The Pathway to Success Begins with

SPēD

Security Professional Education Development

Security Asset Protection Professional Certification

Candidate Handbook

October 2, 2012

Defense Security Service
Center for Development of Security Excellence
938 Elkridge Landing Road
Linthicum, MD 21090
www.dss.mil

Table of Contents

Table of Contents

Message from the Director, Defense Security Service

On behalf of the Defense Security Service, and as the functional manager for security training in the Department of Defense I want to thank you for your interest and participation in the Security Professional Education Development (SPēD) Certification Program. The Department is confronting times of critical and dynamic change, and we are adapting to these challenges during a period of larger nationwide and global transition. The challenges to security professionals in particular have never been greater or more complex than they are today. The Security Fundamentals Professional Certification (SFPC) serves as a visible symbol of your expertise and skill in protecting national security. The SFPC credential will be a testimonial to your experience and a significant milestone in your security career.

The information in this Candidate Handbook is designed to support you and provide important information about the program. The SPēD Program is a vital part of the Department's initiative for professionalizing the security workforce. You are among a select few employees who are leading this effort.

I wish you the best in your security career and commend you for your pursuit of excellence in the security profession.

Stanley L. Sims
Director
Defense Security Service

Introduction

This *Candidate Handbook* provides individuals with an overview of the SPēD Certification Program, including benefits and objectives. The Defense Security Service (DSS) administers the SPēD Certification Program under the direction of the Office of the Under Secretary of Defense for Intelligence (OUSD(I)).

The Security Asset Protection Professional Certification (SAPPC) is one certification in the SPēD Certification Program. This *Candidate Handbook* contains information regarding SAPPC eligibility, registration, and assessment.

What is the SPēD Certification Program?

The SPēD Certification Program is part of the Department of Defense's (DoD) initiative to professionalize the security workforce. The SPēD Certification Program ensures that security practitioners can demonstrate proficiency in a common set of competencies. The purpose of the SPēD Certification Program is to promote interoperability across DoD and among the different security disciplines; facilitate professional development and training; and develop a workforce of certified security professionals.

SPēD Certification Overview

Governance

The Department of Defense Security Training Council (DSTC), in its role as the governing body for the SPēD Certification Program, has approved the design as well as the policies and procedures necessary to establish the SAPPC as a key element of the SPēD Professional Certification Program. DoD Instruction 3305.13, "DoD Security Training," December 18, 2007, establishes the DSTC as an advisory body on DoD security training and responsible for promoting certification programs for the security workforce. The DSTC reports to the Defense Intelligence Training and Education Board (DITEB), which has established the DoD-wide security and intelligence community certification requirement. On August 18, 2009, the DSTC agreed to focus on the development and governance of the SPēD Certification Program. The DSTC is responsible for:

- Certification Administration Oversight
- Technical Development Oversight
- Certification Governance

The DSTC is composed of security professionals and managers from 23 DoD Components. The DSTC represents the shared interests of all DoD Components and their respective workforce in the design, management, and maintenance of certification.

Benefits of SPēD Certification

For individuals:

- Fosters understanding of the concepts and principles deemed critical to protect DoD assets
- Promotes professional development

For employers:

- Provides a reference point for determining an individual's understanding of the concepts and principles deemed critical to protect DoD assets
- Identifies competent professionals in the security discipline

For the profession:

- Defines standards and drives professional accountability
- Assures continuing competency of certificants

SPēD Certification Program Structure

The SPēD Certification Program is an essential element of the overall SPēD program for the professional development of security professionals. The SPēD Certification Program is comprised of four core certifications described below and multiple specialty certifications that target more narrow security disciplines and responsibilities.

The SAPPC serves as a valid and reliable indicator of a security practitioner's ability to apply foundational security concepts, principles, and practices the DoD community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets.

Certification	Acronym	Certification Description
Security Fundamentals Professional Certification	SFPC	The individual understands foundational security concepts, principles, and practices.
Security Asset Protection Professional Certification	SAPPC	The individual applies foundational security concepts, principles, and practices.
Security Program Integration Professional Certification	SPIPC	The individual understands and applies risk assessment and security program management based on security concepts, principles, and practices.
Security Enterprise Professional Certification	SEPC	The individual understands and applies concepts, principles, and practices for managing enterprise-wide security.

This *Candidate Handbook* addresses ONLY the description and related policies and practices associated with the SAPPC.

SAPPC Policy Matrix

The certification policy matrix summarizes the essential characteristics and design requirements of SAPPC.

Security Asset Protection *Professional Certification*		
The Security Asset Protection Professional Certification is open to all personnel affiliated with a Federal Agency and/or the National Industrial Security Program. Volunteers who submit to and subsequently meet the SAPPC program requirements can be conferred the SAPPC. The Security Asset Protection Professional Certification is ideal for: • Personnel who will be or are already performing security functions as an additional and/or embedded duty on behalf of (and as specified by) a DoD Component • Personnel who are working toward or already occupy full-time security positions for which attainment of this certification has been deemed a requirement or a professional development milestone		
To obtain the Security Asset Protection Professional Certification, the individual must:		**Waivers**
Prerequisites:	• Be a certificant of the Security Fundamentals Professional Certification (SFPC) • Be in "good standing" by having his or her employment status and/or affiliation confirmed by Component's or Agency's SPēD Program Management Office (PMO) Point of Contact (POC)	NONE
Requirements:	• Successfully meet the certification assessment's qualifying score • Be designated by his or her employing Component or Agency as a candidate of "good standing"	NONE
To maintain the Security Asset Protection Professional Certification, the certification holder must:		**Waivers**
Requirements:	• Successfully meet approved continuing professional development units biennially • Continue to be an employee in "good standing" (per employing Component or Agency)	As specified in Component's or Agency's implementation Plan*
The certification holder will need to retest:		**Waivers**
Conditions:	• The DSTC concludes that the content addressed by the certification's assessment modules is significantly out-of-date • The individual fails to meet the certification maintenance requirements within the designated two-year certification period	As specified in Component's or Agency's implementation Plan*

* A DoD Component or Agency can, under special circumstances such as deployment or special duty assignments, waive the maintenance cycle or retest requirement.

SAPPC Eligibility

An individual is considered eligible for the SAPPC if they are assigned to any security position identified by the DoD Component as requiring a SAPPC-certified person (these positions are referred to as indexed positions). After the DoD Component determines that the person is an employee in "good standing," as defined in the "SAPPC Policy Matrix" of this handbook, they forward his or her name to the SPēD PMO. Individuals affiliated with a Federal Agency and/or the DoD may also volunteer to pursue the SAPPC. These individuals must coordinate with their Federal Agency or DoD SPēD POC before contacting the SPēD PMO. The SAPPC is available to DoD contractors if they are performing security duties directly for a DoD Component. They must contact the DSS SPēD PMO to verify their eligibility. Facility Security Officers and National Industrial Security Program—affiliated security professionals performing security duties on behalf of their respective companies are also eligible for SAPPC. These individuals should email the DSS SPēD PMO at SPED@dss.mil to schedule testing.

SAPPC Credentialing Process

There are four stages in the certification process:

1. **Eligible Applicant** - An individual is eligible for certification after gaining approval from the DoD Component, Agency, or SPēD PMO.
2. **Applicant -** The eligible applicant registers for SPēD Assessment and establishes or updates his or her Security Training, Education, and Professionalization Portal (STEPP) account.
3. **Candidate** - The applicant registers to take the SPēD Certification Assessment.
4. **Certificant -** The individual meets the requirements and a certification is conferred.

SAPPC Registration Process

The list below outlines the steps eligible applicants follow to participate in the SAPPC.

- Create or update STEPP account through https://stepp.dss.mil/SelfRegistration/Login.aspx. STEPP is the SPēD system of record. If your STEPP account is not current, your results may be delayed or undeliverable.
- Choose your testing date and location from the SPēD web site testing schedule and register for the testing event as indicated by the schedule.

Once an applicant's status is confirmed with the Center for Development of Security Excellence (CDSE) Registrar's Office, the candidate will be notified by email of registration. The candidate can review the resource documents and frequently asked questions online.

Conferral and Revocation of Credentials

DoD Instruction 3115.11, "DoD Intelligence Human Capital Management Operations," designates the OUSD(I) as the accreditation and certification official for the Defense Intelligence Components Department—Level programs. This empowers the OUSD(I) to confer or revoke SAPPC credentials. Specifics regarding this conferral and revocation authority can be found in DoD Manual 3305.13-M.

Candidates meeting the required assessment scores and eligibility requirements will be recommended by the Director, DSS, to the OUSD(I) for conferral of the SAPPC. The OUSD(I), upon recommendation from the Director, DSS, may also revoke the individual's SAPPC designation. Revocation of the SAPPC credential will be considered when a certificant is removed from their position for misconduct or poor performance.

Using SAPPC Credentials

Those persons who have been granted the Security Asset Protection Professional Certification are authorized to use the SAPPC designation on business cards, resumes, and signature lines. SAPPC certificants may use this designation as long as they maintain active status. The designation "SAPPC" should appear in all capital letters after a comma following the certificant's name. For example, John Dough, SAPPC.

Topic Areas of Expertise

The SAPPC Assessment measures the applicant's ability to apply fundamental security knowledge and skill across the DoD security landscape. Although a security professional's current work may primarily be in one of the core security disciplines (information, personnel, physical, industrial, or general security), the results of the practice analysis performed by DoD showed that it is important to have awareness and a fundamental body of knowledge across the core security disciplines and the ability to apply foundational security concepts, principles, and practices. The SAPPC is not only valuable to security professionals as their careers advance, but it also strengthens DoD's confidence in its security professionals' general knowledge.

The areas of expertise specified in the charts on the following pages were identified during the practice analyses as critical domains that should be addressed by the SAPPC. The weights indicated were derived from importance ratings provided by subject matter experts (SMEs) during the development process.

SAPPC Examination Development

The initial step in the development of a fair and objective test was to measure the ability to apply fundamental knowledge and skill required of a DoD security professional. A job/practice analysis was conducted to assure that the knowledge and skills identified were representative of those required by professionals from across all of DoD, including tasks and functions performed by civilian, military, and contractor personnel. The job/practice analysis was designed and facilitated by technical experts contracted by DSS, engaged DoD Leaders, and SMEs from the uniformed Services and multiple DoD Agencies who participated in each of four job/practice analysis phases. These phases included a detailed review of studies that had been performed before, defining specific work performed and required knowledge and skills necessary to perform that work, and verifying the results with SMEs and the DSTC. The job/practice analysis led to creation of the Defense Security Skill Standards (DS3), which clarifies the Department's expectations of what security professionals must know and be able to do to successfully perform responsibilities that support the Department's security functions. This information was then used to generate the certification test outline (blueprint) that specifies objectives associated with the 47 knowledge and skill topics and sub-topics that are to be measured with the SAPPC Assessment.

The test questions were developed by a process that included (1) developing draft questions that assess mastery of selected and codified objectives that are based on these knowledge and skill requirements (2) facilitating senior SME review of draft assessment items for accuracy and relevance to the objectives, and (3) piloting the resulting test for effective and accurate measurement in order to generate the final version of the test.

The DSS will continue to monitor "change factors" (e.g., policy change, system change) on a continuing basis to identify those changes that could affect test questions used within the certification test and result in adjustments as required. The test questions themselves will also be reviewed on a quarterly basis to ensure they continue to function as intended. The review involves generating and reviewing question and test level statistics to gauge continued effectiveness.

Area of Expertise (AOE)	
Information Security	**Exam Weight (28%)**
Classification Considerations for Critical Program Information (CPI)	1%
Classification Levels and Types	2%
Classification Markings	2%
Disposition and Destruction Procedures	1%
Duration	1%
Handling Incidents of Potential and Actual Compromise	3%
Handling Special Types of Information	1%
Information Assurance Concepts	2%
Information Protection Concepts	3%
Procedures in a Classified Workplace	6%
Safeguarding	1%
Transmission and Transportation Procedures	2%

Note: Sum of sub-topic area percentages may not be equal to AOE exam weight due to rounding.

Area of Expertise (AOE)	
Personnel Security	**Exam Weight (31%)**
Adjudicative Guidelines	3%
Civilian Employment Investigative Requirements	2%
Designation of Position Sensitivity Types	1%
Military Appointment, Enlistment, and Induction Investigative Requirements	1%
Personnel Security Clearances	3%
Personnel Security Investigation Requests	1%
Personnel Security Investigations, Limitations, and Restrictions	2%
Safeguarding Personnel Records	3%
Security Systems	5%
Special Personnel Security Clearance Requirements	1%
Standards – Access to Classified Information/Sensitive Duty Assignment	2%
Types of Personnel Security Investigations	2%
Unfavorable Administrative Actions	1%
Waivers of Investigative Requirements	4%

Note: Sum of sub-topic area percentages may not be equal to AOE exam weight due to rounding.

Area of Expertise (AOE)	
Physical Security	**Exam Weight (10%)**
Facility Access Control Procedures	2%
Lock and Key Systems	1%
Physical Security Concepts	2%
Protective Barriers	2%
Secure Rooms, Containers, and Vaults	1%
Security Systems and Devices	1%
Site Lighting	1%
Area of Expertise	
Industrial Security	**Exam Weight (13%)**
Contracting Process	1%
Facility Security Clearance	1%
FOCI	1%
Industrial Security Basics	5%
Visits and Meetings	1%

Note: Sum of sub-topic area percentages may not be equal to AOE exam weight due to rounding.

Area of Expertise (AOE)	
General Security	Exam Weight (18%)
Basic Security Forms	2%
Counterintelligence Concepts	2%
OPSEC Concepts	1%
Research and Technology Protection Concepts	2%
Risk Assessment and Management	2%
SAP Basics	2%
Security Briefings	1%
Security Education and Training	2%
Security Policy Landscape	4%

Note: Sum of sub-topic area percentages may not be equal to AOE exam weight due to rounding.

Assessment Administration

Scheduling an SAPPC Assessment

Prior to registration for the SAPPC Assessment, candidates must contact their supervisor for coordination and, if required, approval, and adhere to their organization's policies regarding SAPPC participation. SAPPC candidates must have an active and up-to-date STEPP account to register for the certification assessment. STEPP is the system of record for the SPēD Certification Program.

After registering for the certification assessment, candidates will receive a notification email from STEPP informing them their registration is pending approval. Approval to take the test is granted from the Registrar's Office after candidates are approved by the DSS SPēD PMO and/or respective DoD Component.

Procedures

Once the candidate has registered as a SAPPC candidate in STEPP, the SPēD PMO will send an email to the candidate which includes the test site address, report date and time, the registered exam, and items the candidate needs to bring to the testing site, including the following:

- Registrar email
- Government-issued photo identification (DoD Common Access Card (CAC), passport, or driver's license) OR
- Commercial and Government Entity (CAGE) Code (if employer is a DoD contractor)

For testing outside the United States, candidates must bring two forms of identification. One form of identification must be a CAC and the other can be a driver's license, passport, or military ID.

Assessment Security and Confidentiality

The questions and answers that comprise the SAPPC Assessment are for official use only and not subject to public release.

Prior to beginning the SAPPC Assessment, the candidate is asked to accept the terms and conditions of the SPēD Certification Program Notice (found in this handbook). Among other things, this notice states: "By accessing and participating in this assessment, you accept the responsibility to protect the integrity of this assessment by not disclosing, disseminating, copying, publishing, or transmitting any parts of this assessment in any form to any person."

The SPēD Certification Assessment will be proctored. Proctors are responsible for ensuring consistent testing environment across the DoD for the SPēD Certification Program and protecting the integrity of the SPēD Certification Program.

The SPēD Certification Assessment is password-protected and hosted on a secure server. The assessment cannot be accessed, copied, printed, or distributed without approval from the DSS SPēD PMO.

Pass/fail information will be provided to the Primary Office of Responsibility for the candidate's owning Component or Agency. A candidate may access his or her results via STEPP, the SPēD system of record.

Except as described in this handbook, individual information and results are confidential and will not be disclosed without candidate consent, unless when necessary to comply with mandatory legal demand or court order. Any authorized written request must state the specific data that may be released and specifically identify the third party to receive the data. Data distributed as a result of the SAPPC studies and reports will be aggregated and personal identification information will be redacted.

SPēD Terms and Conditions

Prior to taking the certification assessment, candidates will be asked to accept the following terms and conditions.

Materials Provided at the Assessment Location

The following items are provided to test takers:

- Blank paper or worksheets, as applicable
- Computer for delivery of test

See the Accommodations for Disabilities section of this handbook for guidance in requesting special accommodations for testing.

The test takers are not permitted to bring electronic communications devices, including smart phones, into the testing area.

Assessment Completion Time

The SAPPC Assessment has a two-hour time limit.

Rescheduling an SAPPC Assessment

If needed, candidates may cancel and reschedule their assessment date. They may log onto STEPP, then view and select a new assessment date and location.

Retaking an SAPPC Assessment

If a candidate does not obtain a passing score on the SAPPC Assessment or does not complete the assessment, he or she can retake it after a 90-day waiting period. This waiting period is applied after each sitting, regardless of whether the assessment was completed. Sitting for the assessment occurs when the candidate enters the proctor-provided user ID and password. It is recommended that the candidate refer to the website for suggested courses addressing the topic areas to improve performance when retaking the assessment.

Scoring the SAPPC Assessment

The candidate must earn a score that is equal to or higher than the passing score in order to be considered to have passed the assessment. Candidates can access their pass/fail results in STEPP within 15 days after taking the SAPPC.

Feedback

After completing and submitting the assessment, each candidate will also receive information indicating strengths and weaknesses across the Areas of Expertise (general security, information security, personnel security, physical security, and industrial security), which can be helpful for developmental purposes.

Determination of Passing Scores

The Angoff method was used to set the minimum passing score for the SAPPC. The Angoff method has a well-established history of determining creditable passing standards for multiple-choice examinations and is easily adapted for use with the SAPPC Assessment. The method involves two basic elements: conceptualization of a minimally competent examinee and using SMEs to estimate whether a minimally competent examinee will answer an item correctly or incorrectly. Minimally competent examinees are examinees who demonstrate behaviors that are sometimes correct, but often not. They have a 50:50 probability of passing or failing the exam, which places them just at the cut-off score for an assessment. SMEs define the characteristics of a minimally competent examinee and then try to estimate if a minimally competent examinee is likely to successfully perform each of the items on the assessment. A panel of SMEs made predictions for each item (represented as a percentage) and the average of the SMEs ratings on the items sets the minimum passing score for the assessment. Results of the Angoff method inform the provisional cut score. The provisional cut score is then calibrated using data collected during the beta test phase.

Appeals Policy and Procedures

Appeals Policy

The appeals policy governs the process for reviewing decisions made about registration, eligibility, assessments, and other registration/assessment-related certification issues and/or challenges.

A SPēD Certification appeal can be filed based on all decisions relating to:

1. Examination results, criteria for obtaining a passing score on the SAPPC Assessment or the candidate registration and test-taking protocols

2. Certification renewal requirements, such as completion of approved professional development units (PDUs) or timeliness of completing and reporting PDUs

3. Eligibility evaluations. Appeals regarding eligibility requirements should be filed with the DoD Component that made the eligibility decision.

The test taker can request a rescoring of the test as part of his or her appeal process.

Appeals regarding any matters not described above are not within the purview of the SPēD Certification Program, including the following DoD Component decisions:

- Employment policy
- Eligibility criteria for identifying billets or individuals for SPēD Certification conferral
- Affiliation

Contact the appropriate Component SPēD PMO (check the "Contacts" list in the SPēD website) with questions or appeals of decisions outside the purview of the SPēD Certification Program.

Appeal and Review Process

Individuals must submit an appeal request within 90 calendar days of receiving notice of an appealable decision.

In order to be accepted, an appeal must be in writing and must include: (1) a description of the decision being appealed, (2) any evidence or argument as to why the decision should be overturned, and (3) the individual's name and contact information.

The appellant must send the appeal statement in an email or letter to SPED@dss.mil or to the following address (appeals must be postmarked or emailed no later than 90 calendar days from the date the candidate first received notice of the decision being appealed):

Defense Security Service
Center for Development of Security Excellence
Attn: Department of Defense Security Training Council
c/o SPēD Program Management Office
938 Elkridge Landing Road
Linthicum, MD 21090

Appeals, reviews, and decisions will be made by two authorities: the SPēD PMO and DTSC SPēD Appeals Board (DSAB). The DSAB will consist of five people: three members (elected by the DSTC) serving a two-year term, a fourth member appointed by the DSTC to represent the candidate's employing organization, and the fifth member is the DSTC Chair. The DoD Inspector General will be requested to represent appeals from contractor or industry personnel.

First Appeal Decision

The DSS SPēD PMO will conduct the initial review of the appeal request. It will first determine if the event is within the jurisdiction of the DSS SPēD PMO. If it is not, the office will forward the appeal to the appellant's employing organization.

If the appeal request is within the jurisdiction of the SPēD PMO, the SPēD PMO will review the appeal and render a written decision on the appeal within 90 calendar days of receipt of the appeal, if practicable.

The DSS SPēD PMO will provide the appellant with the office's written decision. The PMO will compile recommendations to be reviewed by the DSAB as required.

SPēD PMO appeal decisions become final when 90 calendar days have passed after the appellant's receipt of the SPēD PMO decision, unless the appellant has submitted an appeal of the PMO decision with the DSAB within those 90 days.

Second Appeal Decision

Appellants who are dissatisfied with the SPēD PMO decision on the appeal may pursue a second appeal to the DSAB.

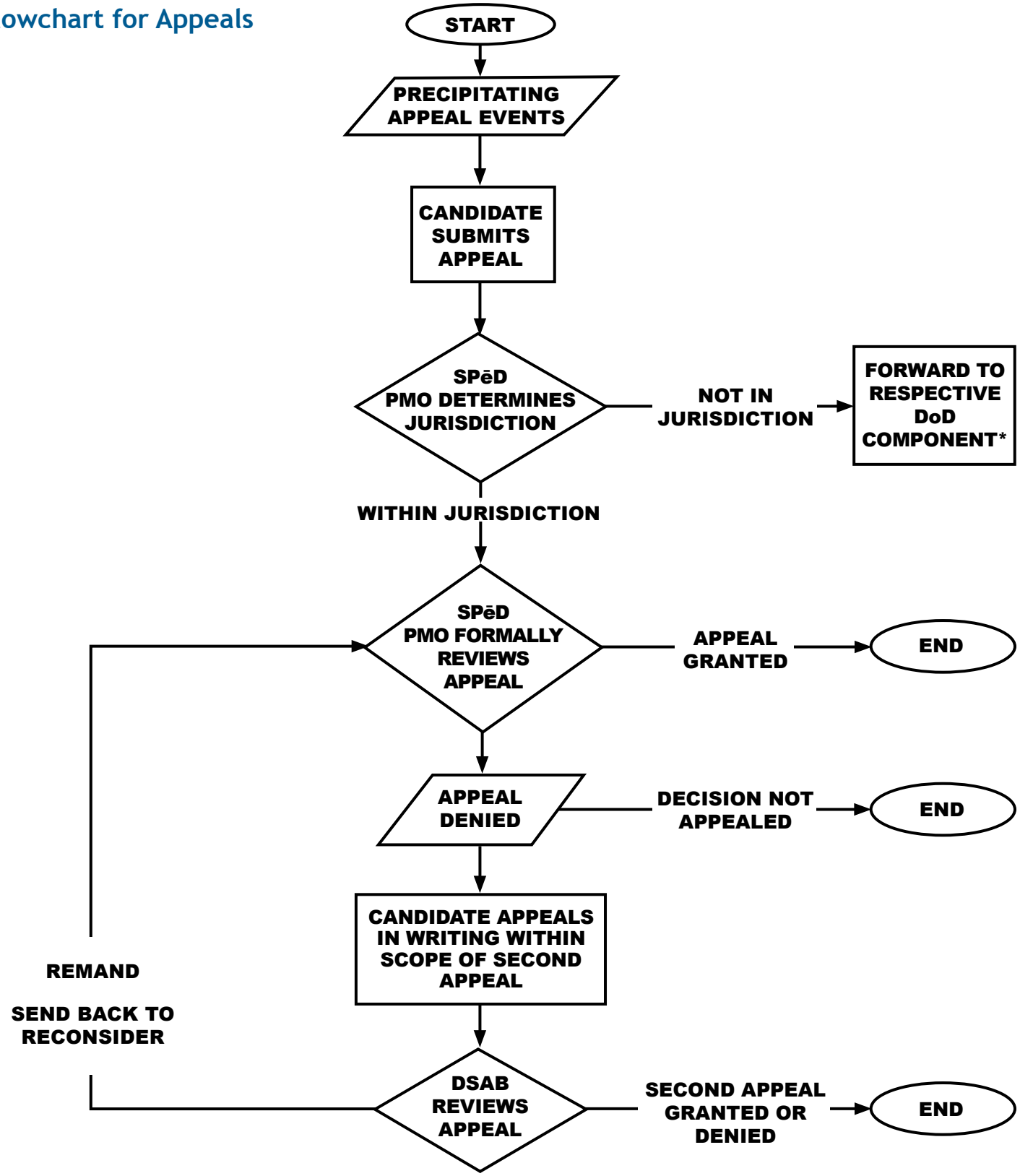
Defense Security Service
Center for Development of Security Excellence
SPēD Program Management Office
Attn: DSAB
938 Elkridge Landing Road
Linthicum, MD 21090

The DSAB will not consider an appeal unless the DSS SPēD PMO has rendered a decision. Appeals to the DSAB of a SPēD PMO decision must be supported by written statements that identify how and why the appellant believes the SPēD PMO's decision was erroneous or contrary to established procedures, regulations, or laws. Appeals to the DSAB must be submitted no later than 90 days following the appellant's receipt of the SPēD PMO decision on the first appeal.

DSAB members receive recommendations from the SPēD PMO on submitted second appeals for the current quarters on December 7, March 7, June 7, and September 7, or on the closest duty day to these dates if these dates fall on a non-duty day. DSAB members will have one week to accept or not accept recommendations.

DSAB decisions will be made by majority vote. The DSAB will provide its decision to the SPēD PMO, and the SPēD PMO will notify appellants of the final decision. The DSAB is the final decision authority and there are no further appeals from a DSAB decision.

Flowchart for Appeals



*Referred back to candidate in case of industry with explanation

Disciplinary Policy and Procedures

As stated in the Secretary of Defense Memorandum, "Ethics, Integrity, and Accountability," dated May 2, 2012, SPēD Certification candidates and credentialed individuals must understand that unethical or unprofessional behavior may be cause for the SPēD PMO to deny entry into the SPēD Certification process, to terminate participation during an examination, or to invalidate the result of an examination. As a result of any of these actions, the individual may be required to retake an entire step in the process (or portions thereof), or to have their certification(s) revoked.

Grounds for disciplinary action include, but are not limited to the following:

1. Falsification of information on any document needed to acquire a SPēD Certification.

2. Actions that compromise the integrity of the SPēD assessment instrument, including but not limited to unauthorized possession of or access to real assessment questions; copying a SPēD Certification Assessment; or the receipt of assessment information before, during, or after the assessment session that gives the tester an unfair advantage over other candidates.

3. Revocation or denial of security clearance due to misconduct.

4. Request by the certificant's parent organization that the certification be revoked.

5. Misrepresentation or false statements regarding conferral of a SPēD credential when the credential has not been conferred or the certification has not been renewed in accordance within the SPēD Certification Assessment guidelines.

6. Non-compliance with the DoD Component's Code of Ethics, standards of conduct, rules, or professional behavior.

Inquiries into suspected violations of the SPēD Certification Assessment disciplinary policy will be characterized by fair and equitable inquiry into the facts.

Cheating on an assessment consists of willfully consulting a notebook, textbook, or any other source of information not specifically authorized by the proctor during the assessment; willfully aiding, receiving aid, or attempting to aid or receive aid from another candidate before, during, or after an examination; obtaining or attempting to obtain copies of the examination before it is given; or any act which violates or attempts to violate the stated conditions governing the administration of an examination.

The DSTC is responsible for establishing and implementing standards of conduct, and policies and procedures governing disciplinary action for the SPēD Certification Program.

Suspected violations may be submitted by any interested party. The complainant's name, witnesses, and the content of the complaint will remain confidential, unless legal requirements mandate disclosure. Notices of suspected violations will be sent to the owning candidate's Component and/or organization where the alleged violation occurred for investigation. The appropriate officials should notify the SPēD PMO/DSTC of their determination and action taken so the DSTC can determine if DSTC action is required or if additional information is needed.

On disciplinary matters, the DSTC may only address the certification aspects of the violation. The SPēD Certification Program will address violations of its code of ethics within 60 days of being informed that a violation has occurred and the investigating official has made a decision regarding the event.

The DSTC may impose sanctions that include, but are not limited to, the following:

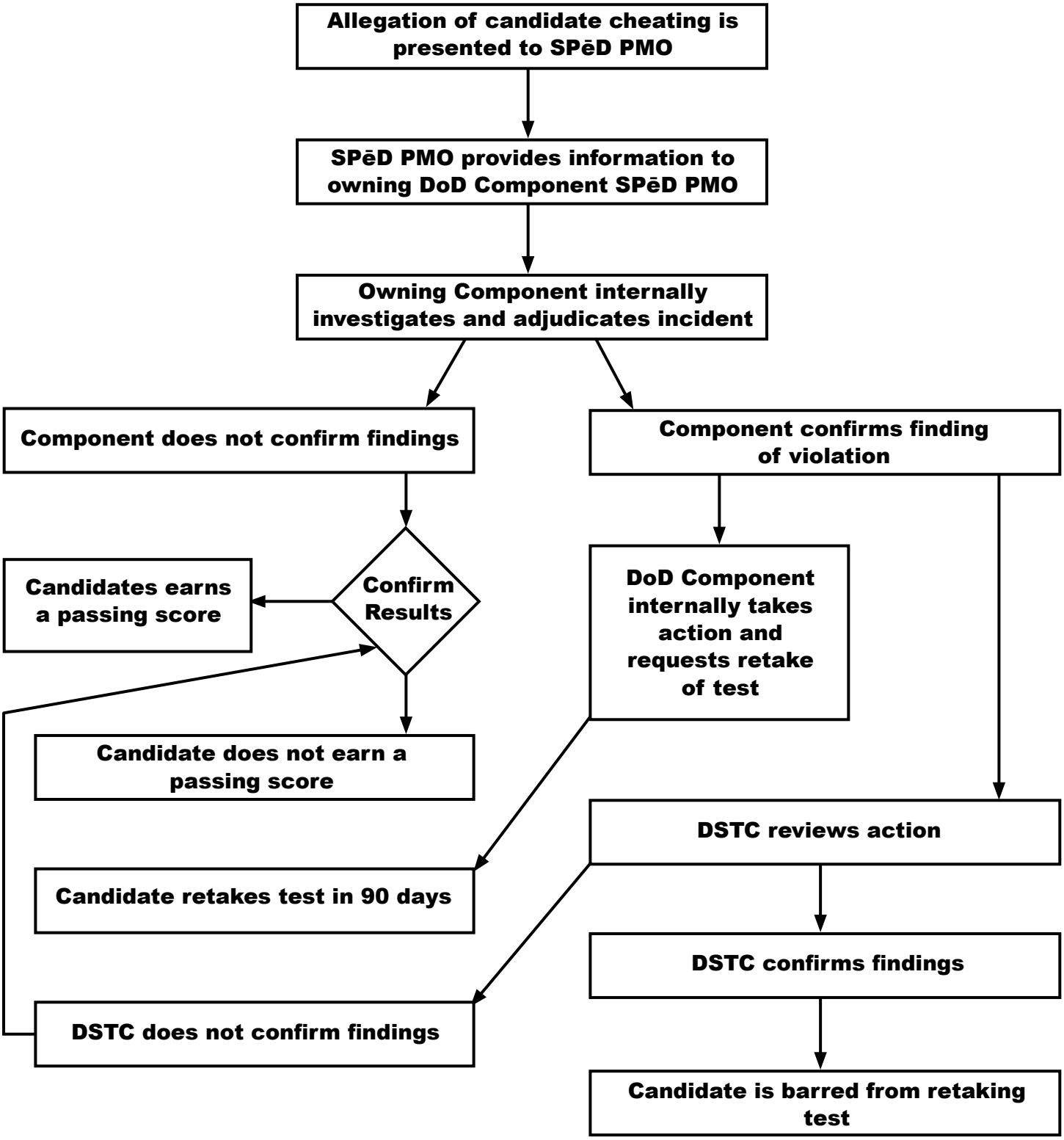
1. Written reprimand to the violator, copy furnished to his or her commander/senior official
2. Correction of the record
3. Probation

When the DSTC determines that a violation(s) to its standards has occurred, that warrants revocation of the certificate, the DSTC will forward a recommendation to the OUSD(I) for recommendation of revocation.

Documentation of the disciplinary process and record of action will be placed in the individual's STEPP file and will be available for review by the DSTC or other authorized official parties should circumstances warrant.

Actions taken under this policy do not constitute enforcement of law, although referral to appropriate agencies may occur. Individuals found in violation of the SPēD Certification Program code of ethics or honor are not entitled to relief or damages by virtue of this process and complaints requesting such relief will not be considered. No one who has personal involvement in the potential violation(s) or conflict of interest will be permitted to participate in the adjudication of the matter.

Disciplinary Policy and Procedures



Certification Renewal

Obtaining an SAPPC is a significant achievement in an individual's career in the DoD. An SAPPC indicates the individual has demonstrated the ability to apply foundational security concepts, principles, and practices the DoD community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks to and protect DoD assets. However, the SAPPC is not the end of an individual's professional development.

The DoD has a professionalization goal of establishing a systematic approach for fostering learning and professional growth of the security workforce. The SPēD Certification Renewal Policy is the long-term strategy for meeting this goal. This approach allows DSS and the DSTC to enable DoD to meet National Intelligence Strategy Enterprise Objective 6 and OUSD(I) Human Capital Goals and Objectives for the security workforce.

The Renewal Policy for the SAPPC was initially drafted by the Policy and Procedures Working Group and approved by the DSTC, acting in their role as the Governing Board. Refinements were made regarding PDUs in February 2012.

The PDU count policy and the two-year maintenance cycle was based on several significant factors: the two-year probation cycles for professionals in new positions for which these certifications are relevant, the typical training budget adjustment period required for professional development, turnover patterns, and a judgment about typical policy and practice adjustment cycles. In an effort to assure continuing competence, maintenance and recertification must be defined. Maintenance and recertification are essential elements of the renewal of the SAPPC certificate.

Certification Renewal

Certification Maintenance

As defined by the SPēD Certification Renewal Policy, a SPēD certification holder must (1) continue to be an employee in "good standing" per the certificant's Component and (2) successfully obtain approved continuing PDUs biennially. To accrue PDUs, you must participate in and successfully complete professional development activities that fall under one of the approved professional development categories. The categories are as follows: certification programs (SPēD and pre-approved non-SPēD certifications), certificate programs, non-credit bearing training and/or education courses, credit-bearing training and/or education courses, conferences/workshops, joint-duty assignments, and SPēD Certification Program projects. A point matrix for PDUs associated with the seven categories is available on the SPēD website. Credential holders may keep their credentials as long as they meet the renewal policy requirements and their STEPP account is current, regardless of DoD affiliation. If the SPēD PMO cannot contact the certificant, then he or she forfeits the certification.

Security professionals conferred the SFPC or the SAPPC must accrue 100 PDUs within a 2-year cycle. At least 50% of the 100 PDUs must be fulfilled through approved professional development activities focusing on security topic areas. The remaining PDUs must be fulfilled through professional development activities focusing on core academic topic areas. A catalog of approved professional development activities is available at the following link: http://www.dss.mil/seta/sped/pdu.html.

The certification renewal clock for SFPC and SAPPC is on hold pending the SPēD PMO's implementation of technology systems for managing PDUs. Please reference the SPeD FAQs (http://www.dss.mil/seta/sped/faqs.html), in the SPeD Certification web site for updates on this situation.

Failure to meet the renewal requirements will result in the immediate revocation of the SAPPC. Termination, in turn, will result in the loss of all rights and privileges that comes with holding a SPēD Certification. Security professionals whose certifications have been terminated must successfully meet all applicable certification requirements in order to renew those certifications.

See the policy matrix regarding waivers.

Recertification/Retest: The SPēD Certification Program will define recertification policies and procedures for each certification. Recertification may be required if:

a. Conditions and/or events trigger the need for certification holders to recertify in one or more topic area of the assessment, or

b. An individual fails to meet the certification renewal requirements.

Sample Diagnostic Test

The SAPPC diagnostic tool allows candidates an opportunity to review learning content available to them in preparation for the SAPPC Assessment by assessing candidates' strengths and weaknesses of SAPPC content. The following presents examples of scenarios. Each scenario is followed with questions that assess the candidate's understanding of the subject matter. Additionally, a listing of relevant Intelligence Community Directive (ICD) 610 competencies, which align to the scenario and to existing learning content, is available for review. Finally, a list of question topics is presented after each scenario to provide an orientation of what to expect during the actual examination.

Scenario 1

Cast

- Rick: a cleared engineer
- Manuel: a cleared senior engineer
- Terry: a foreign national co-worker of Rick's
- Jack: a newly hired cleared engineer
- Unnamed: security manager

Brief Description of the Scenario

In Scenario 1, we meet Rick. Rick, a cleared engineer, is requesting classified information from a Security Manager for a research assignment he is currently working. In the beginning of the scenario, we learn whether the Security Manager has made the correct decision on whether Rick had the necessary requirements to gain access to the information. The next part of the scenario refers to the following day, when Rick gives the same classified information to a foreign national co-worker, named Terry, who has Limited Access Authority. The last section describes the following week, when another engineer gives Rick access to a different piece of classified information. Here, candidate questions focus on how they would react if the classified information was under special classification requirements (i.e., SCI, FGI, and NATO).

The scenario aligns to the following security competencies:

- Information Security

  Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

- **Incident Response**

  Responds to crisis or urgent situations including accidents; man-made, biological, chemical, radiological, or natural disasters; and other incidents that could result in harm to people, property, or the environment. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life and preservation of property.

- **Classification Management**

  Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding of protected and/or classified information.

- **Counterintelligence**

  Gathers information and conducts activities to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

- **Security Tools and Methods**

  Applies tools and methods to a substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for the substantive discipline, domain, or area of work.

- **Vulnerabilities Assessment and Management**

  Conducts assessments on threats and vulnerabilities, determines the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations. Conducts assessments in a counterintelligence context to protect against espionage; other intelligence activities; and sabotage conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

During this scenario, you will be asked questions about the following knowledge areas:

- Security Violations/Incidents
- JPAS
- SF-312
- Access/Eligibility Requirements
- Risk Managements
- Working with Counterintelligence (CI)

- Damage Assessments
- SCI Information
- NATO Information
- FGI Information
- Destruction of Classified Information

Scenario 2

Cast

- Roger: BAIT Program Manager
- Matthew: BAIT Senior Test Engineer
- Mitch: BAIT Senior Scientist
- Mary Ann: a member of the Unit compliance Inspection team
- Unnamed: a foreign visitor

Brief Description of the Scenario

Scenario 2 discusses the BAIT (Best Airplane in Town) program. BAIT is a multi-engine, turbofan, wide-body, strategic airlift aircraft capable of stealthily moving combat equipment into and within austere theater environments. It is expected to provide significant improvements in both performance and operational costs compared to the aircraft in the current airlift fleet. In the first part of the scenario, Roger, the BAIT Program Manager, reports a security incident stemming from a conversation between two team members. The candidate will be given a copy of the BAIT Security Classification Guide to answer the questions to this scenario. In the second part of the scenario, Mary Ann, a member of the Unit Compliance Inspection team, learns that the BAIT's new radar system is based on a particular signature control technology included in the Military Critical Technology List (MCTL). The candidate will explore questions on the ramifications of this discovery. The final part of the scenario involves Mary Ann's discovery that a group of foreign academics visited the facility and gained access to an unclassified website. During the visit, one of the visitors seems to know a little more about the radar system than he or she should.

The scenario aligns to the following security competencies:

- **Information Security**

  Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

- **Incident Response**

  Responds to crisis or urgent situations including accidents; man-made, biological, chemical, radiological, or natural disasters; and other incidents that could result in harm to people, property, or the environment. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life and preservation of property.

- **Classification Management**

  Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding of protected and/or classified information.

- **Counterintelligence**

  Gathers information and conducts activities to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

- **Personnel Security**

  Applies personnel security principles and methods to process initial clearances, periodic re-investigations, clearance upgrades/downgrades, and to complete the adjudication and appeals processes. Evaluates internal and external security clearance requests and ensures applicants' actions are consistent with regulatory requirements. Analyzes and reports on clearances and appeals findings to senior security officials and makes appropriate notifications.

- **Program Security**

  Employs an array of acquisition and contract security measures to sustain secrecy of highly sensitive U.S. Government programs and/or activities. Prevents unauthorized disclosure of national intelligence program information throughout the contract lifecycle (e.g., FOCI, connections with adversarial or terrorist organizations).

- **Vulnerabilities Assessment and Management**

  Conducts assessments on threats and vulnerabilities, determines the level of risk, and develops and recommends appropriate mitigation countermeasures in operational and non-operational situations. Conducts assessments in a counterintelligence context to protect against espionage; other intelligence activities; and sabotage conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

During this scenario, you will be asked questions about the following knowledge areas:

- Security Violations/Incidents
- Following Security Classification Guidance
- Military Critical Technology List (MCTL)
- Acquisition Security
- OPSEC
- Risk Management
- Counterintelligence (CI)
- Technology Control Plan (TCP)

SAPPC Diagnostic Tool—Additional Information

The purpose of the SAPPC Diagnostic Tool is to familiarize candidates with scenarios, as well as topic areas that are assessed through the SAPPC. Please note that SFPC is a prerequisite to SAPPC. A candidate must hold the SFPC before becoming eligible to take SAPPC. For more information regarding SPēD Certification Program tools and resources, please visit: http://www.dss.mil/seta/sped/sped_resources.html **and** http://www.dss.mil/seta/sped/diagnostic-tools.html. For more information on the ICD 610 Competencies, please visit http://www.dni.gov/electronic_reading_room/ICD_610.pdf.

Tips for Success on the SAPPC Assessment

The SAPPC Assessment is training agnostic. "Training agnostic" indicates that a person does not have to take any specific prescribed training prior to taking the certification assessment. Often, preparing for the assessment test by taking related training may be a good idea, but it is not required and does not have to be a specified course.

Preparing for the Assessment

Consider the following courses and resources when preparing to take the SAPPC Assessment:

- Although no courses or training are required to take the assessment, it is recommended that you familiarize yourself with courses addressing the topic areas listed in "The SAPPC Credential" section of this handbook. The following courses have been helpful to many preparing for the assessment.

- Introduction to Industrial Security Course IS011.16
- Introduction to Information Security Course IF011.16
- Introduction to Physical Security Course PY011.16
- Introduction to Personnel Security Course PS113.16
- Introduction to DoD Personnel Security Adjudication Course PS001.18
- Introduction to Critical Program Information Awareness Course CI120.16
- Special Access Program (SAP) Overview Course SA001.16

- Access "Resources for SPēD" at https://go.usa.gov/5We or through STEPP. Use the diagnostic tool to help you gauge your level of knowledge in the various security topic areas. Based on your results, download and review the appropriate recommended resources to increase your proficiency. Please note: The diagnostic tools merely help you to gauge your level of understanding in the security topic areas covered on the assessment. The diagnostic tool does NOT contain the actual certification assessment questions.

Study Suggestions

Here are a few helpful hints for studying for the SAPPC Assessment:

- Recognize that the material cannot be memorized in its entirety; use memory techniques only to help recall key points.
- Focus on the application of accepted principles, practices, and theories, not memorizing facts, dates, and names.
- Consider studying in pairs or starting or joining a face-to-face or virtual study group.
- Review sample test questions.

Test Taking Tips

When taking the test,

- Do what is needed to feel comfortable and relaxed before the test; check out the test site in advance and make sure to get enough rest and nourishment prior to taking the exam.
- Arrive early—at least 20 minutes before the scheduled test time.
- Trust first impressions; do not over-analyze answers.
- If uncertain about a question, return to it later, and if you are still uncertain, make an educated guess.
- Do not look for answer patterns.
- Do not select an answer based on length; it may contain a false clue.
- Do not rush. Consider each choice before selecting the best one.
- Use time well. Extra points are not awarded for finishing early.
- Each item is worth one point and there is no penalty for guessing wrong answers, so make every attempt to answer all the questions.

Accommodations for Disabilities

The SPēD Certification Program will provide reasonable accommodation in its testing process in compliance with the Americans with Disabilities Act (ADA), Rehabilitation Act, and DoD Policy for individuals requesting accommodation.

In general, an accommodation is made when a disability is relieved by an auxiliary aid or a procedural change in the administration of the assessment. Reasonable accommodations will be made for known physical or mental limitations of a candidate who is a qualified individual with a disability.

It is the responsibility of the candidate to seek accommodation from the DSS SPēD PMO by emailing SPeDCert.Registration@dss.mil at least four weeks in advance of the assessment.

A request for a reasonable accommodation is a verbal or written statement from a candidate requesting an adjustment or change in the testing for a reason related to a disability. A request does not have to use any special words, such as "reasonable accommodation," "disability," or "Rehabilitation Act." An individual with a disability may request a reasonable accommodation whenever he or she chooses, even if he or she has not previously disclosed the existence of a disability.

Documentation, from an appropriate health care or rehabilitation professional, about an individual's disability and functional limitations may be requested when the disability and need for accommodation is not obvious. Appropriate professionals include, but are not limited to, doctors (including psychiatrists), psychologists, nurses, physical therapists, vocational rehabilitation specialists, and licensed mental health professionals. The documentation should identify the disability, state clearly that the disability necessitates an accommodation, and identify the specifics of the accommodation.

The need for reasonable accommodation is determined on an individual basis depending on the unique circumstances involved and taking into consideration the candidate's specific disability and the existing limitations in completing the certification process.

DSS will make reasonable efforts to accommodate the candidate's request, including offering an alternative means of access to take the SAPPC Assessment. If DSS SPēD PMO determines that it would impose an undue burden on either the DSS SPēD PMO or the DoD Component to provide the required testing environment, and the candidate's sponsoring Component cannot provide the necessary accommodation, the candidate will be notified with a written explanation of the denial and a statement of the reasons for the denial. Denied accommodations can be grieved to the DSS Office of Equal Employment Opportunity at eeo@dss.mil or 571-305-6726.

Non-Discrimination Policy

The SPēD Certification Program does not discriminate on the basis of any of the following: race, color, national origin, sex (including pregnancy or childbirth), religion, age (40 or over), disability (physical or mental), sexual orientation, marital status, parental status, political affiliation, genetic information or retaliation for participating in protected activities.

The Pathway to Success Begins with

Security Professional Education Development

Visit http://dssa.dss.mil/seta/sped/sped.html
Send questions to SPED@dss.mil