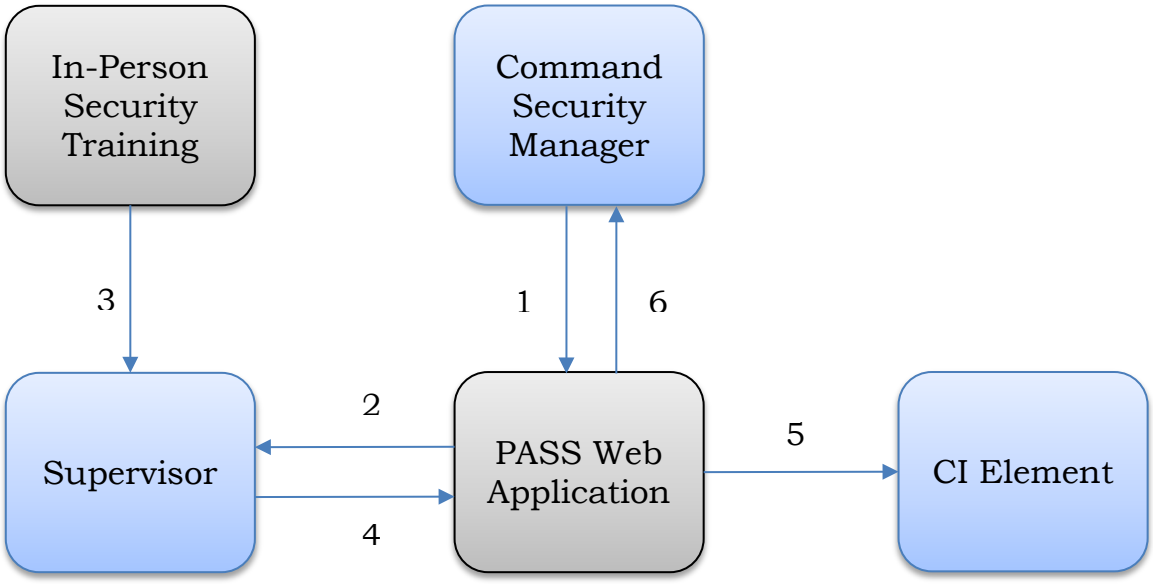

Figure 5 Proposed Stand-Alone Web Application Procedure in Conjunction with In-Person Security Awareness Training

One of the commands that participated in this study serves as an example of how a stand-alone web application could work in conjunction with in-person security awareness training. This command uses a pair of software applications (i.e., administration and attendance confirmation) to verify attendance at events and presentations. The system works by generating a set of random codes that are distributed on small cards to attendees at the end of events. Attendees enter the code by way of local intranet to confirm their attendance. The event administrator can export the data at any time and print materials using mail merge. The system only accepts a single registration for each code and rejects any additional attempts to register using that code. It also leverages users' domain credentials to identify who is registering. If supervisors were identified in advance by the security manager, the event attendance software could automatically route supervisors to a PASS module or separate stand-alone application. The security manager then could generate a PASS user log to ensure compliance with the certification requirement.

Application Prototype Design

This section presents an outline of the prototype design for the PASS application (see Figure 6), as well as sample pages for a web application. Each of the boxes in Figure 6 represents a page from the proposed PASS application. As can be seen in the figure, users begin at the 'Authentication' page.[16] Upon successful authentication, all users automatically are routed to the 'Home' page. From the 'Home' page, users with application administration privileges would have access to a menu of administrative functions depending on their role. For example, security managers would be able to input authorized user lists and generate user logs for their commands. Site administrators would be able to perform maintenance tasks. All other users would go from the 'Home' page to an 'Instructions' page by clicking the 'Next' button.

Clicking the 'Next' button on the 'Instructions' page takes users to the 'Certification' page. The three core items on this page require a yes or no response. Certain responses to each item automatically route users to a different page for follow-up. When users complete the required follow-up actions, they return to the 'Certification' page. Selecting 'No' for the first statement automatically routes users to a directive review page. The directive review page provides a synopsis and link to DoDD 5240.06, a link to reportable indicators, and navigation buttons. Users who reach this page would be able to review the directive, as well as navigate to another page to explain what they do not understand about their reporting responsibilities. Users selecting 'Yes' for the second statement on the 'Certification' page would automatically be redirected to the 'Subordinate Information' page to report their observations. This page requests subordinate name, identification number, and remarks. It also contains links to foreign intelligence, international terrorism, and cyberspace pages for users to select relevant indicators. Users may submit as many reports as necessary. Users who select 'No' for the third statement on the

[16] Authentication helps ensure that only authorized users access the application.

'Certification' page would automatically be routed to another page to explain why they are unable to comply with the directive.

Ultimately, all users would be required to provide the requested information on the 'Certification' page to complete the procedure. Users who select 'Yes,' 'No,' 'Yes' for items one, two, and three respectively as well as provide the additional requested information (i.e., name, grade/rank, telephone number, and email address) would be able to submit the certification without redirection to other pages. A 'Confirmation' page will appear upon successful form submission. Figure 7 through Figure 19 show notional designs for the pages that make up the prototype PASS application.

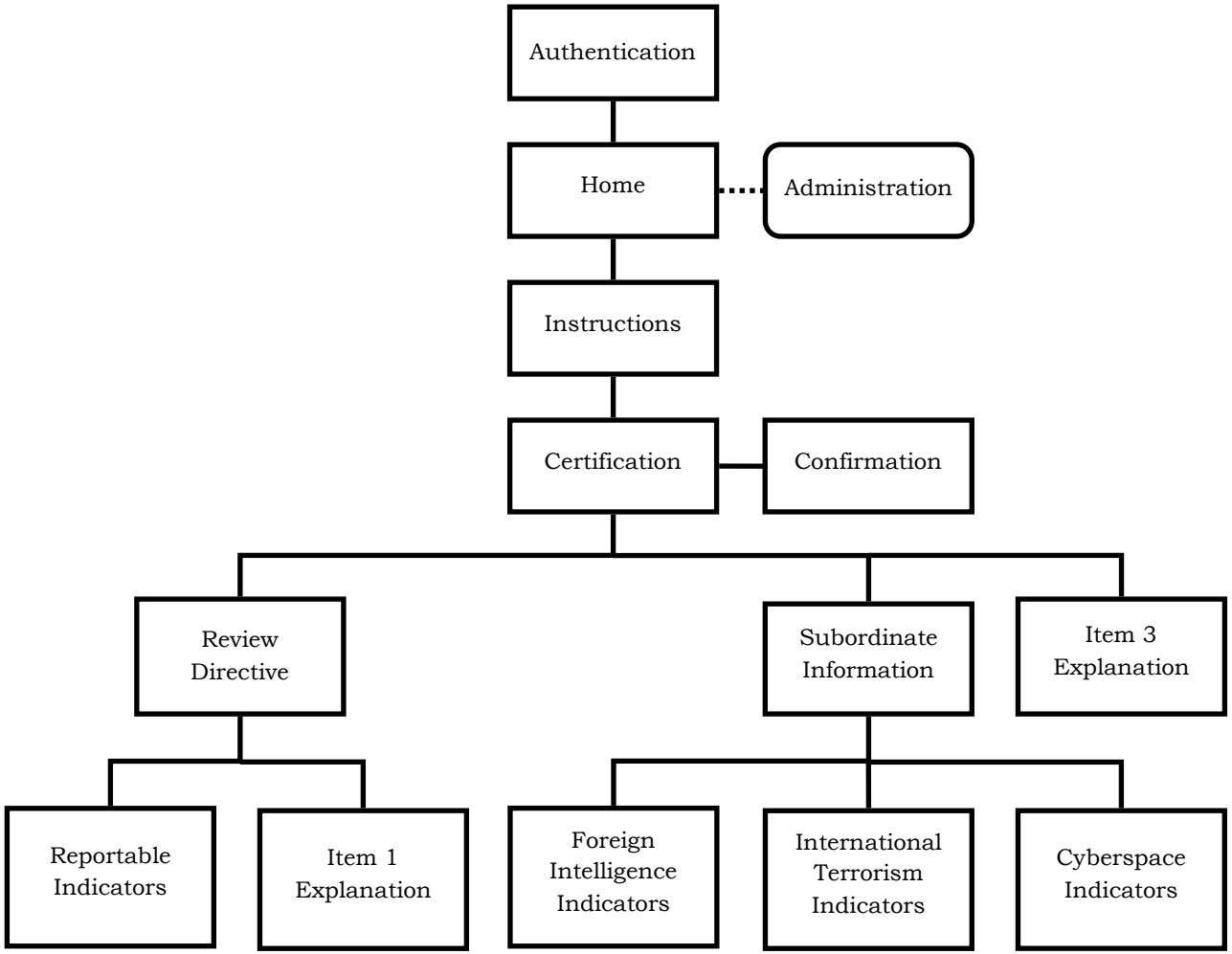

Figure 6 PASS Application Prototype Design

Figure 7 shows the 'Authentication' page for the prototype application. In the stand-alone version, users would login to the PASS application with a DoD approved PKI credential (e.g., Common Access Card) or username and password.

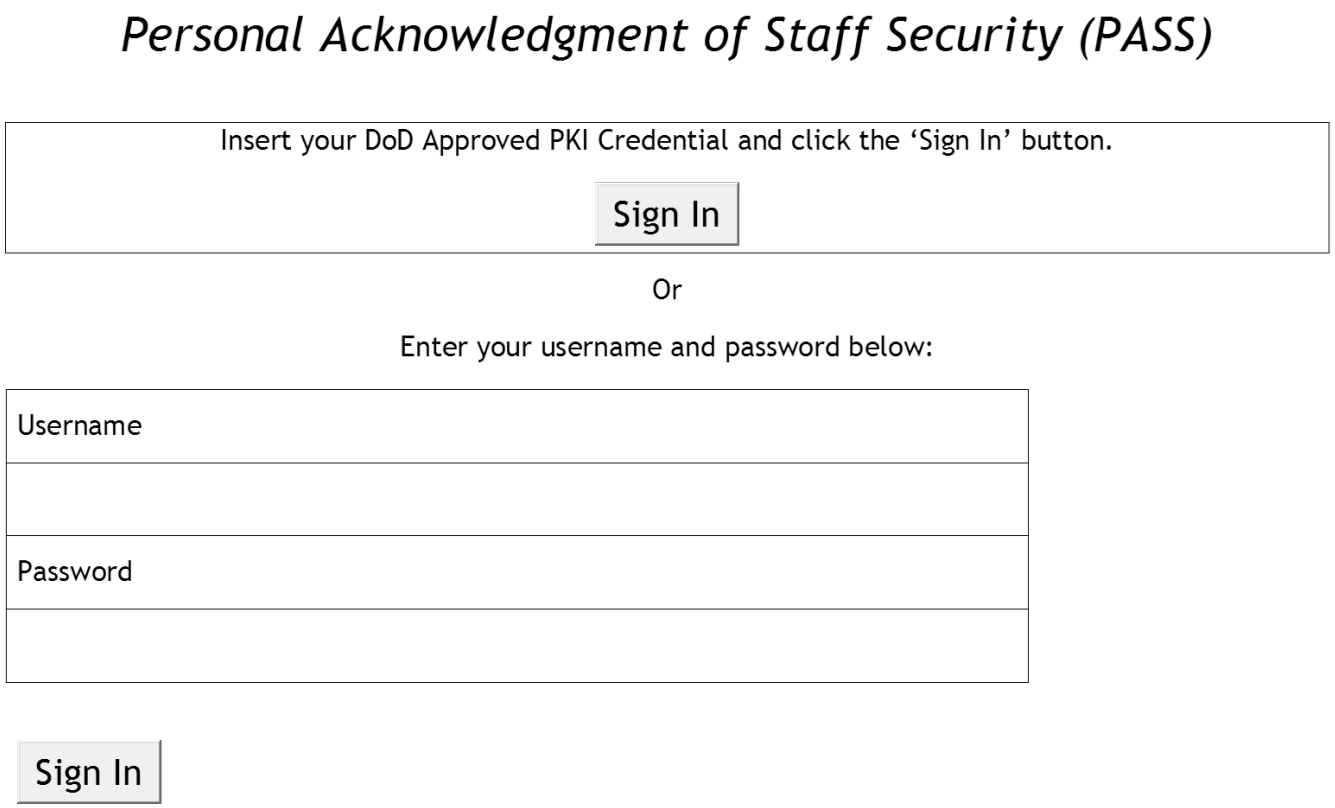

Figure 7 Authentication Page

Figure 8 shows the 'Home' page. All users begin the PASS procedure at the home page. The home page will contain a brief introduction, a link to a downloadable copy of DoDD 5240.06, links to other relevant web sites, and navigation buttons.

Figure 8 Home Page

Figure 9 shows the 'Instructions' page. The instructions page will explain the necessary steps to complete the PASS procedure. This page also will contain a link to the home page as well as navigation buttons. All users will view this page to complete the procedure.

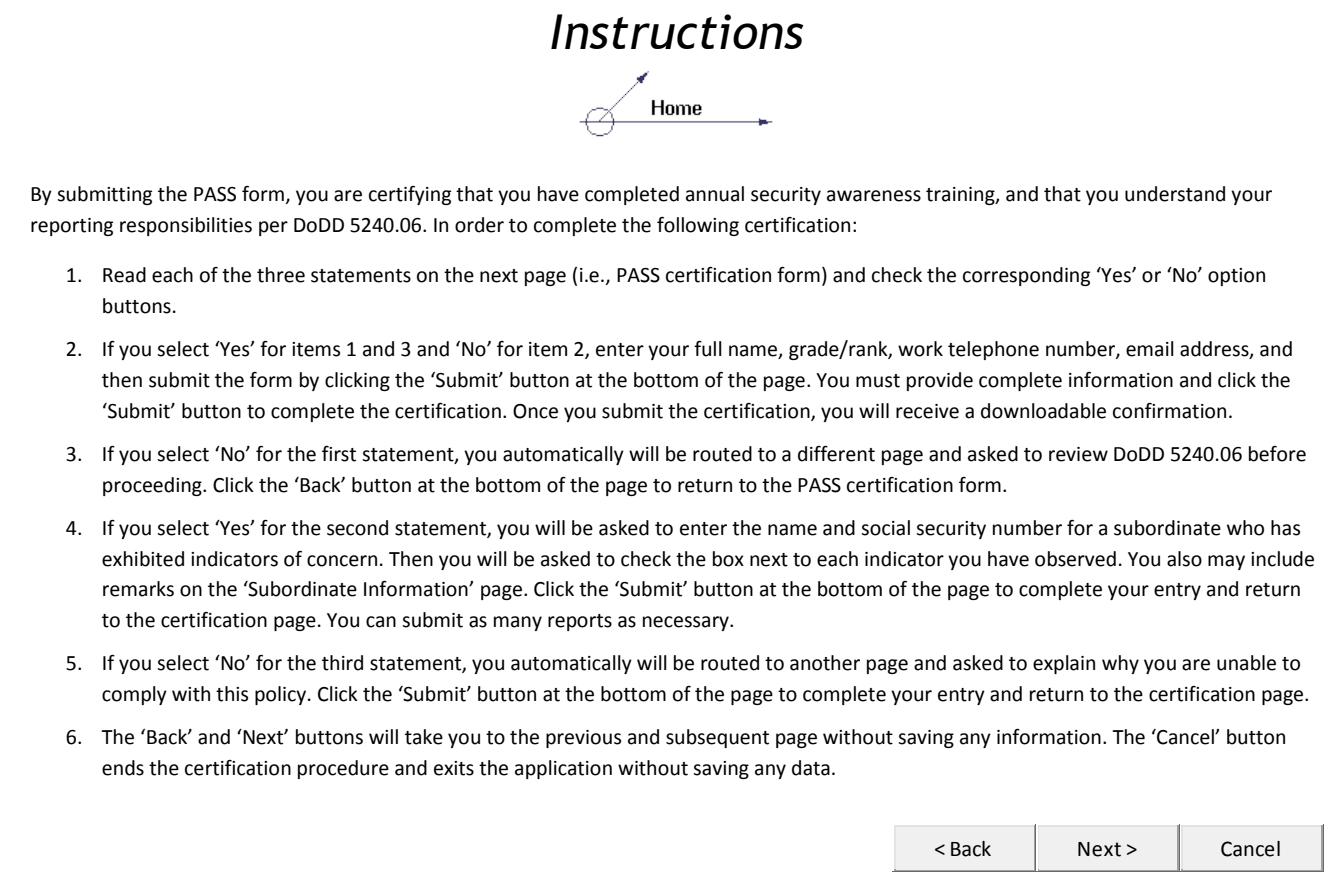

Figure 9 Instructions Page

As shown in Figure 10, the 'Certification' page will contain three statements for which users must respond either 'Yes' or 'No'. Only one response per statement will be possible, and all fields must have a response prior to form submission. The page includes links to a downloadable copy of DoDD 5240.06, a summary of reportable indicators, and navigation buttons. Users may automatically be redirected to another page based on their responses to the Yes/No items on this page.

Figure 10 Certification Page

Figure 11 shows the 'Review Directive' page. This page will be accessible from the 'Certification' page, and users who select 'No' for item one will automatically be routed to this page prior to form submission. The purpose of this page is to help users understand their reporting responsibilities.

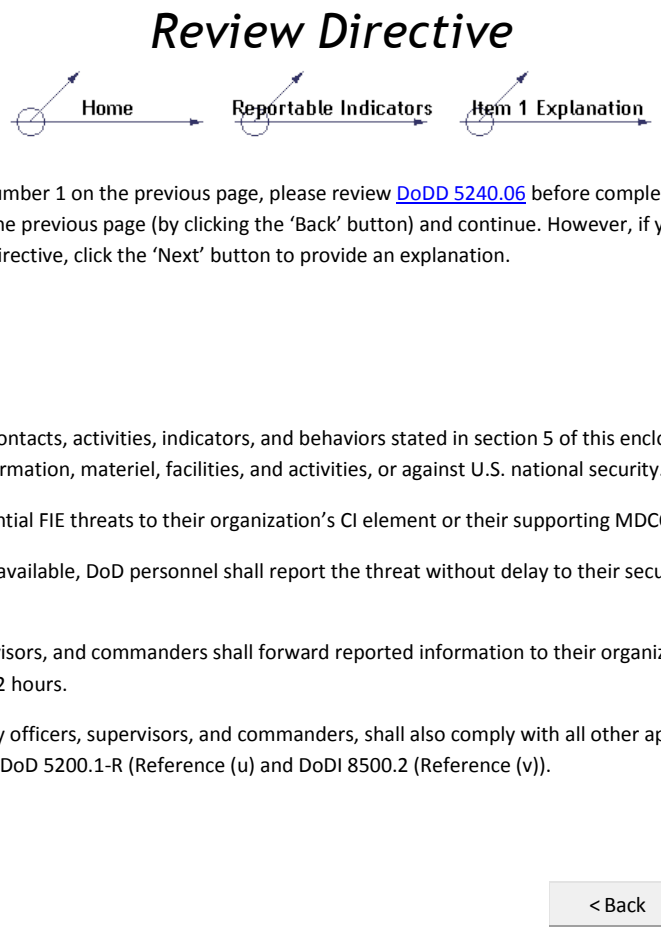

Figure 11 Review Directive Page

Figure 12 shows a *truncated* version of the 'Reportable Indicators' page. This page is accessible from the 'Certification' and 'Review Directive' pages. Its purpose is to help users understand what to report.

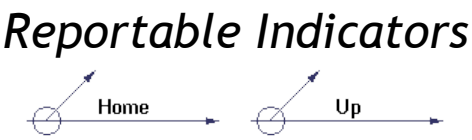

Figure 12 Reportable Indicators Page

The 'Item 1 Explanation' page shown in Figure 13 is required for users who wish to submit the PASS certification with a 'No' response to item one. Users may access this page from the 'Review Directive' page.

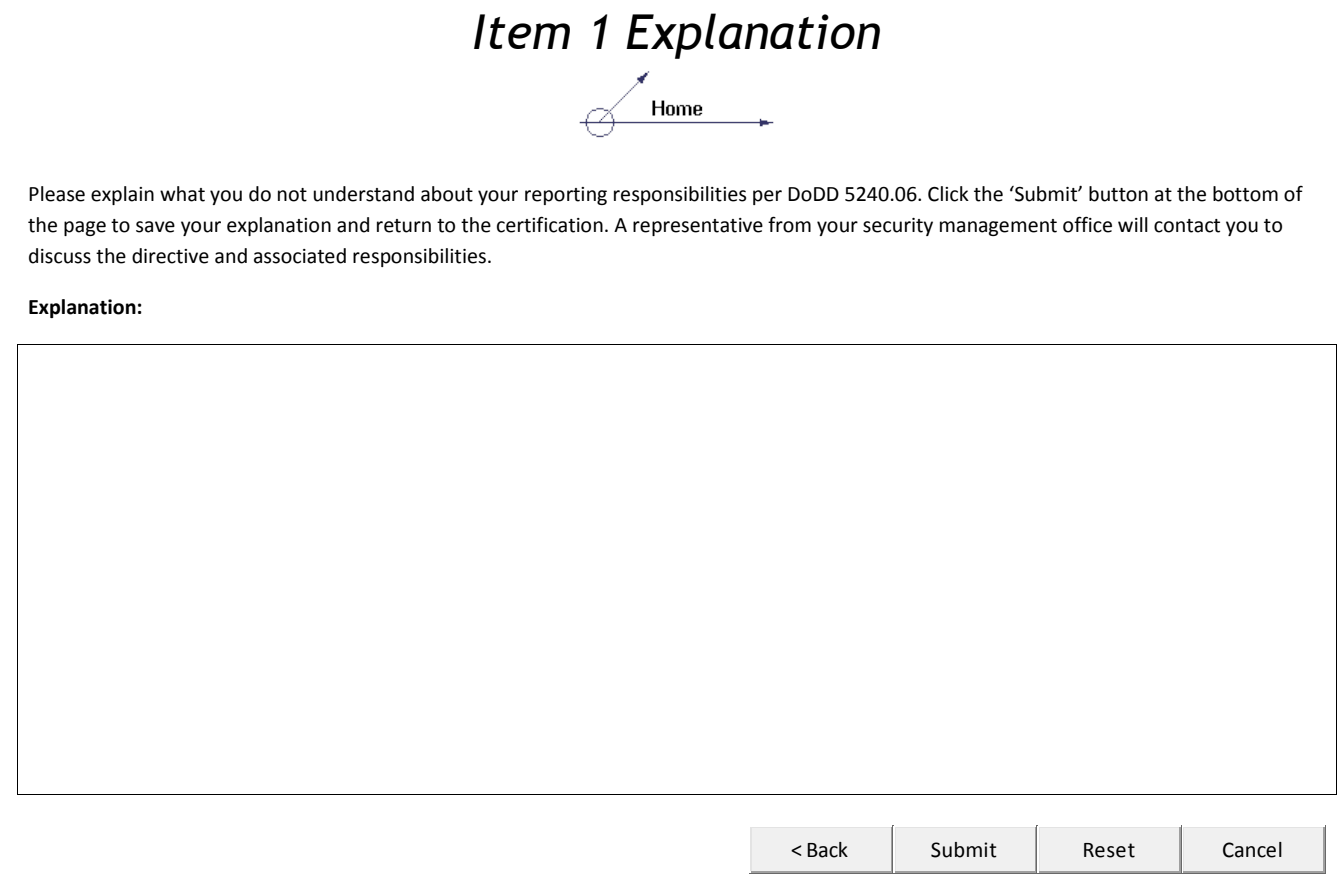

Figure 13 Item 1 Explanation Page

Users are routed to the 'Subordinate Information' page if they select 'Yes' for item two on the 'Certification' page. This page is for reporting relevant observations of individual subordinates.

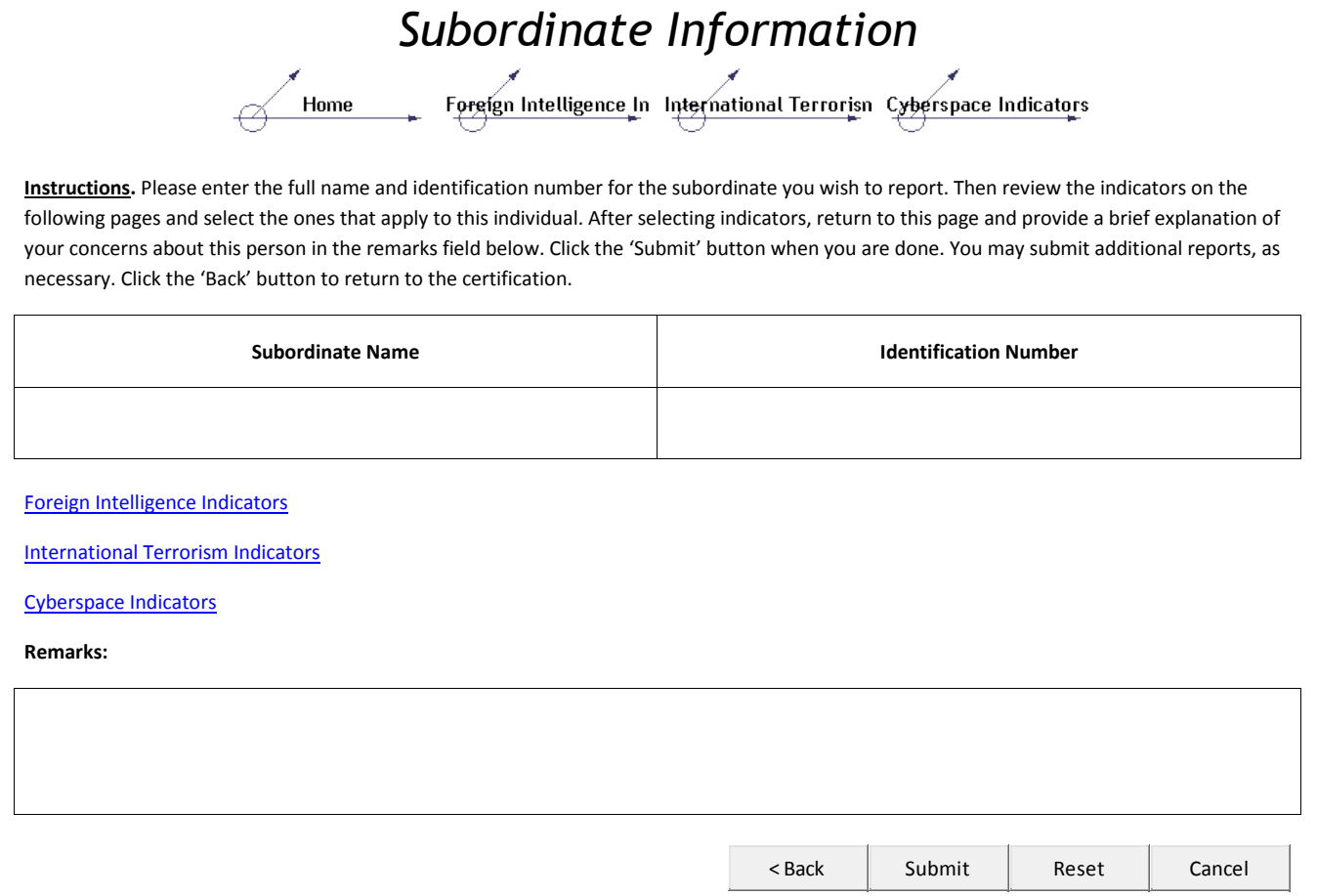

Figure 14 Subordinate Information Page

A *truncated* version of the 'Foreign Intelligence Indicators' page is shown in Figure 15. This page is accessible from the 'Subordinate Information' page. Indicators selected on this page become part of a report to counterintelligence elements.

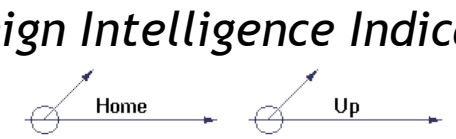

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors Select all that apply (Click the 'Up' link to return to the 'Subordinate Information' page):	
☐	1. When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.
☐	2. Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
☐	3. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
☐	4. Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
☐	5. Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
☐	6. Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
☐	7. Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
☐	8. Discovery of suspected listening or surveillance devices in classified or secure areas.
☐	9. Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
☐	10. Discussions of classified information over a non-secure communication device.
☐	11. Reading or discussing classified or sensitive information in a location where such activity is not permitted.
☐	12. Transmitting or transporting classified information by unsecured or unauthorized means.

Figure 15 Foreign Intelligence Indicators Page

A *truncated* version of the 'International Terrorism Indicators' page is shown in Figure 16. This page is accessible from the 'Subordinate Information' page. Indicators selected on this page become part of a report to counterintelligence elements.

International Terrorism Indicators

Reportable Contacts, Activities, Indicators, and Behaviors from DoDD 5240.06, Enclosure 4, Section 5

Table 2. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors Select all that apply (Click the 'Up' link to return to the 'Subordinate Information' page):	
☐	1. Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
☐	2. Advocating support for a known or suspected international terrorist organizations or objectives.
☐	3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
☐	4. Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
☐	5. Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
☐	6. Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
☐	7. Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
☐	8. Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
☐	9. Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
☐	10. Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

Figure 16 International Terrorism Indicators Page

A *truncated* version of the 'Cyberspace Indicators' page is shown in Figure 17. This page is accessible from the 'Subordinate Information' page. Indicators selected on this page become part of a report to counterintelligence elements.

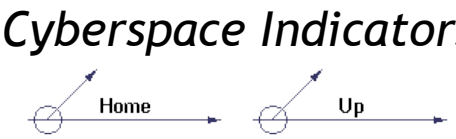

Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors Select all that apply (Click the 'Up' link to return to the 'Subordinate Information' page):	
☐	1. Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
☐	2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
☐	3. Network spillage incidents or information compromise.
☐	4. Use of DoD account credentials by unauthorized parties.
☐	5. Tampering with or introducing unauthorized elements into information systems.
☐	6. Unauthorized downloads or uploads of sensitive data.
☐	7. Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
☐	8. Downloading or installing non-approved computer applications.
☐	9. Unauthorized network access.
☐	10. Unauthorized e-mail traffic to foreign destinations.
☐	11. Denial of service attacks or suspicious network communications failures.
☐	12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
☐	13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
☐	14. Data exfiltrated to unauthorized domains.
☐	15. Unexplained storage of encrypted data.

Figure 17 Cyberspace Indicators Page

The 'Item 3 Explanation' page shown in Figure 18 is required for users who wish to submit the PASS certification with a 'No' response to item three. Users who select 'No' for item three will be routed to this page from the 'Certification' page.

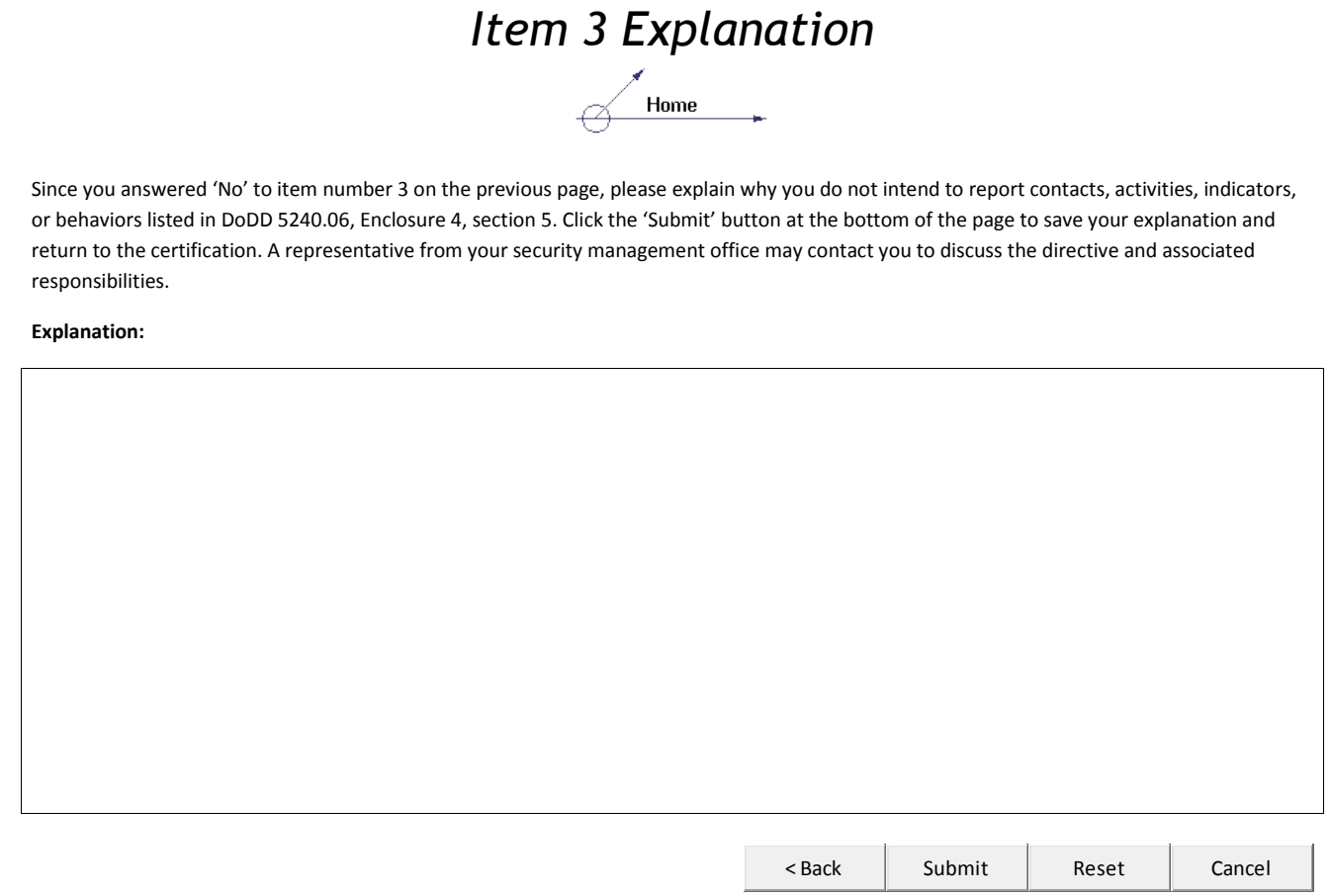

Figure 18 Item 3 Explanation Page

Upon successful submission of a PASS certification, users will be routed to a 'Confirmation' page (Figure 19) that includes their name and date of completion.

Figure 19 Confirmation Page

Pros and Cons

The potential benefits of a computer-based PASS procedure include the possibility of central data storage, relatively efficient data management and analysis capability, and reduced burden for local security managers compared to a paper version of the procedure.

There are several potential disadvantages of computer-based administration. First, software development and maintenance costs would be relatively expensive. Second, it would be relatively difficult to customize the procedure for local conditions. For example, some commands may wish to modify information flow to better meet their needs, which would require more resources than modifying a paper and pencil version of the procedure. Third, computer administration may seem less significant to some supervisors compared to paper administration. The relative efficacy of computer versus paper administration is unknown at this time, but interview data suggested possible differences.

SUPPORT ENVIRONMENT

The support environment for the proposed procedure could include several DoD components depending on the implementation medium.[17] Regardless of medium, The DCHC could be involved in management and oversight of the procedure. The DCHC develops and manages DoD counterintelligence and human intelligence programs worldwide (DoDI O-5100.93, Defense Counterintelligence [CI] and Human Intelligence [HUMINT] Center [DCHC], August 13, 2010; Directive Type Memorandum [DTM] 08-032, Establishment of the Defense Counterintelligence and Human Intelligence Center [DCHC], July 22, 2008). The DCHC also is responsible for administrative and management oversight of national security investigations performed by DoD counterintelligence elements. Among other things, the Director, DCHC recommends to the USD(I) fundamental DoD counterintelligence training standards. The DCHC likely would contribute substantive content and analytic support for the PASS procedure.

The Defense Technical Information Center (DTIC) is a DoD Field Activity under the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L); DoDD 5105.73, Defense Technical Information Center (DTIC), August 19, 2005). DTIC is operated under the authority, direction, and control of the Director of Defense Research and Engineering (DDR&E) as part of the DoD Scientific and Technical Information Program (STIP). Its purpose is to function as the central scientific, research, and engineering information support activity for the DDR&E. The DTIC administers an online version of Level I AT Awareness Training, which could be a good vehicle for computer-based administration of the PASS procedure.

[17] The support environment includes organizations that could support implementation of the proposed procedure with facilities, equipment, support software, technical expertise, etc.

The Defense Information Systems Agency (DISA) is a Combat Support Agency that operates under the authority, direction, and control of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO; DoDD 5105.19, Defense Information Systems Agency (DISA), July 25, 2006). The DISA is responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions, and it supports national security communications requirements in accordance with National Security Presidential Directive – 28 and Executive Order 12472. Its core functions include communications, command and control capabilities, information assurance, computing services, interoperability, testing, and standards, Global Information Grid enterprise services, engineering, and acquisition. DISA could support the PASS procedure by providing information technology solutions and advice for computer-based administration.

DISCUSSION

The Defense Personnel Security Research Center developed a simple procedure called the Personal Acknowledgment of Staff Security to increase supervisor awareness, felt responsibility, accountability, and reporting of behaviors related to espionage, terrorism, and malicious cyberspace activity. The procedure was designed to supplement existing security awareness and reporting programs aimed at moderating the harm caused by trusted insiders who threaten national security. The distinguishing component of the PASS procedure is the requirement of a signed certification by supervisors that they understand and intend to comply with the reporting policy in DoDD 5240.06. Recent psychological research suggests that the additional step of requiring a signed acknowledgment may make the requirements more salient and improve compliance (Shu, Gino, & Bazerman, 2011).

Initial interviews with counterintelligence and security personnel about the PASS concept resulted in positive feedback, but responses from a small sample of military and civilian supervisors indicated the need for more research to test and optimize the procedure. Stakeholders and subject matter experts were interested in the PASS concept, but some noted concerns about the utility of behavioral indicators for identifying potential threats, the effect of false positive reports on employees' careers, resistance to the procedure by supervisors, and legal/privacy concerns. Some military and civilian supervisors thought that the procedure was unique, straightforward, reasonable, and potentially effective. However, others felt that some of the materials needed revision to maximize effectiveness, and there were questions about the relative efficacy of paper versus computer-based administration. Another challenge noted by participants was that it would be necessary to distinguish the PASS procedure from a plethora of other requirements requiring supervisors' signatures.

OPERATIONAL AND ORGANIZATIONAL IMPACTS

The PASS procedure would entail some operational impacts. Command security managers would be responsible for administering the proposed procedure in conjunction with security awareness training. The paper and pencil version of the procedure would require security managers to identify supervisors who must submit certifications, as well as administer and collect PASS materials when supervisors complete their training. This approach also could include tasks such as data entry and secure transmission to appropriate counterintelligence personnel.

As with paper and pencil administration, any computer-based approach would necessitate identification of end users and some level of oversight by command security managers. All of the proposed approaches would require supervisors to submit certifications as part of periodic security awareness training, and counterintelligence elements would acquire a new data source, which could lead to additional investigations. If the proposed procedure is implemented as a web

application, it could require coordination between the existing training system and the system hosting PASS.

Other organizational impacts probably would be minimal. Some training may be necessary to ensure that command security managers understand their responsibility for administering the procedure, and counterintelligence elements would need to know what to expect. This could be accomplished relatively easily through electronic mail and an informational web site. A potential impact that is more difficult to gauge is whether or not the procedure could affect trust and cohesion within organizational elements (Kramer, 1999; Dirks, 2000). More research should be conducted to ensure that the proposed procedure would not adversely affect unit trust and cohesion. This is very unlikely given the egregious nature of most of the indicators in DoDD 5240.06, but it may be worthwhile to explore this issue further, especially in settings where trust and cohesion are critical.

Organizational impacts during development of the PASS procedure would include personnel involvement in studies, meetings, and discussions throughout the process; user and support involvement in reviews and demonstrations, evaluation of initial operating capabilities and evolving versions of the system, development or modification of databases, and required training; possible parallel operation of new and existing systems; and operational impacts during system testing of the proposed application.

IMPROVEMENTS AND POTENTIAL DISADVANTAGES

The proposed procedure could help improve security in a number of ways. It could reinforce existing security awareness training, as well as increase felt responsibility, accountability, and reporting of potential FIE threats. This would be accomplished by requiring supervisors to go on record that they intend to report potential insider threats related to FIEs, and by providing an immediate opportunity to practice what they preach. The procedure presumably would create cognitive dissonance for individuals who (a) register their intention to report and (b) have observed reportable indicators but have not yet reported the behavior (Dickerson et al., 1992). Cognitive dissonance may cause some individuals to report information that otherwise may have been withheld. This procedure also would make individuals accountable for reporting observed indicators, which could increase felt responsibility and reporting (Dose & Klimoski, 1995). Ultimately, the procedure might result in additional data for counterintelligence efforts to impede insider threats.

The PASS procedure would be an additional burden for command security managers and, to a lesser extent, supervisors. Command security managers would have additional responsibilities for ensuring that the procedure is completed by the right people at the right time. Supervisors would have to be familiar with their reporting responsibilities and submit PASS certifications at least annually. The

proposed procedure would be an additional expense for the Department. In addition, the procedure has not been pilot tested to determine its effectiveness.

ALTERNATIVES CONSIDERED

Several alternatives were considered as part of the research for this project. One consideration was whether or not administration of the procedure should be paper or computer-based. Additional research should be conducted to determine the relative efficacy of these approaches. Computer-based administration might be easier to implement throughout the Department, but it may not be as effective as a paper and pencil approach. Previous research that showed participants were more honest after signing an honor code was done using paper and pencil methods (Mazar et al., 2008; Shu et al., 2011). Thus, while there is some evidence to suggest that a paper and pencil version of the PASS procedure would be beneficial, it is unclear how computer administration would affect supervisors' commitment to complying with reporting requirements. Signing something digitally at one's computer may have a different psychological significance than an ink signature on paper, especially if the handwritten signature is done in the presence of others (i.e., making a public commitment; Cialdini, 2009). In the absence of additional investigation to determine the best approach, a paper and pencil version of the procedure is recommended because it is supported by previous research.

Central versus local data transmission, storage, and retention also are fundamental considerations for the proposed procedure. Data generated by the PASS procedure could be stored by local counterintelligence elements or in a central database (e.g., maintained by the DCHC). These decisions will largely depend on how the data will be used and by whom. However, if a paper and pencil approach was employed initially as part of a pilot test, it would be best to opt for local transmission, storage, and retention, in part, to defer software development costs until more definitive findings can be obtained.

Another important consideration was whether supervisors should certify subordinates individually as part of the annual performance appraisal process or as a group in conjunction with security awareness training. Collective certification would be less of a burden for supervisors, but it may be less effective than evaluating individuals separately. Nevertheless, if collective certification is done with security training, it would have the advantage of immediate application and reinforcement of the training material. On the other hand, individual certification as part of performance appraisals might serve as a reminder, as well as encourage supervisors to reflect more deeply upon each of their subordinates' behavior, which could result in increased reporting. However, supervisors would have to spend more time completing separate forms for each of their subordinates, which may cause some frustration as well as additional costs for the Department. In the absence of pilot testing to establish the best approach, collective certification in conjunction with security awareness training is recommended.

Other lists of behavioral indicators were considered in the course of PASS research. Initially, the plan was to encompass a broader array of topics, but subject matter experts and expanding indicator lists persuaded the authors to limit the scope of the procedure for practical reasons. Since DoDD 5240.06 provided reporting policy and reasonable indicators for most of the original areas of concern, it became the focus of the proposed procedure. Nevertheless, there are other lists of threat and safety indicators that could be utilized with the procedure. For example, Army Regulation 381-12, *Threat Awareness and Reporting Program*, October 4, 2010 also includes sensible indicators that could be used in a different version of the PASS procedure. While the current version of the procedure was designed to enhance counterintelligence efforts to thwart FIE threats in accordance with DoDD 5240.06, it also could be used in a similar manner to augment suicide and workplace violence prevention programs.

CONCLUSION

This report provides the rationale, description, and key considerations for a simple procedure to help increase reporting of potential FIE threats. The next phase of PASS research and development should include a pilot test to demonstrate its utility, determine the relative efficacy of paper and computer-based administration of the procedure, and inform implementation planning. Future research also could explore the differences between collective and individual certification. This research could be done on a relatively small scale to minimize costs, but a well-designed pilot test would be essential for ensuring that DoD resources are used sensibly.

RECOMMENDATIONS

- Pilot test the PASS procedure to (a) demonstrate its utility, (b) determine the most effective administration approach, (c) produce a cost estimate, and (d) inform implementation planning
- If the pilot test results indicate that the procedure is useful, develop an implementation plan and consider using it to enhance reporting in other domains

REFERENCES

Air Force Instruction 71-101 Volume 4 (2011). *Counterintelligence*. Washington DC: Department of the Air Force.

Army Regulation 381-12 (2010), *Threat Awareness and Reporting Program*. Washington, DC: Department of the Army.

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

Campbell, M. A., French, S., & Gendreau, P. (2009). The prediction of violence in adult offenders: A meta-analytic comparison of instruments and methods of assessment. *Criminal Justice and Behavior*, 36 (6), 567-590.

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.

CSO Magazine, United States Secret Service, CERT® Coordination Center, & Microsoft Corporation (2007, September 11). 2007 e-crime watch survey - survey results. Retrieved from http://www.cert.org/archive/pdf/ecrimesummary07.pdf

Department of Defense Instruction 2000.12 (2012). *DoD Antiterrorism (AT) Program*. Washington, DC: Department of Defense.

Department of Defense Instruction 2000.16 (2006), *DoD Antiterrorism (AT) Standards*. Washington, DC: Department of Defense.

Department of Defense Instruction 5240.26 (2012). *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*. Washington DC: Department of Defense.

Department of Defense Instruction 5240.6 (2004). *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*. Washington DC: Department of Defense.

Department of Defense Instruction O-5100.93 (2010). *Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center (DCHC)*. Washington DC: Department of Defense.

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.

Dirks, K. T. (2000). Trust in leadership and team performance: Evidence from NCAA basketball. *Journal of Applied Psychology*, 85 (6), 1004-1012.

DoD Directive 5105.19, *Defense Information Systems Agency (DISA)*, July 25, 2006.

DoD Directive 5105.73, *Defense Technical Information Center (DTIC)*, August 19, 2005.

DoD Directive 5143.01, *Under Secretary of Defense for Intelligence (USD(I))*, November 23, 2005.

DoD Directive 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, May 17, 2011.

DoD Directive O-5240.02, *Counterintelligence*, December 30, 2010.

DoD Directive Type Memorandum 08-032, *Establishment of the Defense Counterintelligence and Human Intelligence Center (DCHC)*, July 22, 2008.

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

Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, as amended by E.O. 13286 February 28, 2003.

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

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.

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

International Association of Chiefs of Police (1996). *Combating Workplace Violence: Guidelines for Employers and Law Enforcement*. Alexandria, VA: IACP.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, 50, 569-598.

Lieberman, J. I., & Collins, S. M. (2011). *A ticking time bomb: Counterterrorism lessons from the U.S. Government's failure to prevent the Fort Hood attack.*

United States Senate Committee on Homeland Security and Governmental Affairs. Washington, DC.

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.

Morrison, E. W., & Phelps, C. C. (1999). Taking charge at work: Extrarole efforts to initiate workplace change. *The Academy of Management Journal*, 42 (4), 403-419.

National Security Presidential Directive 28. *United States Nuclear Weapons Command and Control, Safety, and Security*, June 20, 2003.

Office of Personnel Management (1998). *Dealing with workplace violence: A guide for agency planners*. Washington, DC: Author.

Pressman, D. E. (2009). *Risk assessment decisions for violent political extremism*. Ottawa, Canada: Carleton University.

Sageman, M. (April 1, 2011). Presentation to FBI Academy. *Behavioral Indicators of Concern: Radicalization and Terrorism*.

Secretary of the Navy Instruction 3850.2C (2005). *Department of the Navy Counterintelligence*. Washington, DC: Department of the Navy.

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.

Silber, M. D. & Bhatt, A. (2007). *Radicalization in the West: The homegrown threat*. New York Police Department Intelligence Division.

Sims, R. L., & Keon, T. L. (2000). The influence of organizational expectations on ethical decision making conflict. *Journal of Business Ethics*, 23(2), 219-228.

Storey, J. E., Gibas, A. L., Reeves, K. A., & Hart, S. D. (2011). Evaluation of a violence risk (threat) assessment training program for police and other criminal justice professionals. *Criminal Justice and Behavior*. Retrieved from http://cjb.sagepub.com/content/early/2011/03/31/0093854811403123).

United States Department of Justice, Federal Bureau of Investigation (2002). *Workplace Violence: Issues in Response*. Washington, DC: Author.

United States Department of Justice, Office of the Inspector General (2003). *A review of the FBI's performance in deterring, detecting, and investigating the espionage activities of Robert Philip Hanssen: Unclassified executive summary.* Washington, DC: Author.

REFERENCES

Verizon RISK Team (2012). *2012 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/Products/security/dbir/?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z041).

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.

APPENDIX A:

COPY OF DODD 5240.06, ENCLOSURE 4

ENCLOSURE 4

REPORTING

1. GENERAL. DoD personnel shall report, in accordance with section 3 of this enclosure, the contacts, activities, indicators, and behaviors in section 5 of this enclosure.

2. FAILURE TO REPORT. DoD personnel who fail to report information as required in paragraph 3.a and section 5 of this enclosure that identifies reportable contacts, activities, indicators and behaviors, may be subject to judicial or administrative action, or both, pursuant to applicable law and regulations.

a. Persons subject to the UCMJ who violate the referenced specific provisions of this Directive may be subject to punitive action under Article 92, UCMJ.

b. Civilian employees under their respective jurisdictions who violate the referenced specific provisions of this Directive may be subject to appropriate disciplinary action under regulations governing civilian employees.

3. REPORTING REQUIREMENTS

a. DoD personnel shall report the contacts, activities, indicators, and behaviors stated in section 5 of this enclosure as potential FIE threats against the DoD, its personnel, information, materiel, facilities, and activities, or against U.S. national security.

b. DoD personnel shall report potential FIE threats to their organization's CI element or their supporting MDCO.

(1) When CI support is not available, DoD personnel shall report the threat without delay to their security officer, supervisor, or commander.

(2) Security officers, supervisors, and commanders shall forward reported information to their organizational CI element or their supporting MDCO within 72 hours.

c. DoD personnel, and their security officers, supervisors, and commanders, shall also comply with all other applicable reporting requirements, including those in accordance with DoD 5200.1-R (Reference (u) and DoDI 8500.2 (Reference (v)).

4. ACTIONS ON REPORTED INFORMATION. Upon receiving information on reportable contacts, activities, indicators, and behaviors, the MDCOs and organizational CI elements shall:

a. Take appropriate and authorized action in accordance with References (i) through (n).

b. In the event a contact, activity, indicator, or behavior is not associated with FIE, report such contacts, activities, indicators, and behaviors, to include self-radicalization, to the appropriate law enforcement or command authorities.

c. Inform the DoD Components about reported incidents, as appropriate, to allow the DoD Components to implement protection measures.

5. REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS. Tables 1 through 3 contain reportable contacts, activities, indicators, behaviors, and cyber threats associated with FIEs.

a. Table 1. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 22 are subject to punitive action in accordance with section 2 of this enclosure. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.
2.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
3.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
4.	Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
5.	Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
6.	Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
8.	Discovery of suspected listening or surveillance devices in classified or secure areas.
9.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
10.	Discussions of classified information over a non-secure communication device.
11.	Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12.	Transmitting or transporting classified information by unsecured or unauthorized means.
13.	Removing or sending classified or sensitive material out of secured areas without proper authorization.

14.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
15.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
16.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
17.	Unwarranted work outside of normal duty hours.
18.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
19.	Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
20.	Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.
21.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
22.	Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or SNS.
23.	Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
24.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.

b. Table 2. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 9 are subject to punitive action in accordance with section 2 of this enclosure. The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action.

Table 2. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.

6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

c. Table 3. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 10 are subject to punitive action in accordance with section 2 of this enclosure. The indicators in items 11 through 19 are reportable, but failure to report these indicators may not alone serve as the basis for punitive action.

Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of DoD account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data exfiltrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.

19.	Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

APPENDIX B:

COPY OF DODD 5240.06, ENCLOSURE 3

ENCLOSURE 3

AWARENESS TRAINING

1. GENERAL. CIAR training shall include instruction on:

a. The threat from FIEs.

b. The methods, also known as "modus operandi," of FIEs.

c. FIE use of the Internet and other communications including social networking services (SNS).

d. The CI insider threat.

e. Anomalies in accordance with References (l) and (m).

f. Reporting responsibilities regarding foreign travel and foreign contacts.

g. The reporting requirements in Enclosure 4.

2. INDIVIDUAL TRAINING REQUIREMENTS

a. All DoD personnel shall receive CIAR training in accordance with this Directive.

b. Failure to receive training does not relieve individuals from their reporting responsibilities in Enclosure 4 of this Directive.

3. DoD COMPONENT TRAINING REQUIREMENTS. DoD Components shall:

a. Provide CIAR training to DoD personnel within 90 days of initial assignment or employment to the Component and every 12 months thereafter.

b. Provide CIAR training with a CI-experienced person in a classroom environment.

(1) When a CI-experienced person is not available, an individual knowledgeable of CIAR may conduct the training; however, the Component shall provide the training materials to the organizational CI element or supporting MDCO for review.

(2) When classroom training is not feasible, provide CIAR training through other media.

c. Provide CIAR training tailored to their Component's mission, functions, activities, and locations.

d. Record CIAR training in the USD(I)-approved CI information systems in accordance with Reference (c) and, upon request, make the record available to the supporting MDCO and the CIAR functional manager. The record shall identify the:

(1) Organization receiving the training.

(2) Attendees.

(3) Trainer and his or her organization.

(4) Date(s) of training.

(5) Subject of the training and a summary of the training content.

e. Maintain training records for a period of 5 years in accordance with Reference (e) and other applicable records management policy.

f. Conduct training in compliance with this Directive in addition to the antiterrorism training requirements of DoDD 2000.12 (Reference (q)).

4. CI SUPPORT TO CIAR TRAINING. The MDCOs and organizational CI elements shall:

a. Provide their supported Components with assistance to establish and maintain CIAR training.

b. Upon request and when possible, provide their supported Components with a CI-experienced person to conduct the CIAR training.

c. When unable to provide a CI-experienced person to conduct training, review Component CIAR training materials for accuracy and completeness.

5. FOREIGN TRAVEL. DoD personnel with access to:

a. Critical program information shall notify their security personnel of all projected foreign travel in accordance with DoDI 5200.39 (Reference (r)). Personnel who travel to overseas locations shall receive foreign intelligence threat briefings and anti-terrorism briefings prior to their departure.

b. Sensitive compartmented information shall meet their special security obligations, including advance foreign travel notification for official and unofficial travel and receipt of defensive travel briefings, in accordance with Director of Central Intelligence Directive 1/20P (Reference (s)).

c. Special access program information shall notify their security personnel of all projected foreign travel. Such personnel shall receive foreign intelligence threat briefings and antiterrorism briefings prior to overseas travel in accordance with the DoD Overprint

to the National Industrial Security Program Operating Manual Supplement (Reference (t)).

APPENDIX C:

SAMPLE COVER LETTER

DEFENSE PERSONNEL SECURITY RESEARCH CENTER
20 Ryan Ranch Road, Monterey, CA 93940 | 831-583-2800 | perserec.security@osd.pentagon.mil

Friday, April 20, 2012

Sam Smith
Supervisor
PERSEREC
20 Ryan Ranch Road
Monterey, CA 93940

Dear Sam Smith:

The Department of Defense (DoD) employs an enormous workforce and relies on that workforce to secure and safeguard critical information, facilities, personnel, and other key aspects of its mission. Department of Defense Directive (DoDD) 5240.06, *Counterintelligence Awareness and Reporting (CIAR),* May 17, 2011 outlines employee training and reporting requirements for foreign intelligence entity (FIE) threats and activities. It also includes detailed lists of reportable FIE, terrorism, and malicious cyberspace contacts, activities, indicators and behaviors. Despite all of the measures taken by DoD to ensure the trustworthiness of the workforce, some individuals become vulnerable to FIE and misuse that trust. Potential damage caused by FIE threats may be reduced by timely reporting to appropriate personnel. While it is every employee's responsibility to report potential threats, supervisors are critical for ensuring that threats are recognized and reported at an early stage so that intervention will have a reasonable chance of success and minimize harm to personnel and national security.

If you have not already done so, please review DoDD 5240.06 (available online at www.dtic.mil/whs/directives/corres/pdf/524006p.pdf) and especially Enclosure 4, Reporting. Enclosure 4 prescribes reporting requirements, to include three lists of reportable contacts, activities, indicators, and behaviors associated with FIEs. Once you are familiar with your reporting responsibilities per this directive, complete the attached form. It asks you to acknowledge your familiarity with DoD reporting requirements, and your intention to report possible FIE threats. This form must be submitted to the security management office no later than close of business on June 30, 2012.

If you have questions or concerns, please call me at 831-583-2800.

Sincerely,

SECURITY MANAGER

ENCLOSURES