Report No. DoDIG-2012-001
October 6, 2011

Inspector General
United States Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSESSMENTS

Assessment of Security Within the Department of Defense - Training, Certification, and Professionalization

Additional Information and Copies

For information and to request copies of this report, contact the DoD Office of Inspector General at (703) 604-8841 or (DSN) 664-8841.

Suggestions for Audits and Evaluations

To suggest ideas for or to request future audits or evaluations, contact the Office of the Deputy Inspector General for Intelligence and Special Program Assessments at (703) 604-8800 (DSN 664-8800) or UNCLASSIFIED fax (703) 604-0045. Ideas and requests can also be mailed to:

ODIG-ISPA (ATTN: ISPA Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

Acronyms and Abbreviations

ACTEDS	Army Civilian Training Education and Development System
COCOM	Combatant Command
DARPA	Defense Advanced Research Projects Agency
DSS	Defense Security Service
FCM	Functional Community Manager
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OSD	Office of the Secretary of Defense
SPēD	Security Professional Education and Development Program
USD(I)	Under Secretary of Defense for Intelligence
USSOUTHCOM	United States Southern Command

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

October 6, 2011

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DEPUTY UNDER SECRETARY OF DEFENSE FOR
INTELLIGENCE AND SECURITY

SUBJECT: Assessment of Security Within the Department of Defense - Training, Certification, and Professionalization (Report No. DoDIG-2012-001)

We are providing this report for your information and use. This is the second in a series of reports designed to provide an overall assessment of security policies and procedures within the Department. We issued a draft of this report on June 6, 2011. We considered comments from the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security in preparing the final report. Management generally concurred with our recommendations. While management either partially or fully disagreed with two recommendations, proposed actions and actions taken to date, along with corresponding details, satisfies the intent of those recommendations. Therefore, we will not require further comment.

We appreciate the courtesies extended to the staff. Please direct questions to Mr. William Rainey at (703) 604-8873 (DSN 664-8873), william.rainey@dodig.mil, or Mr. David Ingram at (703) 604-8826 (DSN 664-8826), david.ingram@dodig.mil.

Patricia A. Brannin
Deputy Inspector General
Intelligence and Special
Program Assessments

Results in Brief: Assessment of Security Within the Department of Defense - Training and Certification

What We Did

This is the second in a series of reports designed to provide an overall assessment of security policies and procedures within the Department. In this report, we address how the Department trains, certifies, and establishes professional standards for security professionals across the DoD security enterprise. We addressed security costs in a previous report. We will focus on the classification and grading of security personnel and the policies associated with these security issue areas in subsequent reports.

What We Found

We found that security training is sporadic and not consistently applied throughout the Department. This is due, in part, to the inability to ensure that funding for security training is dedicated and not re-allocated for non-security efforts. Furthermore, the Security Professional Education Development (SPēD) Certification Program is only partially developed at this time and linkages to identified security job requirements and competencies are not well understood by the DoD security workforce.

A certification program to assess the proficiencies of individuals in security positions will ensure they are appropriately placed in security positions with competencies that best serve the security needs of the Department. The certification program needs to be fielded in a timely and consistent manner with support from the DoD for the program's implementation and sustainment.

The Under Secretary of Defense for Intelligence directed the Defense Security Service to establish a certification program for security professionals with a goal towards the professionalization of the security field. The SPēD Certification Program is in its preliminary stages and full implementation has not been completed. Developers of the program have provided quarterly program status updates to the DoD Security Training Council but program status regarding implementation plans have not been effectively disseminated to the security community. As a result there are some doubts across the Department regarding the viability of the certification program and whether it will be implemented in a timely manner.

What We Recommend

The Director, Defense Security Service: examine the current implementation strategy and develop a standardized certification program implementation plan for use by all organizations and commands, including a means to track those with certifications and the level of certification; develop an awareness plan to communicate the status of the security certification program across the Department; and address timeliness concerns to ensure the expeditious implementation of certification for security professionals and a consistent level of protection of DoD resources. The Deputy Under Secretary of Defense for Intelligence and Security should develop a mechanism to ensure consistent oversight and monitoring of funds allocated to support the security certification program to ensure funds are not repurposed for non-security training endeavors.

Management Comments and our Response

While comments from the Director of Security generally concurred with our recommendations, they either partially or fully disagreed with two recommendations; however, proposed actions and actions taken to date, along with corresponding details, satisfies the intent of those recommendations. Therefore, we will not require further comment.

Table of Contents

Introduction

Security spans the Department of Defense and is essential to protecting its resources. For this reason, the DoD has long sought to create a corps of well trained, competent security personnel to support protection efforts. Properly applied, a capable security structure can be effective in the possible deterrence of another Fort Hood or WikiLeaks incident. Several security reviews and audits have assessed the state of security training and certification, both within the Federal Government and specific to the DoD, and have made recommendations to further enhance the professionalization and proficiencies of the security workforce. The process for training and certifying DoD security professionals remains fragmentary with no standardization across the security enterprise.

The Under Secretary of Defense for Intelligence (USD(I)) directed the Defense Security Service (DSS) to establish a training and certification program for security professionals with a goal towards security professionalization. DSS is in the process of fielding the SPēD Certification Program, which will provide a path towards security professionalization through a four level certification program. SPēD is a DoD-wide security training and certification program that will identify security proficiencies and accountabilities. When fully implemented, SPēD will provide the DoD security workforce a path towards professionalization and will establish standardized competencies across Services and commands. However, the program is in its preliminary stages and the path toward full implementation has not been completed.

Objectives

This is the second in a series of reports on security within the DoD requested by the USD(I) to assess the state of security in the Department. The overall assessment objective is to determine:

- how the Department programs and tracks its security costs and measures the return on investment for security expenditures;
- how security professionals are trained, certified, and professionalized;
- how security professionals' jobs are classified and graded; and
- how effective security policy is in addressing the security needs of the Department.

The focus in this report is on security training, certification, and professionalization issues. Of note, security professionals that fall under the purview of the Office of the Under Secretary for Intelligence (OUSD(I)) are in the security administration, GS-0080 series career field. Accordingly, references in this report to security personnel will refer specifically to GS-0080s.

Background

The creation of a cadre of security professionals within the government has been an ongoing effort since the latter half of the 20th century. A study commissioned by the War Department in 1947 recommended the creation of a National Security University with the stated goal of educating security practitioners from all agencies tasked with supporting national security. In 1997, a national defense panel proposed establishing an interagency workforce of security personnel to occupy positions across government security organizations. In 2001, the Hart Rudman Commission recommended the formation of a National Security Service Corps with associated rotational assignments, professional development, and educational opportunities. More recently, in May 2007, Executive Order 13434 "National Security Professional Development," was issued with the intent to advance the education, training, and experience of security practitioners occupying security positions throughout executive departments and agencies.

Executive Order 13434, commissions, studies, and panels sought to address security training and professionalization issues within the national security enterprise. Within the DoD, a 2006 Defense Personnel Security Research Center[1] study "Development and Application of Skills Standards for Security Practitioners" identified inconsistent levels of training, work requirements, and responsibilities among security professionals. The study noted that variances in training and competencies undermined the Department's ability to successfully accomplish its security mission.

Steps have been taken to address these concerns. The OUSD(I) has taken the position that all disciplines under its organizational cognizance will move towards certification of their respective staff, to include security. The current state of security training within DoD, however, remains problematic.

Our previous security report[2] noted that the DoD needs a comprehensive methodology to track security costs, more accurately program future years' security budgets, and examine the return on investment for security expenditures. The ability to implement a standardized methodology to track security costs is hindered by the Department's inability to "fence" or control security funds which are often drawn from Operations and Maintenance funds. For this reason, security funds – to include training funds – can be reallocated at command discretion.

---

[1] The Defense Personnel Security Research Center seeks to improve the efficiency and effectiveness of the DoD personnel security system. A component of the Defense Human Resources Activity in the Office of the Under Secretary of Defense for Personnel and Readiness, the Defense Personnel Security Research Center receives direction and research priorities from the Office of the Deputy Under Secretary of Defense for Intelligence and Security.

[2] "Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs," Report No. 10-INTEL-09, August 6, 2010.

Finding A. DoD Needs to Support the Implementation and Sustainment of a Security Certification Program

Currently, the DoD lacks a standardized and consistent training program that addresses the training needs and requirements of security professionals. The Services do not have consistent mechanisms for the training and education of their security staff. Moreover, the Combatant Commands often lack resources and are often required to train military personnel with no previous security background who are assigned on a temporary basis.

The absence of a coordinated security training program across the DoD security enterprise results in a fragmentary training structure and reflects the absence of an integrated security framework. The OUSD(I) is addressing this insufficiency through the implementation of the SPēD Certification Program. However, the OUSD(I) needs to address concerns regarding the program's implementation as similar efforts have been unsuccessful in the past. In addition, the OUSD(I) must address potential funding issues by ensuring appropriate application of security funds for the implementation and sustainment of certification and professionalization efforts.

Policies Establishing Standards for the Conduct of Security Education, Training, and Professional Development

Executive Order 13434, May 2007, mandated the creation of a framework to enable security personnel a path towards professionalization through integrated security education, training, and professional experience. The goal was to enhance the knowledge, skills, and proficiencies of security professionals and thus enhance overall national security. In response to this requirement, federal agencies have instituted professional development programs for security personnel. DoD policies establishing authorities and implementing policy changes specific to security training are detailed below.

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)), November 23, 2005, established the responsibilities, functions, relationships, and authorities of the USD(I) to include security. The Directive identifies the USD(I) as the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for security matters. As such, the USD(I) is required to develop policy and provide oversight on training, education, and career development of personnel within the Defense Intelligence enterprise which includes security.

DoD Instruction 3305.13, "DoD Security Training," December 18, 2007, requires the USD(I) to exercise policy oversight of personnel in defense intelligence positions of which security is a component, to ensure that Defense intelligence, counterintelligence, and security components are manned, trained, equipped, and structured to support the missions of the Department and fully satisfy the needs of the Combatant Commands (COCOMs), the Services, and the Office of the Director of National Intelligence, as appropriate. As a result, in June 2007, the USD(I) established the Human Capital Management Office to professionalize the DoD intelligence workforce.

In furtherance of this effort, the USD(I) created the DoD 3305 series of issuances to address the training, education, and professional development needs of the DoD Intelligence Enterprise. The series authorizes DoD functional managers and training councils to define workforce training standards. The training and professionalization of security personnel is governed by these issuances. With respect to training, DoD Instruction 3305.13:

- establishes policy, standards, and procedures and assigns responsibilities for the conduct of DoD security education, training, and professional development;
- assigns the Director, DSS, as the functional manager responsible for the execution and maintenance of DoD security training;
- establishes and designates the SPēD program as the DoD-level security training program; and
- establishes the DoD Security Training Council as an advisory body on DoD security training that reports to the Defense Intelligence Training and Education Board.

The DoD Security Training Council functions as the training oversight council for DoD security and serves as the central source for functional training issues. The training council provides the Security Functional Manager with the means through which intelligence training issues, policy changes, establishment of standards, allocation of responsibilities, and other related topics can be addressed and recommendations made to the USD(I).

DoD Manual 3305.13-M, "Security Accreditation and Certification Manual," March 14, 2011, serves as the implementation guide for DoD Instruction 3305.13. DoD Manual 3305.13-M further defines the roles and responsibilities of the USD(I), DSS, the DoD Security Training Council, and the Components with respect to security education and professional development. With regard to resources to ensure sustainment of training efforts toward the professionalization of the security workforce, the manual states that the:

- USD(I) will ensure that sustainment requirements of the SPēD Certification Program and institutional accreditation are identified and included during the program and budget build and during development of supplemental requests.

- USD(I) will review SPēD certification program resource requests upon budget submission and provide additional guidance as needed.

- DSS will identify SPēD certification program resource requirements and submit for inclusion in the DoD budget.

- Heads of Components will identify SPēD certification program education, training, and certification renewal requirements including associated costs for time required for professional development and include in planning, programming, and budgeting actions.

DoD Instruction 3115.11, "DoD Intelligence Human Capital Management Operations," January 22, 2009, establishes policy, prescribes procedures, and assigns responsibilities for the development and execution of the DoD Intelligence Human Capital Programs, including Security. The Instruction also designates the USD(I) as the accreditation and certification official for the Defense Intelligence Components Department-level programs. With respect to implementation, the Instruction assigns the responsibility of developing human capital policies and guidance for the DoD intelligence workforce to the Human Capital Management Office within the OUSD(I). Specific to training, DoD Instruction 3115.11 authorizes the Defense Intelligence Training and Education Board as the decision-making body for policy coordination and oversight on Defense Intelligence, workforce development, training, and education matters in support of the Defense Intelligence Human Resource Board.

The Defense Intelligence Training and Education Board, which includes the Chair of the DoD Security Training Council, addresses DoD intelligence education and training matters of Defense Intelligence Components. The board also provides a forum to address DoD intelligence professional development issues and matters such as policy changes, establishment of standards, allocation of responsibilities, and other related topics.

Recommendations can then be made to the USD(I) via the Defense Intelligence Human Resource Board. Defense Intelligence Training and Education Board meetings occur at least bi-monthly or as determined by members. In addition, participation in meetings is extended to non-Defense Intelligence Components (e.g., National Intelligence University, American Council on Education, and the Council on Occupational Education) as associate members to allow full access to DoD intelligence education and training, as appropriate.

Survey Findings Regarding Security Training

We solicited input from Security Managers via surveys in an attempt to ascertain the state of security training and certification across organizations, Services and commands. Respondents were provided with a password to access the survey online. The survey was sent to 48 Security Managers throughout the DoD and addressed funding, certification and training, classification and grading, and policy issues related to security. As the security managers of their respective organizations, respondents were able to provide knowledgeable responses which in turn inform this report. We received a response rate of 35%, which is consistent with voluntary response rates.

Specific to training, survey respondents noted that security training was primarily received on-line, on-the-job, or via on-site training. Nearly two thirds of respondents felt security training prepared security professionals for security responsibilities. The dissatisfaction of one third of respondents indicated the lack of uniformity in available programs and inconsistent access to security training across the DoD security enterprise.

Survey responses identified that re-allocation of funds occurs more frequently with training funds as security training is often a low priority at DoD commands; and unfenced funds can be easily shifted to meet command exigencies. As a result, security training occurs primarily on-the-job or is very limited.

While survey respondents provided somewhat consistent feedback regarding the state of security training, there were a few exceptions. One survey response is detailed below to highlight the complexity of the security mission across the DoD security enterprise and to underscore that a "one size fits all" approach may not meet all DoD organizational security needs.

Highlight – The Defense Advanced Research Projects Agency (DARPA). DARPA is the research and development organization for the Department. DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming national security. To that end, DARPA funds unique and innovative research through the private sector, academic, and other non-profit organizations as well as government laboratories. DARPA's research runs the gamut from conducting scientific investigations in a laboratory to building full-scale prototypes of military systems.

DARPA utilizes contract and civilian security professionals in support of their complex mission. According to DARPA, the requirements for their contract security professionals are far above the standards set for ordinary security officers. Moreover, unlike some commands, all of DARPA's security personnel perform security as a primary rather than collateral duty. DARPA has no assigned military personnel in support of security. Their security team has an average of over 24 years of security experience and both contract and civilian security personnel have at least a bachelor's degree.

DARPA's main concern does not lie with the proficiencies of their security professionals but rather with the level of training and proficiencies of other DoD security organizations tasked to provide oversight of DARPA activities. Security managers noted that outside organizations often do not have the training to understand the environments they are required to oversee. Thus, an unintended consequence of delegating authorities to an outside agency is the questionable value of assessments that an outside organization is able to provide. Moreover, outside components cannot make informed risk management decisions about programs with which they do not interact on a regular basis. As a result, the inability to understand the complexity of programs can also affect cost.

When outside organizations are tasked to enforce security requirements, they do so with no understanding of the impact on cost, schedule, and performance – factors that can impede the delivery of the product. If inspecting organizations understood the nuances of projects, they could provide DARPA with the leeway to apply risk management principles resulting in significant cost savings for the DoD.

As the research and development organization for the DoD, DARPA is an organization that faces unique security requirements. By leveraging the capabilities of a highly trained caliber of security professionals, DARPA has been able to adequately meet their organization's security needs. This heightened level of proficiency is an effective model for an advanced research organization where security lapses could have national level implications.

Military Department Security Training Efforts

Information obtained via interviews with security officials confirmed the need for standardized, requisite, and consistent security training across the Services for both military and civilian personnel. Army security officials said during interviews that with the exception of their security intern program, there is no consistent approach to security training. Navy security officials are in the process of refreshing competencies for the GS-0080 security workforce through an executive committee that is addressing professional development. Marine Corps security officials have a career roadmap for their GS-0080 security professionals, but there is no requirement to take the specified training. Air Force security officials have taken steps to achieve their goal of improving security training and are employing an enterprise approach to security issues to include the integration of risk management principles.

Army Security Training Efforts

The state of security training in the Army is inconsistent. One of the main causes is the manner in which training funds are allocated. Once security monies are provided to commands, Army headquarters loses control over how the funds are spent. While this situation is not unique to the Army, Army security officials also stated that the reapportioning of funds has had an adverse impact on security training. Training funds are not fenced and can be repurposed at command discretion to address other command priorities. Without consistent funding, security training occurs primarily on-the-job or is very limited.

Another concern is the level of preparedness of military personnel who are required to fill security slots. There are no regulations mandating training for military personnel performing security as an assigned duty. For example, a military person can be assigned to a post as a special security officer without receiving any specialized training. As a result, military personnel are often ill prepared to fulfill security requirements.

With respect to Army civilian security professionals, the Army distinguishes between two groups: security personnel who support intelligence programs and security personnel engaged in physical security and law enforcement. The two groups fall under career programs 35 and 19, respectively. The Army noted that where training does exist, it is available primarily for individuals who are in career program 19, physical security and law enforcement.

The Army has the Army Civilian Training Education and Development System (ACTEDS) that provides security professionals with guidance for career planning and development. Career program 19 has four levels of professionalization (entry/intern, specialist, intermediate, and management) with associated knowledge, skills, and abilities. The program provides a career path, identifies the professional characteristics for physical security and law enforcement and establishes a master training plan. Army security officials stated that career program 35 does not currently have the formalized training structure that career program 19 has. However, career program 35 is in the process of being tied to SPēD.

Moreover, information gleaned from interviews, indicates that ACTEDS is somewhat dated. Army headquarters personnel said that the Army had previously considered updating ACTEDS information for security personnel, but determined that it would be counterproductive to update ACTEDS without first aligning the course information with SPēD. Once SPēD is implemented by the DSS, the Army will fully integrate SPēD course information into ACTEDS.

The Army is currently collaborating with the DSS on the SPēD program through the development of implementation protocols. Through their presence on the DoD Security Training Council and with the assistance of Army subject matter experts, the Army is also providing input into the skills standards review – a critical component of the SPēD program design.

SPēD will address funding issues because a significant portion of security training can occur on-line at no additional cost to Service organizations. However, Army security professionals expressed some concerns regarding the completeness of SPēD, the transparency of the implementation process, and whether the program would be fielded in a timely manner.

The Army does not have a military occupational specialty or an additional skills identifier for security personnel. Accordingly, the task to ensure that military members are appropriately credited for any SPēD training and or certification that they might receive could be problematic. This concern is consistent with a 2008 report[3] that detailed the decision to exempt the Foreign Service, the Intelligence Community, and the DoD from certain National Security Professional Development requirements. Per the Congressional Research Service report, some officials reportedly feared that full participation in the National Security Professional Development program might impinge on time and resources available to meet their existing career development requirements.

Army representatives expressed similar concerns noting that the Army Training and Doctrine Command might not accept the mandatory SPēD training and certification if there is not a mechanism in place to appropriately credit military members for their security training and ensure that the training is career-enhancing. In the absence of an additional skill identifier or a military occupational specialty for security, it will be difficult to ensure that security training will provide career benefits to Army service members. Despite expressed concerns, the Army is invested in the implementation of SPēD to address their current security training and certification needs.

Navy Security Training Efforts

The Navy is in the process of updating the career professional development standards for their civilian security workforce. The existing development standard identifies prerequisites, job assignments, training, responsibilities, and competencies at the entry, journeyman, expert, and senior executive service level. The Navy security manager tasked with career development noted that standards would be harmonized with DoD standards as established in the SPēD certification program.

The Navy is satisfied with the security training provided by the DSS noting that a majority of courses are available on-line at no cost to the organization. The only issue in connection with available on-line training is ensuring that commands allow their security workforce adequate time to take the training. With respect to the SPēD program, the security manager noted that legacy security personnel would retain their existing positions but would be required to have SPēD certification for advancement opportunities. In the absence of further certification, legacy personnel might have their billets recoded to accurately reflect their job requirements.

---

[3] Congressional Research Service Report, "Building an Interagency Cadre of National Security Professionals: Proposals, Recent Experience, and Issues for Congress," July 8, 2008.

The Navy security manager also noted that SPēD testing would assist in identifying competencies across the organization which would allow them to identify positions or individuals that were misclassified. Of note, the security manager expressed satisfaction with the performance of Navy security personnel who participated in SPēD beta testing, citing the high percentage of participants who successfully mastered the first level of certification. In all, the Navy security manager feels that the SPēD program is on track and looks forward to the program's full implementation.

Marine Corps Security Training Efforts

The Marine Corps has unique challenges with respect to security training as they are subject to both Navy and Office of the Secretary of Defense (OSD) policies as well as internal Marine Corps regulations. Nevertheless, the Marine Corps applies an enterprise approach to security ensuring that security standards are applied across the board and throughout the organization. Moreover, the Marine Corps has established career development plans for their anti-terrorism; chemical, biological, radiological, and nuclear; information; personnel; and physical security workforce. The career development plans identify competencies at the apprentice, journeyman, and expert levels with associated target grades. In addition, desired certifications and credentials are specified for each proficiency level. The plans list training opportunities for each skill level along with identified institutions that offer the associated courses. There is no requirement that Marine Corps security professionals take the identified courses; however, it is recommended. The Marine Corps security managers feel that SPēD makes sense and will ensure that their security professionals have comparable skills that will be transferrable across the Department. They expressed concern that there is no physical security component with the exception of handling classified material. However, they stressed that the Marine Corps and the military as a whole desperately need certification programs for their security professionals.

Air Force Security Training Efforts

The Air Force is employing an enterprise approach to security matters to include the training of security professionals. In 2006, the Air Force made the decision to transform the manner in which information was protected. This transformation decision resulted in the creation of an Information Protection Directorate, which was established in 2007. The directorate serves as the single reporting entity on matters related to information protection and reports directly to the Administrative Assistant to the Secretary of the Air Force, the Air Force's senior security official. As a result of ongoing transformations, the directorate is progressing in the finalization of a training and certification program for Air Force security personnel.

The creation of the training and certification program reflects an understanding on the part of the Air Force that modern-day security professionals need to have a greater depth of knowledge and the technical matching skill sets to address the demands of security in the information age. According to Air Force leadership, an effective security professional needs to be a knowledgeable advisor with an understanding of how to manage information protection. He or she has to know all aspects of security to understand how security disciplines are integrated. Moreover, Air Force security personnel will need to recognize the importance of integrating corresponding disciplines such as counterintelligence, law enforcement, and biometrics into a comprehensive security framework. The Air Force assesses that as a result of automation and increased proficiencies, fewer people will be needed to perform required security tasks; thus improved competencies will result in increased efficiencies.

The Air Force training and certification program is slated to be fully implemented in 2011 and integrates the SPēD program implemented by the DSS. Similar to SPēD, the Air Force program has a four level certification structure designed to gauge the proficiencies of security professionals at entry, mid-career, and leadership levels. Training will consist of DoD Security Training Council-approved curricula. However, the Air Force is also seeking to create an undergraduate program for security professionals in which risk management principles will be incorporated throughout the curriculum. This program will be conducted through the Advanced Technical Intelligence Center for Human Capital Development[4] with the intent that an undergraduate degree will serve as a basis for Level-III certification. Notwithstanding the status of the SPēD program, Air Force security leadership indicated that they are prepared to move forward with their security training and certification plans.

Combatant Command Security Training Efforts

The COCOMs are joint service commands composed of two or more armed services. Each one of the COCOMs has a broad continuing mission under a single commander at the four-star level or equivalent. Given their joint structure and expansive mission, the COCOMs face unique security challenges.

With respect to security training, we found that the security professionals at the COCOMs primarily receive their security training through on-line courses, on-the-job training, or tailored short-term security courses available on installations. The ability of the COCOMs to send security professionals to offsite training is considerably restricted by the reality of insufficient security training funds – a factor that was consistently cited in survey responses and interviews. In addition, security managers stressed the importance of educating leadership regarding the value of the security mission. Without leadership support, security needs – especially training – are often unmet. The COCOMs anticipate the fielding of SPēD and believe it will assist in improving the proficiencies of security personnel. However, there were concerns that the program would not work as advertised or that it would never be fully implemented, primarily because similar programs have been attempted in the past. In addition, there was some concern that SPēD would be implemented with no consideration for how the program would be resourced and managed at the local level.

While most security managers knew about the SPēD program, some noted that they had only heard about it either via e-mails from their peers or through a one-time mailing. Additional outreach to the COCOMs would likely allay some of the concerns and better prepare security managers to administer the SPēD program at the local level. For example, providing information on the implementation DoD Manual 3305.13 could alleviate concerns about funding. The manual addresses the funding concerns by requiring the USD(I) to "ensure that sustainment requirements of the SPēD Certification Program and institutional accreditation… are identified and included in Planning, Programming, and Budgeting (PP&B) actions."

---

[4] The Advanced Technical Intelligence Center for Human Capital Development is a university and industry-focused research, education, and training nonprofit corporation in the Dayton, Ohio region consolidating technical intelligence education and training available in the DoD, national agencies, and civilian institutes and industry.

Half of Command security managers who were interviewed or responded to surveys did not feel that existing training adequately prepared security professionals to do their jobs successfully. Personnel performing security as a collateral duty were dissatisfied with the on-line training provided by the Center for Development of Security Excellence (formerly the DSS Academy).

Moreover, because assigned security duties were not a primary responsibility, collateral security professionals could not devote the time needed to become proficient in security matters. Training was also characterized as basic. As a result, security training did not address the range and complexities of security requirements. There was also a concern regarding the absence of an education requirement for security personnel to include the absence of required ongoing security training.

Where Command security managers were satisfied with security training, the security personnel were either full time civilians, the mission was functional rather than regional, or the Command was better resourced. Nevertheless, even amongst satisfied respondents, there was a desire for SPēD to be fielded, with the expectation that individuals would arrive with the necessary training to do requisite security tasks beginning with their first day on the job.

Command security managers provided detailed and comprehensive descriptions of the security training environment at their respective installations. One response is detailed below to afford readers an understanding of some of the security challenges experienced at the Command level.

Highlight – United States Southern Command (USSOUTHCOM). Under the leadership of a four-star commander, the USSOUTHCOM staff is organized into directorates, component commands, and military groups that represent USSOUTHCOM in the regions of Central America, South America, and the Caribbean. USSOUTHCOM is a joint command composed of military and civilian personnel representing the Army, Navy, Air Force, Marine Corps, Coast Guard, and several other federal agencies. It is responsible for providing contingency planning, operations, and security cooperation for Central and South America, the Caribbean (except U.S. commonwealths, territories, and possessions), and Cuba; as well as for the force protection of U.S. military resources at these locations. USSOUTHCOM is also responsible for ensuring the defense of the Panama Canal and canal area.

The USSOUTHCOM security staff is responsible for personnel, industrial, information, physical, and sensitive compartmented information security, as well as freedom of information act actions. Additional duties include visitor reception, badging, media destruction, foreign visits, plans, exercises, mandatory declassification, security reviews, pre-publication reviews, biometrics, technical security, technical security countermeasures, special access program control, special programs, Top Secret control, security investigations support, security services, and inspections. The Security Manager has over 30 years in the security field.

The Security Manager supervises seven civilian personnel with over 20 years average security experience and 13 military personnel in temporary slots who oftentimes do not have a security background. The staff provides security support to approximately 2,000 Command personnel. With respect to security training, the security manager noted that training either occurs on-line through the Center for Development of Security Excellence, via on-the-job training, "just in time,"[5] or through onsite ad hoc training.

The available training, however, does not prepare security professionals for the complexities of the USSOUTHCOM security mission. This is especially true for military personnel who are assigned on a temporary basis. Civilian security professionals, by comparison, bring an established skill set and, due to longevity, are able to successfully accomplish security tasks. Per the Security Manager, it takes 18 months to adequately train military personnel who come on board to fill security slots. This represents a very steep learning curve. Moreover, after 18 months, the assigned military personnel usually rotate into intelligence slots. For this reason, the Security Manager advocated that security should be performed exclusively by civilian personnel. In the absence of a dedicated civilian workforce, the Security Manager would prefer military personnel with a security military occupational specialty or at the very least an additional skill identifier in the security field.

The USSOUTHCOM Security Manager expressed a frustration that also was articulated by several other COCOM Security Managers concerning the manner in which security is funded. While not directly a training concern, funding directly affects the ability to give needed security training. Security programs have to compete for Operations and Maintenance funds against programs with greater visibility and security is often the loser in the competition for available funds. The Security Manager said security and other support mechanisms are often the first programs identified for funding cuts. If leadership does not support security requirements, security funds are often reallocated to other programs and security requirements, including training, go lacking. For this reason, USSOUTHCOM's Security Manager also supported improved security awareness training for leadership to assist leaders in understanding the importance of the security mission.

The Office of the Under Secretary of Defense for Intelligence – Efforts to Improve Security Training

The OUSD(I) has been working independently and in coordination with other DoD Components to facilitate the professionalization of DoD security personnel. Pursuant to Section 1122 of Public Law 109-163, "National Defense Authorization Act" for Fiscal Year 2006, January 6, 2006, the DoD issued DoD Instruction 1400.25, "DoD Civilian Personnel Management System: Volume 250, Civilian Strategic Human Capital Planning (SHCP)," November 18, 2008. The instruction established Functional Community Managers (FCMs) to address competency and knowledge issues for all DoD civilian personnel to include security professionals.

---

[5] "Just in time" is training rolled-out immediately prior to its usage. The advantage to implementing Just in time training is the shortened time between learning and the application of the information learned.

In June 2007, the USD(I) established the Human Capital Management Office to professionalize the DoD intelligence workforce. Moreover, the OUSD(I) is directing the DSS to establish a training, education, and certification program for security personnel. The SPēD program is partially complete, and complete roll-out of the program is not scheduled to be completed until 2014.

Functional Community Managers. DoD Instruction 1400.25 Volume 250 established OSD FCMs as senior functional leaders responsible for working with the DoD Components to monitor and track policy implementation. The OSD FCMs manage mission critical occupations with oversight from the Office of Personnel Management. There are nine mission-critical occupational areas which exist across several agencies while three occupational areas are sector-specific to national security agencies and the Veteran's Administration, the Department of Health and Human Services, and the DoD. The specific areas include intelligence and law enforcement of which security is a component. The OSD FCMs work in coordination with Component FCMs to implement and monitor workforce planning.

The OSD FCM for security is undertaking a comprehensive security review to develop, implement, and monitor workforce planning for the DoD security field. In furtherance of this effort, the OSD FCM for security is assessing "functional training and other strategies to ensure closure of identified competency gaps."[6] The OSD FCM for security fulfills this requirement in coordination with Component FCMs for security who identify constraints that impact the ability to meet end strength targets, the status of competency development, and human capital initiatives.

This information will assist in defining and validating the competencies of DoD security professionals. Component FCMs for security are expected to work in coordination with key stakeholders at the component level (e.g., human resource representatives) to assist the OSD FCM for security in determining their unique security requirements. With timely and accurate information from Component FCMs for security, the OSD FCM for security will be able to more accurately develop, implement, and monitor workforce planning for the DoD Security field. This coordinated approach should provide a better understanding of the DoD security landscape, assist in determining training requirements, and improve proficiencies across the Services and commands.

Human Capital Management Office. The Human Capital Management Office was established within the OUSD(I) to provide oversight, policy, and guidance for all DoD intelligence civilian and military (active and reserve) positions. The office is also the proponent for DoD training manual 3305.13-M and is tasked to develop, implement, and exercise policy oversight of the Defense Civilian Intelligence Personnel System and manage all Defense Intelligence training and education, and professional development. The Deputy Director of the office is also the DoD Intelligence Chief Learning Officer and the Chairman of the Defense Intelligence Training and Education Board.

---

[6] Memorandum "Functional Community Manager Designations," December 19, 2008, David S. C. Chu, Under Secretary of Defense for Personnel and Readiness.

The Deputy Director has worked to institute accreditation and certification procedures for the approximately eleven disciplines[7] that reside under the cognizance of the USD(I), including security. Training will be made available under the aegis of the Advanced Global Intelligence Learning Environment which will work as a clearinghouse for access to intelligence training across the various disciplines. The DSS Center for Development of Security Excellence training catalog is available via the Advanced Global Intelligence Learning Environment and points users to the Center for Development of Security Excellence Security Training, Education and Professionalization Portal, to include courses supporting the SPēD Certification Program.

Specific to security, the Deputy Director is working in coordination with the DoD Security Training Council to track the accreditation and certification process of SPēD. Per the Deputy Director, the COCOMs were identified as having the least training capability. Thus, the implementation of accessible structured on-line training courses will provide great benefit to security practitioners in the field. Moreover, once implemented and approved, credits from security courses will be applicable towards an academic degree.

To make the courses applicable towards a degree, DSS, is working to receive college equivalency recommendations for Center for Development of Security Excellence courses through the American Council on Education (ACE). Later, when the security education curriculum has been sufficiently developed, DSS will apply for accreditation through the Middle States Commission on Higher Education for degree granting eligibility. The Security Training, Education and Professionalization Portal will also feed certification information into the Defense Manpower Data Center to ensure transfer of certification credentials into official personnel records.

Defense Security Service Administration of Training. The DSS is a Defense agency under the authority, direction, and control of the USD(I) that provides security support to Defense agencies, the Services, 23 non-DoD federal agencies, and approximately 13,000 cleared contractor facilities. The organization's core missions are the National Industrial Security Program, and the Security Education Training and Awareness Program. The Security Education Training and Awareness Program oversees the Center for Development of Security Excellence, which provides security education and training to DoD security professionals through formal classroom, computer-based and web-based mechanisms.

The Security Education, Training and Awareness Directorate accomplishes its security education, training and professionalization missions through the Center for Development of Security Excellence and the DSS Academy. The Center for Development of Security Excellence is comprised of five divisions,[8] one of which is the Professionalization Division that is tasked with implementing the SPēD Certification Program.

---

[7] The disciplines include security, counterintelligence, cryptologic, foreign language, general intelligence, geospatial intelligence, human intelligence, joint intelligence, measurement and signature intelligence, leadership, and professional development.

[8] The five divisions are Education, Training, Security Professionalization, Multi-Media Production, and Research, Analysis and Innovation.

SPēD is a four level security certification program that is predicated on established skill standards and job competency requirements that were developed for DoD and approved by the DoD Security Training Council. The SPēD program identifies 11 accountabilities for security practitioners.[9]

In addition, the program identifies 16 security competencies with associated knowledge categories.[10] These requirements will be supported by curriculum that will provide security practitioners with the requisite training to become proficient in their areas of expertise and ensure that security personnel have the competencies to fulfill the identified security accountabilities.

Certification	Scope	Status
Security Fundamentals Professional Certification	Fundamentals, Principles, Methods, and Tools	Operational
Security Asset Protection Professional Certification	Application of Principles, Methods, and Tools	Beta Testing August-November 2011; Operational 2nd Quarter FY 2012
Security Program Integration Professional Certification	Risk Management and Program Management	In Development; Operational 2nd Quarter FY 2013
Security Enterprise Professional Certification	Enterprise Security Leaders	In Development; Operational 2nd Quarter FY 2014

In addition to the core SPēD Certification Program, three certification specialty areas are being integrated into the SPēD Certification Program. The specialty areas provide certification in special disciplinary or topic areas within the DoD security community. The specialty certifications are: DoD Personnel Security Adjudications, Special Access Programs, and DSS Industrial Security Oversight.

The specifics of the certification aspects of the SPēD program will be discussed in greater detail in Finding B.

With respect to training, security courses supporting preparation for the Security Fundamentals Professional Certification are currently available via on-line distance learning. Security courses supporting preparation for the Security Asset Protection Professional Certification will be available through classroom instruction as well as on-line, as a distance learning option.

---

[9] The 11 accountabilities are assess risks; manage risks; execute security awareness training and education; counsel stakeholders on security related concerns, issues, and challenges; evaluate program effectiveness; analyze duties to protect assets which require protection; manage resources; respond to security incidents; support execution of the classification decision process; support execution of the security clearance process; and generate security plans.

[10] The 16 competencies are classification management; communications security; continuity of operations planning; counterintelligence; incident response; information assurance/cyber-security; information security; law enforcement; operations security; personnel security; physical security; program security; security education and training; security program management; security tools and methods; and vulnerabilities assessment and management.

Courses supporting the Security Program Integration Professional Certification and the Security Enterprise Professional Certification will be identified or developed as required to support certification preparation. The courses will incorporate existing curriculum offered by federal agencies that currently provide security training validated as meeting DoD Security Skills Standards. To ensure courses are available to security professionals, DSS has a website, registrar, and learning management systems to schedule and support SPēD.

An on-line diagnostic test for the Security Fundamentals Professional Certification is available to assist security professionals in identifying knowledge gaps aiding them in their preparation to certification testing. The diagnostic test evaluates knowledge area weaknesses and identifies courses that will assist in developing the proficiencies needed to achieve certification at the first level. A similar diagnostic test will be formulated for the second level of certification when it is implemented.

DSS estimates that the development of a web-based course costs approximately $165,000 to $250,000 depending on the complexity of the course. While web-based delivery will provide training at a savings for outside organizations, cost is not the overarching determinant for how training is delivered. The decision for the delivery method (e.g., on-line, classroom or blended) is primarily guided by how well the method achieves course objectives. This determination is made during the analysis phase of course structuring which establishes who and what must be trained, and when and where training will occur.

The design phase provides the blueprint for the training program while the development phase builds on learning objectives. The course is then implemented providing a basis for ongoing evaluation of course efficacies against established standards and criteria. The ability to provide web-based instruction ensures that DSS training is available to the widest audience possible in a cost effective manner. The delivery method, however, will consistently be based on circumstances pertaining to size of student base, locations of individuals in a targeted training population, and the complexity of the task being trained. Additionally, DSS hosts community curriculum reviews on an annual basis where representatives from the Services, USD(I), and the 4th Estate[11] participate in the review of current Center for Development of Security Excellence curricula and identify future course development requirements thereby ensuring curriculum relevancy.

The SPēD Certification Program will assist in the professionalization of the security workforce. SPēD is slated to be implemented over a four year period with a new certification level introduced each year. The 4-year period addresses numerous considerations:

- ensures the Components can implement the program as it rolls out;
- ensures the program is effectively developed to meet established accreditation criteria and sound program design; and
- facilitates the time necessary to develop the supporting training and education.

[11] DoD 4th Estate includes the Office of the Secretary of Defense, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense that are not in the Military Departments or the Combatant Commands.

According to DSS staff, the development of the current SPēD Certification Program began in April 2009 as a DoD security community effort, shortly after the issuance of DoD Instruction 330.13. The development of SPēD has been the primary focus of the DoD Security Training Council and has involved representatives from the Military Departments and the 4th Estate. Prior to this effort, there was an earlier training and certification program effort that was under development from 2005-2007. That particular effort was also called SPēD. It unfortunately lacked the implementing guidance and funding to succeed. The name SPēD was retained for the current program based on the naming convention called out in DoD Instruction 3305.13. The current SPēD Certification Program is a new effort based upon updated skill standards, competencies, and expanded community involvement in the design and development of the program.

There are concerns expressed by interviewees and respondents, however, about whether the program will ever be implemented. Moreover, the concerns expressed regarding the implementation of SPēD are not unfounded. Our review indicates that there have been previous efforts to field a structured security training and professionalization program. Some interviewees noted that similar efforts have been ongoing for at least eight years, perhaps longer, with no concrete results.

It appears, however, that elements within the Department are waiting on the implementation of SPēD to address their security training and certification needs. For this reason, outreach to Department organizations needs to be consistent and ongoing to effectively communicate the status of a program that is both sought after and needed. The DSS has noted that they are increasing their staff to improve outreach to DoD Components. This will be necessary to allay concerns about SPēD implementation.

Conclusion

Security training within the Department is not coordinated and occurs primarily on-the-job or is very limited, resulting in differing levels of proficiencies across the DoD security enterprise. Accordingly, DoD organizations are anticipating the structure that a security certification program will provide. With the implementation of SPēD and the attendant diagnostic exams, security professionals will be able to identify training areas in which they are deficient and increase their competencies within the security field. There remains concern however, about whether SPēD will be implemented, as similar efforts have not borne results in the past. To address this concern, greater outreach will be required to Defense organizations, and the Combatant Commands.

A separate concern involves the manner in which security is funded. Security funds are primarily drawn from Operations and Maintenance funds and as such can be reallocated at command discretion. Our interviews and survey responses found that this reallocation occurs more frequently with training funds. DoD Manual 3305.13-M "Security Accreditation and Certification Manual," March 14, 2011, directs the USD(I) to ensure that sustainment requirements of the SPēD Certification Program and institutional accreditation are identified and included during the program and budget build and during development of supplemental requests. To accomplish this, the USD(I) will review resource requests and provide additional guidance as needed. These provisions can ensure that funding for the SPēD certification program will be available. However, in the absence of a dedicated funding line, an oversight mechanism will be required to track security funds necessary to ensure the availability of adequate resources for the professionalization of security personnel.

Recommendation, Management Comments, and Our Response

A1. We recommend that the Director, Defense Security Service develop an awareness plan that will inform Services and Components of the implementation status of SPēD and educate security managers about the benefits of the program - identifying program milestones and addressing concerns regarding program implementation.

Management Comments

On behalf of the Director, Defense Security Service, the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, concurred, stating that the Defense Security Service is actively marketing the SPeD Certification Program and provided a list of new initiatives along with corresponding dates designed to promote the program and provide status updates on the program to the DoD Community. The Defense Security Service will continue with these current outreach activities and will work closely with the Defense Intelligence Agency to address Combatant Command concerns.

Our Response

The comments of the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, are responsive and meet the intent of the recommendation. The efforts articulated in the response are commendable, especially the inclusion of eight initiatives to improve outreach since the publishing of the draft report on June 6, 2011.

Recommendation, Management Comments, and Our Response

A2. We recommend that the Deputy Under Secretary of Defense for Intelligence and Security develop a mechanism to provide consistent oversight and monitoring of security funds that are allocated to support the implementation and sustainment of the SPēD certification program and ensure funds are not repurposed for non-security training efforts.

Management Comments

The Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, partially concurred, stating that attempts to develop a mechanism to provide consistent oversight and monitoring of security funds that are allocated to support the implementation and sustainment of the SPēD certification program and ensure funds are not repurposed for non-security training efforts have been resisted by some components citing abrogation of authorities. However, the Director of Security further stated that the Office of the Under Secretary of Defense for Intelligence will explore, with the Office of the Under Secretary of Defense for Personnel and Readiness and the DoD Comptroller, options for implementation of an oversight and monitoring plan, and forward the plan to the Deputy Under Secretary of Defense for Intelligence and Security, in January 2012.

Our Response

The comments of the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, are responsive and meet the intent of the recommendation.

Finding B. DoD Needs to Provide a Mechanism for Security Professionalization in a Timely Manner Through a Standardized Certification Process

Certification for DoD security professionals within the GS-0080 series is in the early preliminary stages. Responses to our survey and interviews indicate that the DoD security community is not familiar with the SPēD Certification Program and the certification requirements for DoD security personnel. An earlier assessment of the security field noted that security has few entry barriers or professionalization criteria.[12] While progress is being made, without the success of SPēD, the credibility of the security profession could be adversely impacted.

The Air Force is alone in proceeding with a training and professionalization program that is closely aligned with the planned SPēD Certification Program. In addition, under SPēD, DoD activities will align planned certification standards with existing position descriptions. These undertakings will assist in the professionalization of security personnel. The efforts, however, need to be implemented in a timely and consistent manner.

Policy Related to Certification across the DoD Security Enterprise

DoD Directive 5143.01, DoD Instruction 3315.11, and DoD Instruction 3305.13 established the authorities of the USD(I), established policies and procedures with respect to the DoD Intelligence Human Capital Programs, and established policy, standards, and procedures for the conduct of DoD security education, training, and professional development, respectively. DoD Manual 3305.13-M is the implementation guide for DoD Instruction 3305.13 and further defines the roles and responsibilities of the USD(I), the Under Secretary of Defense for Personnel and Readiness, the DSS, the DoD Security Training Council, and Defense Components, relating to security education, training, and professional development.

DoD Manual 3305.13-M, "Security Accreditation and Certification Manual," March 14, 2011, provides guidance and procedures for developing and implementing a security workforce certification program and establishes roles and responsibilities for the development, implementation, and maintenance of the DoD SPēD Certification Program. Specific to certification, DoD Manual 3305.13-M specifies that the SPēD Certification program will:

- Promote a common and shared understanding of both security's functional tasks and the knowledge and skills associated with the competencies required to perform those functional tasks (hereafter, referred to as the security essential body of knowledge);

[12] Defense Personnel Security Research Center Technical Report 06-01,"Development and Application of Skill Standards for Security Practitioners," July 2006

- Promote an interoperable DoD security workforce by establishing uniform processes for assessing knowledge and skill, and determining whether a member of the security workforce has demonstrated mastery of relevant segments of security's essential body of knowledge;
- Facilitate sound professional development and training by ensuring, through a formal evaluation process, that such programs provide individuals the opportunity to acquire the documented security essential body of knowledge; and,
- Develop a workforce of certified security professionals who will provide the best possible guidance and support to DoD managers and leaders responsible for protecting DoD's personnel, information, facilities, operations, and activities.

Security Professional Certification

The professionalization of GS-0080 security professionals through a structured certification program is in its preliminary stages with the implementation of the first level of certification, the Security Fundamentals Professional Certification. OUSD(I) efforts to put forth a standardized certification program rests with the DSS through the SPēD Certification Program as set forth in DoD Manual 3305.13-M. The COCOMs, surveyed organizations, and the majority of the Services do not have an existing professionalization program to assess the proficiencies of their security personnel. The Air Force, however, is in the vanguard of Services and Commands and stands ready to implement a professionalization and development program for their security workforce.

Air Force Professionalization Program. The Air Force is in the final phases of fielding a training and professionalization program for their security professionals. This is a direct result of the creation of the Information Protection Directorate and is also a reflection of the Air Force's decision to apply an enterprise approach to all areas of security. The Air Force is also integrating risk mitigation into the security paradigm. The goal is to ensure that Air force personnel understand and apply risk management principles at all organizational levels to include the tactical level. To that end, the Air Force is committed to implementing professionalization requirements for their security professionals that incorporate concepts of risk management.

The Air Force professionalization program consists of four levels integrating the SPēD Certification Program at each level. Level-I – Security Fundamentals will provide potential security practitioners with the basic methods and tools to operate in entry level security positions. The courses will be entry level and as such will be open to all Air Force employees with no course prerequisites. In addition to completing courses, the employee will have to obtain concurrence from his or her immediate supervisor noting that the employee has displayed the appropriate level of professionalism and job performance to be granted the Security Fundamentals Professional Certification.

Acceptance into the Level-II – Security Asset Protection professionalization courses is predicated on completion of Level-I professionalization and one year of federal security-related employment. The applicants will be selected from the Air Force military, civilian, and contractor security workforce. Level-II candidates will have to be in security related billets as defined by DoD Manual 3305.13-M in order to apply for the Security Asset Protection Professional Certification candidacy. In addition, applicants must have supervisory concurrence that they have displayed the appropriate level of professionalism and job performance to be granted certification candidate status.

Level-III – Security Program Integration incorporates risk management and program management principles and is intended for military and civilian personnel in or being groomed for management or senior advisory positions. Applicants must have five years of federal security-related employment or be currently assigned to a billet requiring the Security Program Integration Professional Certification. Security Fundamentals Professional Certification is a prerequisite and the candidate must be in a security related billet as defined in DoD Manual 3305.13-M to apply for certification candidacy.

Level-IV – Security Enterprise Professional Certification is intended for military and civilian personnel in or being prepared for senior level management or strategic positions within the DoD. In addition, applicants must have 10 years of federal security-related employment or be an incumbent to a Level-IV billet. The applicants must have attained the Security Program Integration Professional Certification and have their immediate supervisor's concurrence that the employee has displayed the appropriate level of professionalism and job performance to be granted certification candidate status. Finally, the employee must be sponsored by an owning Major Command Information Protection office (or equivalent) or a member of the Air Force Security Advisory Council occupying a GS-15/Computer Network Defense Enclave Security Division level or above. The applicant must also be vectored by an Air Force developmental team, unless currently serving in a billet "coded" for "security enterprise certification."

The Air Force initiated the process for the professional development of security personnel in 2006. In 2008, the design for professional development of the Air Force security workforce was put in place. The career path structure was approved in 2009 and position descriptions were standardized in 2010. The Air Force anticipates full implementation of security workforce professional development this year. Moreover, the Air Force has moved toward civilianizing its security workforce. This will likely minimize any issues related to the appropriate accrediting of military personnel performing security missions. Air Force standards will require Level-II (Security Asset Protection Professional Certification) certification for their security practitioners to be considered fully successful. This will likely differ from other Services and Commands that will only require Level-I (Security Fundamentals Professional Certification) competencies and could be problematic as the standardized protection of DoD resources across the security enterprise should be predicated on consistent performance criteria across the Department.

Office of the Under Secretary of Defense for Intelligence Certification Efforts. As noted in previous sections, the OUSD(I) has set forth policy to further the education and professionalization of DoD security personnel. The OSD FCM for security is undertaking a comprehensive security review to develop, implement, and monitor workforce planning for the security field. The OSD FCM for security is engaged in strategic Human Capital Planning and has designated Component FCMs for security to assist in analyzing the security workforce (to include defining competencies and conducting gap analyses) and implementing strategy (e.g., setting performance metrics and staff plans). The Human Capital Management Office is overseeing the movement of the approximately nine disciplines under the cognizance of the USD(I) to accreditation and certification requirements. Certification of the security workforce, however, is being implemented primarily by the DSS, which was tasked to establish the SPēD security education training and professional development program.

Defense Security Service Certification Efforts. The Department has long sought to establish a certification program for their security professionals. Interviewees have noted that similar efforts have been ongoing at least eight years. That previous undertakings have not been successful, explains the concerns of surveyed commands and organizations that current efforts will not bear fruit.

The 2009 National Intelligence Strategy Enterprise Objective 6, promotes the development of a "diverse, results focused, and high-performing workforce capable of providing the technical expertise and exceptional leadership necessary to address… security challenges." The SPēD program meets this objective and consists of three components under the Center for Development of Security Excellence: Security Professionalization, Training, and Education. The first element is overseen by the Professionalization Division responsible the SPēD Certification Program, security career maps, DoD security journals, and security workshops and forums. The Training Division is the primary agent for security training. The Education Division oversees the security education program.

The certification program was developed in coordination with the Department of Defense Security Training Council, which functions as the advisory body on DoD security training and is chaired by the DSS. The DoD Security Training Council assisted in the formulation of security skill standards and instituted the development of the SPēD program.

DSS also used the services of Global Skills X-change, a professional services firm that specializes in designing workforce education strategies. Global Skills X-change conducted interviews and facilitated meetings to identify nine security disciplines and to define how the disciplines were interrelated. Global Skills X-change also compiled documents that identified the scope of work, knowledge and skills associated with the nine security disciplines, and drafted action statements for each area. Subject matter experts reviewed the statements and provided changes, which were subsequently deconflicted by Global Skills X-change. Similar steps were taken in the identification of security accountabilities. Global Skills X-change also drafted terminal and enabling learning objectives statements to define knowledge and capability requirements for each of the identified knowledge categories for the first and second levels.

The resulting certification structure consists of four levels, which are identified as Security Fundamentals Professional Certification (Level-I), Security Asset Protection Professional Certification (Level-II), Security Program Integration Professional Certification (Level-III) and Security Enterprise Professional Certification (Level-IV). In addition to the standard core disciplines, the SPeD certification program will include specialty certifications such as DoD Personnel Security Adjudications, Special Access Programs, DSS Industrial Security Oversight.

Final certification standards for Security Fundamentals Professional Certification and the Security Asset Protection Professional Certification have been developed. Based on this information, security professionals are conferred Security Fundamentals Professional Certification if they are able to demonstrate an understanding of the central tenets of security principles and display a wide breadth of knowledge of integral security concepts. Candidates must display an understanding of the security landscape, asset protection principles, security countermeasures, and security methods and tools. Mastery of the security landscape requires a comprehension of security policies and the structure and policy guidance of associated security programs.

Asset protection will require an understanding of the security operational landscape, information security principles, physical security principles, and program security principles. A command of security countermeasures concepts will entail an awareness of information security countermeasures, personnel security countermeasures, physical security countermeasures, and program security countermeasure principles.

Proficiency in security methods and tools requires an understanding of basic security forms and security systems. DSS completed beta testing for Security Fundamentals Professional Certification (Level-I) in December 2010 and opened the operational version to the DoD security community in February 2011. The Security Asset Protection professional Certification (Level-II) will be beta tested from August to November 2011 with full operational capability planned for the 2nd quarter of FY 2012.

Certification for Security Asset Protection Professional Certification (Level-II) will be conferred upon candidates who demonstrate an understanding of advanced security concepts and theories and can apply foundational security concepts, principles, and practices. Candidates will be required to master two advanced security principles (1) security tactics, techniques, and procedures and (2) security as risk management. Each principle has identified sub-topics some of which are shared concepts. For example, security practitioners will have to understand the tactics, techniques, and procedures associated with counterintelligence concepts. They will also have to address counterintelligence's role in managing risks to DoD assets. Similar shared concepts include classification levels and types, classification management, information protection concepts, and physical security concepts with associated elements. Whether shared or unique, all concepts fall under the rubric of security principles. The Security Program Integration Professional Certification blueprint has been developed and development of the assessment instruments is currently underway. The Security Program Integration Professional Certification will be beta tested in FY 2012 and planned for release in FY 2013. The Security Enterprise Professional Certification is currently a broad concept and will be addressed in more depth in FY 2012 and scheduled for release in FY 2014.

Implementation of the SPēD certification program commenced with the signing of the DoD Manual 3305.13-M on March, 14, 2011. DoD organizations are required to submit implementation plans one day plus one year after the manual was signed i.e., March 15, 2012. After that, organizations will have five years to implement their respective plans. DSS is developing a template that DoD organizations can use to create their plans; however, the specifics of the implementation plans will be unique to the organization and not consistent across the Department. For example, the certification requirements for a security position in one organization may differ considerably from requirements in another organization and yet the positions could be similar in nature. Furthermore, DSS has not yet fully developed the structure for Security Program Integration (Level-III) and Security Enterprise (Level-IV) certification. DSS has provided updated guidance indicating that organizations will only address specific implementation of each level of certification as they become available for their required implementation plans required by DoD 3305.13-M.

Conclusion

The DoD has worked towards the creation of a certification program for security personnel for at least 8 years. In addition, there has been previous Congressional interest in aggregating security training and professionalization across government agencies. House Resolution 6249 - Interagency National Security Professional Education, Administration, and Development System Act of 2010, advocated the creation of "a system to educate, train and develop interagency national security professionals across the Government." The proposal still has support from current Congressional members. If some version of the proposal is adopted, it will likely impact the implementation of a DoD-centered security training and professionalization program.

While DoD Manual 3305.13-M has been issued establishing the requirement for the implementation of the SPēD certification program, organizations will not be required to provide implementation plans for SPēD until March 15, 2012. Moreover, full implementation is not mandated until 2017. There was concern expressed in interviews that the extended timeframe could present barriers to full implementation. The uncertain status of a professionalization and development program across the national security enterprise creates an even more compelling argument for the timely implementation of SPēD.

Details of the SPēD certification program are finalized for the first two levels. The third level is currently in development and the fourth level will be addressed later in FY 2012. To address concerns regarding the development of implementation plans without specific information on the levels in development, DSS has revised implementation plan requirements to address only active certifications. As a result, the implementation plans due on March 15, 2012 will only address implementation of the Security Fundamentals Professional Certification. Moreover, the standards for implementation will be organization-specific and as such will not be consistent.

At issue will be the variances that will result across the Department as individual organizations apply differing proficiency standards for their respective security professionals. For example, while one organization may view Level-I certification as the standard for a fully competent security professional, another might require Level-II certification. Security missions operating in a joint environment will be particularly affected by the differing skill sets and proficiencies of security professionals who will be tasked to coordinate their security efforts.

Recommendation, Management Comments, and Our Response

B1. We recommend that the Director, Defense Security Service, establish an accelerated schedule for the development, testing, and implementation of Levels III and IV of the Security Professional Education and Development program similar to Levels I and II, to ensure consistency in the application of the program across the Department.

Management Comments

On behalf of the Director, Defense Security Service, the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, non-concurred, stating that SPeD is being developed over a four-year period, with an additional three specialty areas also being integrated into the SPeD Certification Program during this four-year period to address critical security community requirements. The Director of Security expressed that caution must be exercised in accelerating the roll out of the SPeD Certification Program beyond the current projected schedule for the following reasons: Lessons have been learned from the development of the first two levels that will benefit the final two levels ensuring smoother development and implementation and that DoD Components must be capable of implementing the certification program. Current implementation efforts demonstrated that the components need time to address component unique implementation issues. Development of the SPeD Certification Program requires beta testing of each level with target populations of security professionals. With prerequisite certification requirements, DSS has to roll out the program over time to ensure that beta test participants possess the necessary prerequisites and that the beta test audience is large enough to produce valid statistical data. Additionally, training and education courses are being updated and/or developed to address the skills and competencies required for each certification.

Our Response

Although the Defense Security Service disagreed with the recommendation, implementation actions taken to date to ensure that SPeD is being developed in a consistent, thoughtful, and measured manner; along with a detailed implementation schedule, satisfies the intent of the recommendation.

B2. We recommend that the Director, Defense Security Service, examine the current implementation strategy and develop a standardized Security Professional Education and Development certification program implementation plan for use by all organizations and commands. The implementation plan should include a means to track those with certifications and the level of certification.

Management Comments

On behalf of the Director, Defense Security Service, the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, concurred. The Defense Security Service is developing an implementation plan template. On July 18, 2011 an interim implementation plan template was forwarded to DoD Components. The interim plan addresses only the implementation of the Security Fundamentals Professional Certification through FY 2012. The standardized template being developed will be designed to address the addition of certifications as they become available rather than requiring Components to address future certifications before they are operational. The standardized template will be distributed by September 2012. Additionally, both the Security Training, Education and Professionalization Portal and the Defense Manpower Data Center will be used to track certifications.

Our Response

The comments of the Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security, are responsive and meet the intent of the recommendation. We do request that management provide a copy of the standardized template upon completion in September 2012.

APPENDIX A. Scope and Methodology

This assessment was conducted in accordance with Quality Standards for Inspections and Evaluations issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the assessment to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. The evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives. To accomplish our assessment, we:

- reviewed relevant policies, regulations, and related studies;
- conducted a survey of 45 Defense Component security managers; and
- interviewed those managers, along with additional Department officials responsible for security training and related policy development and implementation.

Because of the size and complexity of addressing security within the Department of Defense, we are performing this assessment in phases. The previous phase addressed tracking and measuring security costs. This phase focused on training, certification, and professionalization; and the remaining phases will focus on classification and grading, and security policies.

APPENDIX B. Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoDIG) have issued three reports that have addressed security specific to the DoD and national security enterprise. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodigmil/Ir/reports.

GAO

GAO Report No. GAO-11-108, "An Overview of Professional Development Activities Intended to Improve Interagency Collaboration," November 2010

GAO Report No. GAO-09-0904SP, "Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing," September 2009

DoD IG

DoD IG Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs," August 6, 2010

Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

SEP 14 2011

INTELLIGENCE

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Comments on DoD IG Draft Report: Assessment of Security Within the DoD – Training, Certification, and Professionalization Project No. D2010-DINT01-0066.001

The Defense Security Service (DSS) and the Human Capital Management Office have reviewed the subject draft. Both Security Directorate and DSS have comments on the content of the draft. More specifically, regarding your recommendations:

A1. We recommend that the Director, DSS develop an awareness plan that will inform Services and Components of the implementation status of the Security Professional Education Development Program (SPēD) and educate security managers about the benefits of the program - identifying program milestones and addressing concerns regarding program implementation.

Concur. DSS has been actively marketing the SPēD Certification Program since its inception and continues to promote the program and provide status updates on the program to the DoD Community. The following provides additional details regarding SPēD communications:

- A SPēD marketing plan was initially developed and shared with the DoD Security Training Council membership in August 2010. The plan outlined the marketing plan for the Security Fundamentals Professional Certification (SFPC). Since then, a new plan has been developed (completed July 21, 2011). The plans utilize a multi-prong approach, leveraging a variety of outreach tools.
- A SPēD webpage was developed early in the program and has been updated on a continual basis. The webpage includes links to SPēD Certifications, About SPēD, SPēD FAQs, SPēD Resources, SPēD Diagnostic Tools, SPēD Test Sites, SPēD Contacts, and SPēD News (last updated the week ending August 19, 2011).
- DSS has provided and continues to provide SPēD briefings to DoD Components. Briefings are available upon request. Additionally, DSS has sought out DoD Components in order to educate them on SPēD (last Component meeting was with Army the week ending August 19, 2011).
- DSS provides presentations at various security conferences to include the DoD Worldwide Security Conferences and the DoD European Security Conference. Upcoming events include the Navy Security Conference in September 2011, the DARPA Conference in October 2011, and the SSO Conference in November 2011.
- DSS sponsors a Center for Development of Security Excellence (CDSE) booth that also provides SPēD promotional and information materials at major security conferences and events (supported events over the past year included NCMS, ASIS, OPSEC, IMPACT, DARPA, SSO, etc.).
- DSS utilizes social media including Twitter, Facebook and YouTube to promote the SPēD Certification Program (established March 2011).
- DSS produces quarterly SPēD newsletters that are pushed to the community and made available on the SPēD website (latest newsletter cover was released the 3rd Qtr or FY11).
- DSS provides a weekly SPēD update to DoD Components.

Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security Comments

- SPēD updates are provided at each quarterly DoD Security Training Council (DSTC) meeting (last meeting held on June 6, 2011, next meeting scheduled for September 29, 2011).
- DSS has provided SPēD promotional tools to DoD Component SPēD point of contacts (POC).
- The SPēD Certification Program was the subject of a Pentagon Channel story (September 2010).
- A SPēD mailbox has been established and maintained.
- DSS hosts monthly SPēD certification conference calls with Component SPēD POCs to address program questions and implementation issues (held the 3rd Thursday of each month with a morning and afternoon session in order to accommodate European and Pacific time zones; the last series of calls were held on August 18, 2011).
- A SPēD forum was held on September 30, 2010, and available via web streaming. The day-long event provided SPēD Certification Program overview and a Q&A session. The forum was supported by the Under Secretary of Defense for Intelligence/Deputy Under Secretary of Defense (Intelligence and Security) (USD(I)/DUSD(I&S)).

DSS will continue with the current outreach activities listed above. DSS is also working closely with the Defense Intelligence Agency to address Combatant Command (COCOM) concerns. DSS will provide SPēD Certification Program briefings and testing at the upcoming SSO Conference. Additionally, DSS will continue proactive outreach efforts with DoD Components and Activities.

A2. We recommend that the DUSD(I&S) develop a mechanism to provide consistent oversight and monitoring of security funds that are allocated to support the implementation and sustainment of the SPēD Certification Program and ensure funds are not repurposed for non-security training efforts

Partially concur. This is a noble goal, however attempts to do this have been resisted by some components citing abrogation of authorities. OUSD(I) will explore with the Office of the Secretary of Defense for Personnel and Readiness and the DoD Comptroller options for implementation and forward a plan to DUSD(I&S) by January 1, 2012.

B1. Establish an accelerated schedule for the development, testing, and implementation of levels III and IV of SPēD, similar to levels I and II, to ensure consistency in the application of the program across the Department.

Non-concur. SPēD is being developed over a four-year period. Three specialty areas are also being integrated into the SPēD Certification Program during this four-year period to address critical security community requirements.

Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security Comments

The current development schedule for SPēD Certifications are:

Certification	Status	Operational Date
Security Fundamentals Professional Certification	Operational	February 2011
Security Asset Protection Professional Certification	Beta Test (Aug-Nov 11)	February 2012
Security Program Integration Professional Certification	Development	February 2013
Security Enterprise Professional Certification	Preliminary Development	February 2014
DoD Personnel Security Adjudicator Certification	Program Review and Certification Assessment Revision	August 2010 Revised Assessment September 2011
Special Program Security Certification	Program Review and Certification Assessment Revision	Revised Assessment – Journeyman level - November 2011 Master level - TBD
DSS Industrial Security Professional Certification	Preliminary Development	September 2012

Caution must be exercised in accelerating the roll out of the SPēD Certification Program beyond the current projected schedule for the following reasons:

- DoD Components must be capable of implementing the certification program. Current implementation of the Security Fundamentals Professional Certification has demonstrated that the components need time to address component unique implementation issues.
- Development of the SPēD Certification Program requires beta testing of each level with target populations of security professionals. With prerequisite certification

Director of Security, Office of the Deputy Under Secretary of Defense for Intelligence and Security Comments

requirements, DSS has to roll out the program over time to ensure that beta test participants possess the necessary prerequisites and that the beta test audience is large enough to produce valid statistical data.
- Training and education courses are being updated and/or developed to address the skills and competencies required for each certification.
- Lessons have been learned from the development of SFPC and SAPPC that will benefit SPIPC and SEPC to ensuring smoother development and implementation.

B2. Examine the current implementation strategy and develop a standardized SPēD Certification Program implementation plan for use by all organizations and commands. The implementation plan should include a means to track those with certifications and the level of certification.

Concur. DSS has been pursuing this action since the inception of the current SPēD development effort. Both the Security Training, Education and Professionalization Portal (STEPP) and the Defense Manpower Data Center (DMDC) will be used to track certifications. STEPP is currently serving as the SPēD certification records data system. DSS is currently working with DMDC to establish the SPēD records data transmission capability to transfer data to Official Personnel Records. Funding documents for DMDC support were executed in August 2011.

DSS is developing an implementation plan template. Development of the template has been affected by the delay in approval of 3305.13-M. An interim implementation plan template was forwarded to DoD Components on July 18, 2011. The interim plan addresses only the implementation of the Security Fundamentals Professional Certification through FY12. The standardized template being developed will be designed to address the addition of certifications as they become available rather than requiring Components to address future certifications before they are operational. The standardized template will be distributed by September 2012.

Security Directorate looks forward to working with the Office of the Inspector General to resolve these comments and publish the report. The points of contact are Stephen Lewis, (703) 604-2768 or Stephen.Lewis@osd.mil and Denise Humphrey, (410) 865-3470 or Denise.Humphrey@dss.mil.

Timothy A. Davis
Director of Security

Inspector General
Department of Defense