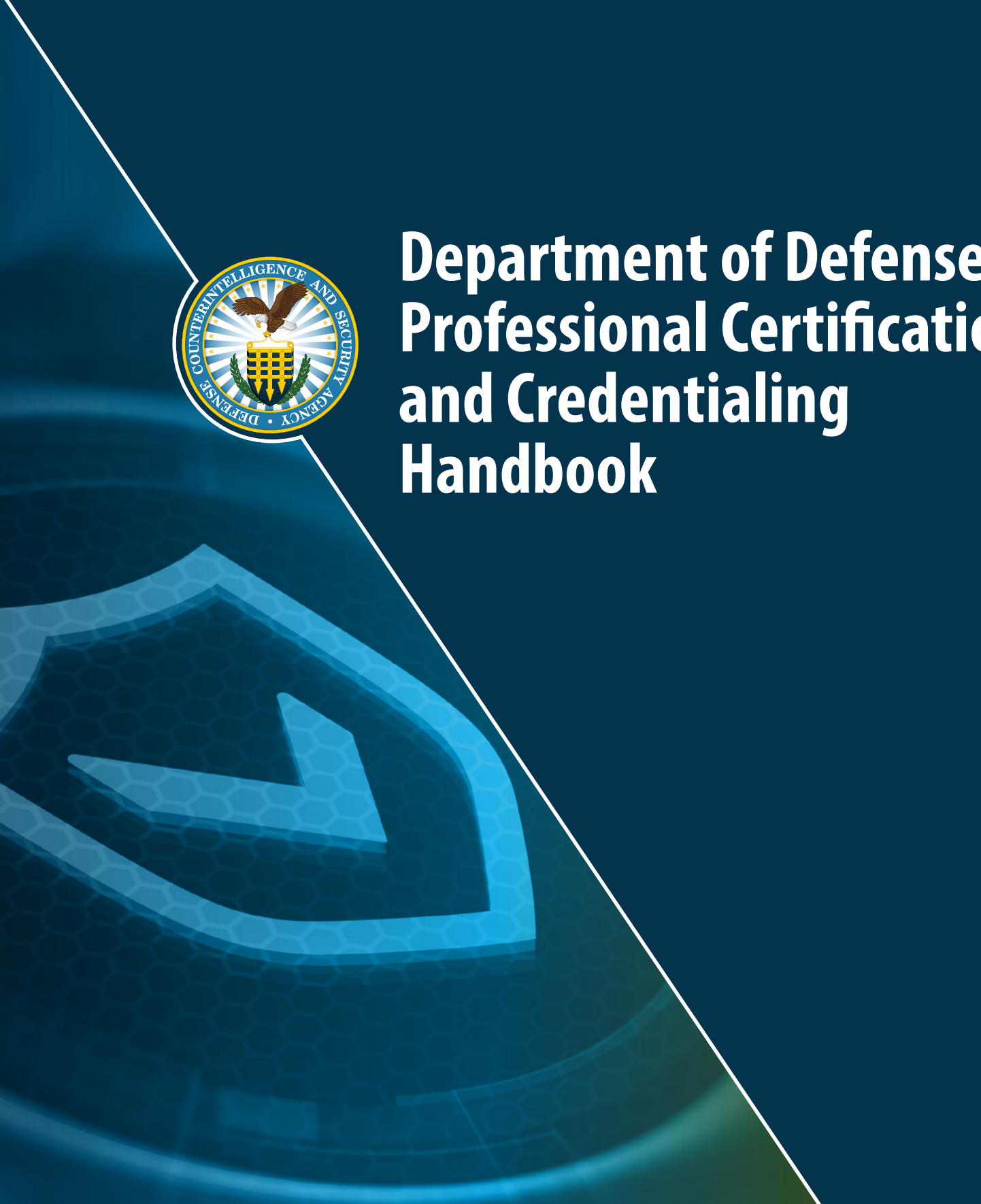
# Department of Defense Professional Certification and Credentialing Handbook



SPēD PROGRAM MANAGEMENT OFFICE

CDSE Center for Development of Security Excellence

February 2025

# CONTENTS

# STARTING YOUR JOURNEY

Congratulations on your decision to pursue a certification and/or credential, which includes five certifications and four credentials maintained by the Department of Defense (DOD) Security Professional Education Development (SPēD) Program!

We look forward to supporting you on your journey toward professional growth and excellence!

## PURPOSE OF THE HANDBOOK

This handbook is a primary source of information for the SPēD Program's certifications and credentials and provides candidates with information about obtaining and maintaining their certifications and credentials.

## NON-DISCRIMINATION STATEMENT

The SPēD and Adjudicator Professional Certification (APC) Programs do not discriminate on the basis of race, color, ethnicity, sex, national origin, handicapping condition, religion, political affiliation, or sexual orientation.

## CONTACT INFORMATION

Candidates should contact their Component Service Representative (CSR) for general information about the **SPēD Program**: https://www.cdse.edu/Certification/Additional-Certification-Credential-Assistance.

**Certification and Credential Account log-in**: https://www.cdse.edu/Certification/Account-Login/

**SPēD Program webpage**: https://www.cdse.edu/certification/index.html

**SPēD Program Candidate Support**: dcsa.spedcert@mail.mil

**Credly Help Center**: https://support.credly.com/hc/en-us

**Pearson VUE test cancellation/rescheduling**: 1-888-477-0284

or visit https://home.pearsonvue.com/Test-takers/Customer-service.aspx

# SPēD PROGRAM OVERVIEW

## WHAT IS THE SPēD PROGRAM?

The SPēD Program is part of the DOD's initiative to professionalize the security workforce. This initiative ensures there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

## GOVERNANCE

DOD Instruction (DODI) 3305.13, "DoD Security Education, Training, and Certification," establishes the DoD Security Training Council (DSTC) as an advisory body on DoD security education and training and serves as the governance board for the SPēD Certification Program. The DSTC is comprised of security professionals and senior managers representing DOD entities with security responsibilities, and others as determined by the DSTC Chair. The DSTC represents the shared interests of the Defense Security Enterprise and the respective workforce in certification design, management, and maintenance.

Specifically regarding SPēD governance, the DSTC is responsible for:

- Certification administration oversight
- Technical development oversight
- Certification governance

## ACCREDITATION

The SPēD Program is an essential element of the DOD initiative to professionalize the security workforce. Per DOD Manual (DODM) 3305.13, "DoD Security Accreditation and Certification," all certifications must be accredited and maintain accreditation by meeting the published standards of the national recognized certification accreditation body, the National Commission for Certifying Agencies (NCCA). Accreditation is the process by which certifications are evaluated against defined standards and, when in compliance with these standards, are awarded recognition by the NCCA. Accreditation is proof the program has been reviewed by a panel of impartial experts and has met the stringent standards set by the NCCA. The NCCA uses established standards to assure programs meet threshold expectations of quality and validates improvement over time.

The Security Fundamentals Professional Certification (SFPC), Security Asset Protection Professional Certification (SAPPC), Security Program Integration Professional Certification (SPIPC), and Physical Security Certification (PSC) are nationally accredited with NCCA. Achieving a SPēD certification publicly confirms certificants meet comprehensive professional standards and are prepared for success in the security profession.

## ELIGIBILITY

Candidates are eligible to pursue SPēD certification if they are DOD personnel performing security enterprise functions or federal employees of a participating agency within the security workforce. Contractors assigned to and performing security functions on behalf of the DOD are eligible if requirements are outlined in either their Performance Work Statement (PWS), Statement of Work (SOW), or authorized in writing by the Contracting Officer's Representative (COR).

- Contractors must complete the 'Contractor Eligibility Verification Form' (https://www.cdse.edu/Certification/SP%C4%93D-Resources/) and submit it to their Component Service Representative (CSR) with their assessment request. For any questions regarding this process, candidates are encouraged to reach out to the CSR of the component or agency they are supporting (e.g., a contractor supporting an Air Force contract needs to reach out the Air Force CSR). CSR contact information can be located at: https://www.cdse.edu/Certification/Additional-Certification-Credential-Assistance/

- For more detailed information regarding eligibility please refer to DoDM 3305.13 (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/330513m.pdf encl. 4, para 5a).

# APC PROGRAM OVERVIEW

## WHAT IS THE APC PROGRAM?

The SPēD Program Management Office (PMO) oversees the Adjudicator Professional Certification (APC) Program. The APC Program is part of a holistic effort to professionalize the adjudication workforce by requiring personnel security adjudicators to demonstrate proficiency in a common set of competencies through training, initial testing and certification, and approved continuing education.

The APC certifies that adjudicators are qualified to perform all essential adjudicative functions related to determining the eligibility of a government employee, military service member, or contractor employee under the National Industrial Security Program (NISP) for access to classified information or assignment to sensitive duties. Certified APC Adjudicators are authorized to perform all adjudicative functions, except due process determinations. Adjudicators must acquire the Due Process Adjudicator Professional Credential (DPAPC) to issue due process determinations.

The APC Program serves as a valid and reliable indicator of an adjudicator's mastery of facts, concepts, and principles the DOD community deems critical to successfully perform functions, implement programs, and pursue missions necessary to manage risks and protect DOD assets.

The APC and DPAPC programs make certain:

- Only fully-qualified and appropriately trained professionals make clearance determinations.
- The developmental program matches job requirements and provides adjudicators with the knowledge and skills needed to perform duties at a high level of proficiency.
- Adjudicators have the opportunity and incentive to continue their professional education in order to keep themselves current on new policies, national security trends, job-related technologies, and industry trends.

## GOVERNANCE

DODI 5200.02, "DOD Personnel Security Program," establishes requirements for DOD personnel security adjudicators to obtain relevant certifications. Requirements are explained in DODM 5200.02, "Procedures for the DOD Personnel Security Program (PSP)."

The Adjudicator Certification Governance Board (ACGB) is chaired by the Office of Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) Branch Chief for Personnel Security and includes voting members from the Defense Counterintelligence and Security Agency (DCSA) Adjudication and Vetting Services (AVS), National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), DCSA Center for Development of Security Excellence (CDSE), and representatives from the Air Force, Army, Navy, and Fourth Estate. The ACGB also includes nonvoting participation from Defense Human Resources Activity (DHRA) Office of People Analytics (Personnel Security Research Center Division), Defense Office of Hearings and Appeals (DOHA), SPēD PMO, and other interested parties.

The ACGB represents the shared interests of the DOD adjudication mission and the respective workforce in certification design, management, and maintenance. The ACGB serves as the entity responsible for making the program's essential certification decisions consistent with the Standards for the Accreditation of Certification Programs published by the NCCA.

## ACCREDITATION

The APC Program is an essential element of the DOD initiative to professionalize the security workforce. Per DODM 3305.13, "DOD Security Accreditation and Certification," all certifications developed under the direction of this Manual must be accredited and maintain accreditation by the National Commission for Certifying Agencies (NCCA). Accreditation is the process by which certifications are evaluated against defined standards and, when in compliance with these standards, are awarded recognition by the NCCA. Accreditation is proof the program has been reviewed by a panel of impartial experts and has met the stringent standards set by the NCCA. The NCCA uses established standards to assure programs meet threshold expectations of quality and validates improvement over time.

The APC Program is nationally accredited with NCCA. Achieving an APC Program certification or credential publicly confirms the program meets comprehensive quality standards and that certificants are prepared for success in the adjudication mission.

## ELIGIBILITY

Candidates must be a personnel security adjudicator at an organization accepted to participate in the APC Program. Organizations accepted to participate in the APC Program include DCSA AVS, DIA, NGA, NSA, and other federal agencies. Specific APC certification requirements are summarized in this handbook on page 26.

**Note**: Eligibility for certification of non-DOD federal agencies requesting inclusion in the APC Program will be coordinated with the requesting agency, the ACGB, and the SPēD PMO.

Candidates may contact their APC Program CSR if they have questions about their eligibility (https://www.cdse.edu/Certification/Additional-Certification-Credential-Assistance/).

If a candidate successfully takes and passes an APC certification or credential assessment and it is discovered they were not eligible to take the assessment, the certification or credential will be rescinded.

# SECURITY FUNDAMENTALS PROFESSIONAL CERTIFICATION (SFPC)

## DESCRIPTION

The SFPC provides a recognized and reliable indication of a security practitioner's understanding of foundational concepts, principles, and practices needed to successfully protect DOD assets. The SFPC received its second re-accreditation in Feburary 2024, demonstrating its continued compliance with NCCA standards.

The SFPC is ideal if a candidate:

- Occupies a full-time security position for which obtaining this certification has been deemed a requirement or professional development milestone (i.e., Security Specialist, Physical Security Specialist, Industrial Security Representative or Facility Security Officer)
- Is performing security functions as an additional or embedded duty

## OBTAIN SFPC

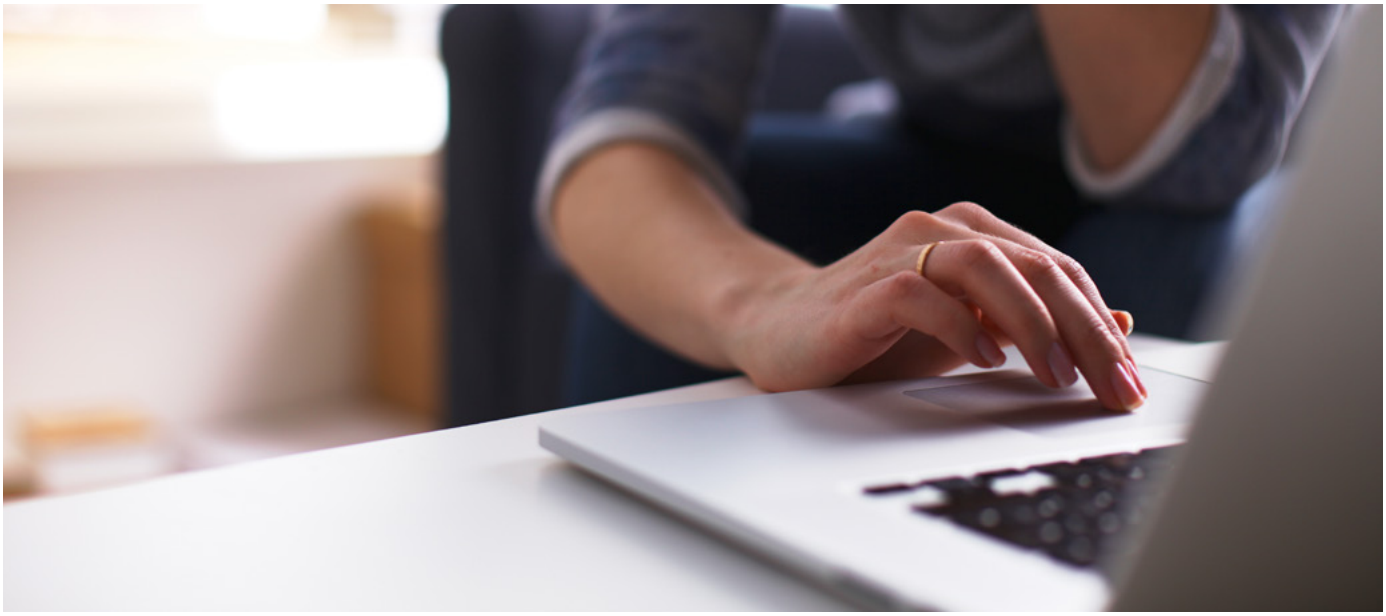
To obtain the SFPC, an eligible candidate must submit an assessment request form through their Defense Acquisition University (DAU) account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the SFPC, the candidate must successfully meet the certification assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN SFPC

To maintain SFPC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the DSTC concludes the content addressed by the certification's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.



# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **Information Security** | **Exam Weight: 28%** |
| Information Security Program | Classification Markings |
| Information Protection Principles | Marking Procedures |
| Classification Concepts | Policies and Procedures for Handling Special Types of Information |
| Classification Duration | Downgrading and Upgrading Classified Information |
| Derivative Classification Concepts | Safeguarding |
| Special Classification Considerations | Storage, Disposition, and Destruction |
| Declassification Concepts | Transmission and Transportation |
| Controlled Unclassified Information | Security Incidents |
| Release of Classified Material to Foreign Persons | Cyber and Information Security Concepts |
| **Personnel Security** | **Exam Weight: 25%** |
| Personnel Security Concepts and Principles | Personnel Security Investigations |
| Position Sensitivity Designations | Personnel Security Investigative Requirements |
| Special Personnel Security Clearance Requirements | Adjudication |
| Unfavorable Administrative Actions | Safeguarding Personnel Records |
| **Physical Security** | **Exam Weight: 12%** |
| Physical Security Concepts | Physical Security Concepts for Storage of Classified Info |
| Facility Access Control | Site Design Strategies |
| Protective Barriers | Site Lighting |
| Key, Combinations, and Lock Control | Security System Devices |
| Antiterrorism (AT) Concepts and Principles | Law Enforcement (LE) Concepts and Principles |
| Search and Seizure | |
| **Industrial Security** | **Exam Weight: 13%** |
| Contracts and Contract Administration | Industrial Security Concepts |
| Personnel and Facility Security Clearance Under the National Industrial Security Program (NISP) | Visits and Meetings |
| **General Security** | **Exam Weight: 22%** |
| Counterintelligence (CI) | Inspections and Assessments |
| Operations Security (OPSEC) Concepts | Protected Information Categories |
| OPSEC Threat Analysis, Indicators, and Measures | Research and Technology Protection Concepts |
| Insider Threat Concepts and Principles | Special Access Program (SAP) Concepts |
| Risk Management Framework (RMF) | Basic Security Forms |
| Information Technology (IT)/Information Security (IS) Security Functionality and Controls | Security Briefings |

## ASSESSMENT INFORMATION

The SFPC is a foundational assessment designed to assess a candidate's awareness of the security disciplines and their ability to apply foundational security concepts, principles, and practices. The assessment has a total of 96 multiple-choice questions to measure the candidate's competence in the SFPC Areas of Expertise. A total of 68 of 96 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 28 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have two hours and fifteen minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The SFPC assessment is training agnostic, meaning candidates do not have to take any prescribed training or courses before sitting for the certification assessment. However, preparing for the assessment by gaining additional training, education, or experience in the topic areas can be beneficial.

## COMPETENCY PREPARATORY TOOLS

Competency Preparatory Tools (CPTs) provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the SFPC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the SFPC Areas of Expertise above. The following courses may be helpful in preparing for the SFPC assessment:

- Introduction to Industrial Security, IS011.16
- Introduction to Information Security, IF011.16
- Introduction to Physical Security, PY011.16
- Introduction to Personnel Security, PS113.16
- Introduction to National Security Adjudication, PS001.18
- Special Access Programs (SAP) Overview, SA001.16
- Introduction to the Risk Management Framework (RMF), CS124.16
- Cybersecurity Awareness, CS130.16
- Foreign Disclosure Training for DOD, GS160.16
- Information Security Management, IF201.01
- DOD Security Specialist, GS101.01

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# SECURITY ASSET PROTECTION PROFESSIONAL CERTIFICATION (SAPPC)

## DESCRIPTION

The SAPPC provides a recognized and reliable indication of a security practitioner's ability to apply foundational concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DOD assets. The SAPPC received its second accreditation in February 2024, demonstrating its continued compliance with NCCA standards.

The SAPPC is ideal if a candidate:

- Occupies a full-time security position for which obtaining this certification has been deemed a requirement or professional development milestone (i.e., Security Specialist)
- Is performing security functions as an additional or embedded duty

## OBTAIN SAPPC

To obtain the SAPPC, a candidate must meet the SFPC prerequisite first, then submit an assessment request form through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the SAPPC, the candidate must successfully meet the certification assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN SAPPC

To maintain SAPPC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the DSTC concludes the content addressed by the certification's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **Information Security** | **Exam Weight: 31%** |
| Information Security Fundamentals | Classification and Declassification Concepts |
| Classification Management | Information Protection Requirements |
| Cyber for Security Professionals | |
| **Personnel Security** | **Exam Weight: 28%** |
| Personnel Security Fundamentals | Personnel Security Standards |
| **Physical Security** | **Exam Weight: 10%** |
| Physical Security Concepts | Physical Security Standards |
| **Industrial Security** | **Exam Weight: 13%** |
| Industrial Security Concepts | |
| **General Security** | **Exam Weight: 18%** |
| Threat, Vulnerability, and Risk Assessment / Management | Cyber for Security Professionals |
| Program Security | General Security Tools and Methods |

## ASSESSMENT INFORMATION

The SAPPC is an application assessment designed to assess a candidate's ability to apply concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DOD assets. The assessment has a total of 110 multiple-choice questions that are either associated with a scenario or a stand-alone question. For each scenario, the candidate is required to read and evaluate the scenario options and courses of action, and then answer multiple-choice questions based on the scenario. Both the stand-alone and scenario-based questions are designed to measure the candidate's competence in the SAPPC Areas of Expertise. A total of 74 of 110 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 36 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have two hours and fifteen minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The SAPPC assessment is training agnostic, meaning candidates do not have to take any prescribed training or courses before sitting for the certification assessment. However, preparing for the assessment by gaining additional training, education, or experience in the topic areas can be beneficial.

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the SAPPC assessment. Outside of CPTs, there are no other official training materials or courses for SPeD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the SAPPC Areas of Expertise above. The following courses may be helpful in preparing for the SAPPC assessment:

- Introduction to Industrial Security, IS011.16
- Introduction to Information Security, IF011.16
- Introduction to Physical Security, PY011.16
- Introduction to Personnel Security, PS113.16
- Introduction to National Security Adjudication, PS001.18
- Special Access Programs (SAP) Overview, SA001.16
- Introduction to the Risk Management Framework (RMF), CS124.16
- Cybersecurity Awareness, CS130.16
- OPSEC Awareness for Military Members, DOD Employees and Contractors, GS130.16

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# SECURITY PROGRAM INTEGRATION PROFESSIONAL CERTIFICATION (SPIPC)

## DESCRIPTION

The SPIPC provides a recognized and reliable indication of a security practitioner's understanding and ability to apply risk management and security program management concepts, principles, and practices. The SPIPC received its second re-accreditation in February 2024, demonstrating its continued compliance with NCCA standards.

The SPIPC is ideal if a candidate:

- Occupies a full-time security position for which obtaining this certification has been deemed a requirement or professional development milestone
- Is performing security functions as an additional or embedded duty

## OBTAIN SPIPC

To obtain the SPIPC, a candidate must meet the SFPC prerequisite first, then submit an assessment request form through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the SPIPC, the candidate must successfully meet the certification assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN SPIPC

To maintain SPIPC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the DSTC concludes the content addressed by the certification's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **Planning, Programming, Budgeting, and Concepts** | **Exam Weight: 8%** |
| Planning, Programming, Budgeting, and Execution (PPB&E) Process, Concepts, and Principles | |
| **Risk Assessment** | **Exam Weight: 41%** |
| Risk Management Benefits and Costs | Sources of Threat and Vulnerability Information |
| Risk Assessment Concepts and Principles | |
| **Risk Management** | **Exam Weight: 35%** |
| Strategies for Controlling and/or Managing Risks | |
| **Program and Mission Assurance** | **Exam Weight: 16%** |
| Approaches and Criteria for Evaluating Effectiveness of Security Policies, Plan, and Program Activities | Essential Functions of a Security Program |

## ASSESSMENT INFORMATION

The SPIPC is an application assessment designed to assess a candidate's ability to apply risk assessment and security program management concepts, principles, and practices. The assessment has a total of 75 multiple-choice questions that are either associated with a scenario or a stand-alone question. For each scenario, the candidate is required to read and evaluate the scenario options and courses of action, and then answer multiple-choice questions based on the scenario. Both the stand-alone and scenario-based questions are designed to measure the candidate's competence in the SPIPC Areas of Expertise. All 75 questions are scored, meaning they count toward the candidate's pass/fail result. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have one hour and forty minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The SPIPC assessment is training agnostic, meaning candidates do not have to take any prescribed training or courses before sitting for the certification assessment. However, preparing for the assessment by gaining additional training, education, or experience in the topic areas can be beneficial.

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the SPIPC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# PHYSICAL SECURITY CERTIFICATION (PSC)

## DESCRIPTION

The PSC is ideal for DOD, Industry, and federal members performing physical security functions. The PSC was accredited by NCCA in March 2016 and received re-accreditation in April 2021, demonstrating its continued compliance with NCCA standards.

The PSC is ideal if a candidate:

- Occupies a full-time security position for which attainment of this certification has been deemed a requirement or professional development milestone
- Is performing Physical Security functions as an additional or embedded duty

## OBTAIN PSC

To obtain the PSC, an eligible candidate must submit an assessment request form through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the PSC, the candidate must successfully meet the certification assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN PSC

To maintain PSC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the DSTC concludes the content addressed by the certification's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **Physical Security Concepts** | **Exam Weight: 22%** |
| Physical Security Concepts | Facility Access Control |
| **Physical Security Standards** | **Exam Weight: 24%** |
| Physical Security Standards for Storage of Classified Information | Physical Security Standards for Sensitive Conventional Arms, Ammunition, and Explosives |
| Physical Security Standards for Special Assets/Resources | |
| **Standards, Countermeasures, and Planning** | **Exam Weight: 41%** |
| Protective Barriers | Site Lighting |
| Keys, Combinations, and Lock Controls | Site Design Strategies |
| Security Systems Devices | |
| **Physical Security Planning and Implementation** | **Exam Weight: 13%** |
| Physical Security Planning and Plan Implementation | Emergency Management/Emergency Response |

## ASSESSMENT INFORMATION

The PSC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of physical security functions. The assessment has a total of 110 multiple-choice questions to measure the candidate's competence in the PSC Areas of Expertise. A total of 70 of 110 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 40 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have one hour and forty minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The PSC assessment is training agnostic, meaning candidates do not have to take any prescribed training or courses before sitting for the certification assessment. However, preparing for the assessment by gaining additional training, education, or experience in the topic areas may prove beneficial.

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the PSC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the PSC Areas of Expertise above. The following courses and shorts may be helpful in preparing for the PSC assessment:

- Antiterrorism Officer (ATO) Level II, GS109.16
- DOD Locks Approved to Safeguard Classified and Sensitive Materials, PY001.16
- Electronic Security Systems, PY250.16
- Exterior Security Lighting, PY109.16
- Introduction to Physical Security, PY011.16
- Lock and Key Systems, PY104.16
- Physical Security and Asset Protection, PY201.PR
- Physical Security Measures, PY103.16
- Physical Security Planning and Implementation, PY106.16
- Storage Containers and Facilities, PY105.16

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# INDUSTRIAL SECURITY OVERSIGHT CREDENTIAL (ISOC)

## DESCRIPTION

The ISOC is ideal for DOD, Industry, and federal members under the National Industrial Security Program (NISP).

The ISOC is ideal if a candidate:

- Occupies a full-time Industrial Security position for which obtaining this credential has been deemed a requirement or professional development milestone
- Is performing Industrial Security functions as an additional or embedded duty

## OBTAIN ISOC

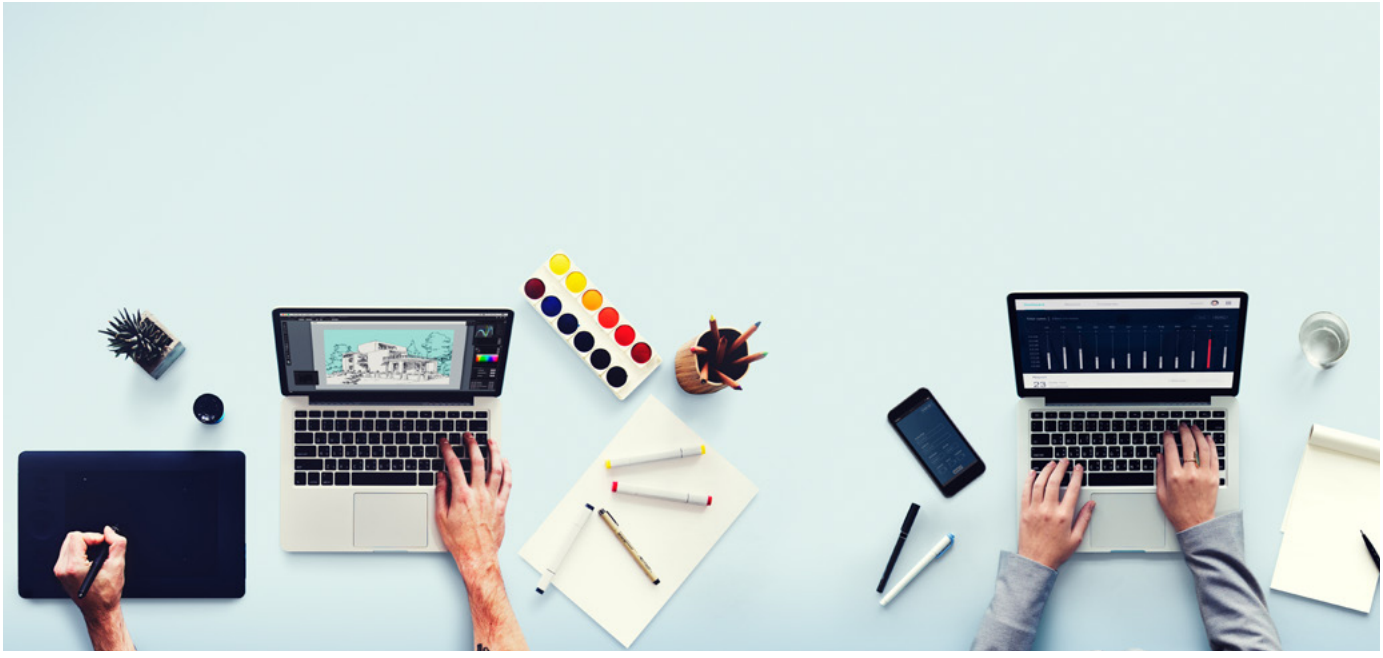
To obtain the ISOC, a candidate must submit an assessment request form through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the ISOC, the candidate must successfully meet the credential assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN ISOC

To maintain ISOC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the DSTC concludes the content addressed by the credential's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.



# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **Industrial Security Basics** | **Exam Weight: 33%** |
| Facility Clearance Requirements and Procedures | Personnel Security Concepts |
| Business Structures | Foreign Ownership, Control or Influence (FOCI) Fundamentals |
| Contractor/Sub-Contractor Reporting Responsibilities | |
| **Security Reviews and Inspection** | **Exam Weight: 27%** |
| Security Review Procedures | Pre-Security Review Research |
| Security Violations and Administrative Inquiry Procedures | Post-Security Review Actions |
| **Security Systems and Requirements** | **Exam Weight: 40%** |
| Security-Related Systems and Databases | Counterintelligence Integration |
| International Security Requirements | Information Systems Security |
| Specialized Mission Areas | Specialized Briefings/Education |
| Classification and Retention | Safeguard/Storage and Classified Material Controls |
| Classified Visits and Meetings | Security-Related Systems and Databases |

## ASSESSMENT INFORMATION

The ISOC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of industrial security oversight functions. The assessment has a total of 113 multiple-choice questions to measure the candidate's competence in the ISOC Areas of Expertise. A total of 76 of 113 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 37 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have one hour and forty minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The ISOC assessment is based on training and experience in the topic areas outlined under the areas of expertise. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the ISOC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the ISOC Areas of Expertise above. The following courses and shorts may be helpful in preparing for the ISOC assessment:

- Preparing the DD Form 254, IS128.16
- Basic Industrial Security for the Government Security Specialist, IS050.CU
- Business Structures in the NISP, IS051.16
- Clearances in Industrial Security: Putting it All Together, IS125.16
- Facility Clearances in the NISP, IS140.16
- Foreign Ownership, Control or Influence (FOCI), IS170.16
- FSO Orientation for Non-Possessing Facilities, IS020.CU
- FSO Program Management for Possessing Facilities, IS030.CU
- Getting Started Seminar for New FSOs, IS121.10
- Industrial Security Basics, IS122.16
- Industrial Security Databases and Systems, IS124.16
- Industrial Security for Non-Security Government Personnel, IS230.CU
- International Visit Requests, IS005.16
- Introduction to Industrial Security, IS011.16
- National Interest Determination (NID), IS155.16
- NISP Reporting Requirements, IS150.16
- NISP Security Violations and Administrative Inquiries, IS126.16
- NISP Self-Inspection, IS130.16
- Personnel Clearances in the NISP, IS142.16
- Safeguarding Classified Information in the NISP, IS109.16
- Security Support to International Programs in Cleared Defense Industry, IS181.16
- Transmission and Transportation for Industry, IS107.16
- Understanding Foreign Ownership, Control or Influence (FOCI), IS065.16
- Visits and Meetings in the NISP, IS105.16

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# ANTITERRORISM CREDENTIAL (ATC)

## DESCRIPTION

The ATC provides a recognized and reliable indication of a security practitioner's understanding and ability to specify purpose, function, and role of the Antiterrorism (AT) Plan to the effective functioning of an AT Program, and appropriately apply that knowledge to contribute to the effective functioning of an AT program.

## ELIGIBILITY

Candidates are eligible to pursue the Antiterrorism Credential (ATC) if they are DOD personnel or contractors currently holding an Antiterrorism Officer (ATO) position and have completed the AT-Level II training requirements outlined by their component or agency.

The ATC is ideal if a candidate:

- Currently holds an ATO position and have completed the AT-Level II and training requirements outlined by their component or agency.
- Occupies a full-time security position for which attainment of this credential has been deemed a requirement or professional development milestone.

## OBTAIN ATC

To obtain the ATC, an eligible candidate must submit an assessment request form along with an ATO appointment letter signed by their supervisor through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the ATC, the candidate must successfully meet the credential assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN ATC

To maintain ATC, certificants must successfully complete and record 75 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year credential maintenance cycle.

## RETESTING

Candidates will be required to retest if the content addressed by the credential assessment modules is significantly out of date, regardless of current credential maintenance. Candidates will also be required to retest if the candidate fails to meet the credential maintenance requirements within a two-year credential maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **AT Planning** | **Exam Weight: 17%** |
| AT Program Elements | Budget Support to AT Plans |
| AT Plan Fundamentals | |
| **Risk Management** | **Exam Weight: 33%** |
| FPCON and RAM Planning, Development, and Execution | Physical Security Fundamentals |
| AT Risk Assessment and Risk Management Process | |
| **AT Standards and Training** | **Exam Weight: 29%** |
| Antiterrorism Officer | AT Training |
| AT Exercises | DOD Enterprise-Wide AT Standards |
| **Reporting and Reviewing** | **Exam Weight: 21%** |
| AT Working Groups | Use of Appropriate Information Reporting System or Tool (e.g., eGuardian System) |
| Use of AT Program Review | |

## ASSESSMENT INFORMATION

The ATC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of anti-terrorism functions. The assessment has a total of 100 multiple-choice questions to measure the candidate's competence in the ATC Areas of Expertise. A total of 75 of 100 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 25 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have two hours and fifteen minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The ATC assessment is based on training and experience in the topic areas outlined under the areas of expertise. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the ATC Areas of Expertise above. The following courses may be helpful in preparing for the ATC assessment:

- Antiterrorism Level 1 Training, DS104.16
- Physical Security Planning and Implementation, PY106.16
- Antiterrorism Officer (ATO) Level II, GS109.16
- Risk Management Project and Advanced Studies, ED603.PR

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the ATC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

# SPECIAL PROGRAM SECURITY CREDENTIAL (SPSC)

## DESCRIPTION

The SPSC is ideal for personnel who will be or are already performing Security Officer functions for and/or on behalf of the DOD Special Access Programs (SAP).

The SPSC is ideal if a candidate:

- Is performing Security Officer functions for or on the behalf of the DOD SAPs
- Occupies a full-time security position for which attainment of this credential has been deemed a requirement or professional development milestone

## OBTAIN SPSC

To obtain the SPSC, a candidate must meet the SFPC prerequisite first, then submit an assessment request form through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the SPSC, the candidate must successfully meet the credential assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN SPSC

To maintain SPSC, certificants must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year credential maintenance cycle.

## RETESTING

Candidates will be required to retest if the content addressed by the credential assessment modules is significantly out of date, regardless of current credential maintenance. Candidates will also be required to retest if the candidate fails to meet the credential maintenance requirements within a two-year certification maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| Personnel Security | Exam Weight: 6% |
| Physical Security | Exam Weight: 11% |
| Program Security | Exam Weight: 14% |
| Vulnerabilities Assessment and Management | Exam Weight: 14% |
| Cybersecurity | Exam Weight: 11% |
| Information Security | Exam Weight 14% |
| Classification Management | Exam Weight: 11% |
| SAP Security and Policy | Exam Weight: 12% |
| Security Education and Awareness | Exam Weight: 7% |

## ASSESSMENT INFORMATION

The SPSC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of special assess program (SAP) functions. The assessment has a total of 94 multiple-choice questions to measure the candidate's competence in the SPSC Areas of Expertise. A total of 76 of 94 questions are scored, meaning they count toward the candidate's pass/fail result. The remaining 18 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have two hours and fifteen minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

The SPSC assessment is based on training and experience in the topic areas outlined under the areas of expertise. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

## COMPETENCY PREPARATORY TOOLS

CPTs provide a means to gauge a candidate's experience and knowledge of the security competencies tested in the SPSC assessment. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are encouraged to familiarize themselves with courses addressing the topics noted in the SPSC Areas of Expertise noted above. The following courses may be helpful in preparing for the SPSC assessment:

- Special Access Program Personnel Security Official (SPO) Training, SA106.16
- Introduction to Special Access Programs, SA101.PR or SA101.10.PR
- Orientation to SAP Security Compliance Inspections, SA210.PR
- SAP Mid-Level Security Management, SA201.PR or SA201.10.PR
- Sensitive Compartmented Information (SCI) Security Refresher, SCI100.16
- Special Access Program (SAP) Security Annual Refresher, SA002.06
- Special Access Programs (SAP) Overview, SA001.16
- ICD 705 Physical Security Construction Requirements for SAP, SA501.16

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

# ADJUDICATOR PROFESSIONAL CERTIFICATION (APC)

## DESCRIPTION

The APC is required for all Personnel Security Adjudicators in the DCSA AVS, DOD IC, and personnel security adjudicators at other agencies accepted to participate in the program. The APC was accredited by NCCA in 2018 and reaccredited in 2023.

## ELIGIBILITY

Candidates must be a personnel security adjudicator at an organization accepted to participate in the APC Program. Organizations accepted to participate in the APC Program include DCSA AVS, DIA, NGA, NSA, and other federal agencies.

**Note**: Eligibility for certification of non-DOD federal agencies requesting inclusion in the APC Program will be coordinated with the requesting agency, the ACGB, and the SPēD PMO.

## OBTAIN APC

In addition to being a personnel security adjudicator at an organization accepted to participate in the APC Program, prior to attempting the APC assessment, candidates must complete the following:

1) Introduction to National Security Adjudication (PS001.18), via STEPP
2) Fundamentals of National Security Adjudications (PS101.10), via STEPP
3) Satisfy and document on-the-job experience requirements.

**Note**: PS001.18 and PS101.10 can be accessed through (PS001.18 - https://cdse.usalearning.gov/enrol/index.php?id=735 and PS101.10 - https://cdse.usalearning.gov/enrol/index.php?id=747).

Candidates who are personnel security adjudicators at an organization accepted to participate in the APC Program, who already have two years of adjudication work experience covering adjudication topics (for example, SEAD 4; FIS; derogatory / non-derogatory cases; DODM 5200.02; Whole Person Concept) may with the approval of their employing organization substitute that adjudication work experience in lieu of completing the requirements described above.

To obtain the APC, Candidates must submit an assessment request form along with required documentation through their DAU account which will be verified by their CSR before being approved to take the APC assessment. In order to be conferred the APC, the candidate must successfully meet the assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN APC

To maintain APC, candidates must successfully complete and record 100 professional development units (PDUs), 50 of which must be security related, and submit their Certification Renewal Package (CRP) within their two-year certification maintenance cycle.

## RETESTING

Candidates will be required to retest if the ACGB concludes the content addressed by the certification's assessment modules is significantly out of date, regardless of current certification maintenance. Candidates will also be required to retest if the candidate fails to meet the certification maintenance requirements within a two-year certification maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| **National Security & Personnel Security Program** | **Exam Weight: 29%** |
| National Security & Personnel Security Program | Type and Scope of Investigations |
| Types of Information Sources | |
| **Adjudication Process** | **Exam Weight: 56%** |
| Adjudication Process Using the Whole Person Concept | Procedures for Due Process |
| Adjudicative Guidelines | Critical Terminologies |
| Reciprocity | |
| **Personnel Security Process** | **Exam Weight: 15%** |
| Pertinent Statutes, Executive Orders, and Regulations Governing the Personnel Security Process | Levels of Eligibility to Occupy a Sensitive Position and/or Access Classified Information |

## ASSESSMENT INFORMATION

The APC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of adjudication functions. The assessment has a total of 114 multiple-choice questions that are either associated with a scenario or a stand-alone question. For each scenario, the candidate is required to read and evaluate the scenario options and courses of action, then answer multiple-choice questions based on the scenario. Both the stand-alone and scenario-based questions are designed to measure the candidate's competence in the APC Areas of Expertise. A total of 80 of 114 questions on the APC are scored, meaning they count toward the candidate's pass/fail result. The remaining 34 questions are unscored and used to test new items that can be used to refresh the assessment as needed; these questions do not count toward the candidate's pass/fail result. Candidates are unaware of which items are scored or unscored; all questions are incorporated throughout the assessment. Questions are dichotomously scored, meaning there are only two scoring options - correct and incorrect. For each correct answer on a scored item, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because they are unaware of which items are scored and any unanswered questions are marked as incorrect. Candidates have two hours and fifteen minutes to complete the assessment.

## PREPARING FOR ASSESSMENT

To take the APC assessment, candidates must meet training, experience, and testing requirements for credentialing. Preparing for the APC assessment by gaining additional training, education, or experience in the topic areas may prove beneficial.

## COMPETENCY PREPARATORY TOOLS

CPTs provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the APC assessment.

CPTs help candidates prepare for the APC assessment. To take the APC assessment, candidates must meet training, experience, and testing requirements for certification. Outside of CPTs, there are no other official training materials or courses for SPēD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are invited to familiarize themselves with courses addressing the topics noted in the APC Areas of Expertise. CDSE provides diverse security courses and products to DOD personnel, DOD contractors, employees

of other federal agencies, and selected foreign governments. Training is presented through a variety of learning platforms and is streamlined to meet performance requirements.

CPTs and courses can be accessed through the Security Training, Education, and Professionalization Portal (STEPP): (https://cdse.usalearning.gov/login/index.php).

To view available CDSE-offered training, visit https://www.cdse.edu/Training/.

CDSE has established a program of advanced and graduate-level courses designed specifically to broaden DOD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. All of the courses are tuition free and are offered in a virtual instructor-led environment.

To view available CDSE-offered education, visit https://www.cdse.edu/education/index.html.

Candidates are also encouraged to familiarize themselves with the CDSE-offered Adjudicator Toolkit available here: https://www.cdse.edu/Training/Toolkits/Adjudicator-Toolkit/

# DUE PROCESS ADJUDICATOR PROFESSIONAL CREDENTIAL (DPAPC)

## DESCRIPTION

The DPAPC provides the recognition and official record of an individual's demonstrated understanding and application of occupational and technical knowledge, skills, and expertise necessary to proficiently perform essential due process adjudicator tasks (i.e., writing Statement of Reasons (SORs), evaluating responses to SORs, recommending eligibility determinations or other functions following evaluation of responses to SORs).

## ELIGIBILITY

Personnel security adjudicators employed by the DOD IC and DCSA AVS are eligible to pursue the DPAPC. Federal Government employees working as personnel security adjudicators are also eligible as long as they are employed by an agency accepted for participation in the APC Program performing due process functions.

Candidates must meet the following training, experience, and testing requirements for credentialing. Candidates must successfully complete a program of instruction, including the Introduction to National Security Adjudication (PS001.18), Fundamentals of National Security Adjudication (PS101.10), and Advanced National Security Adjudications (PS301.10) courses provided by CDSE, or equivalent instruction as determined by CDSE on behalf of the Director, DCSA. Candidates must also satisfy additional due process experience requirements and submit the documentation to their immediate supervisor, and obtain a passing score on the DPAPC assessment.

**Note**: Eligibility for certification of non-DOD federal agencies requesting inclusion in the APC Program will be coordinated with the requesting agency, the ACGB, and the SPēD PMO.

## OBTAIN DPAPC

To obtain DPAPC, candidates must be a DOD Personnel Security Adjudicator at DCSA AVS, DOD IC, or an approved federal agency Personnel Security Adjudicator at an approved federal agency, hold the APC, complete Advanced National Security Adjudication or equivalent as determined by the ACGB, and satisfy on-the-job requirements identified in the DOD Adjudicator Certification and Due Process Credential Experience Documentation Worksheet. To obtain the DPAPC, an APC certificant must submit an assessment request form along with required documentation through their DAU account which will be verified by their CSR before being approved to take the assessment. In order to be conferred for the DPAPC, the candidate must successfully meet the certification assessment's qualifying score. There are no exceptions or waivers to these requirements.

## MAINTAIN DPAPC

To maintain DPAPC, candidates must maintain an APC.

## RETESTING

Candidates will be required to retest if the ACGB concludes the content addressed by the credential assessment modules is significantly out of date, regardless of current credential maintenance. Candidates will also be required to retest if the candidate fails to meet the credential maintenance requirements within a two-year credential maintenance cycle.

# AREAS OF EXPERTISE

| Area of Expertise | |
|---|---|
| Adjudication Process Using the Whole Person Concept (WPC) | Exam Weight: 57% |
| Procedures for Due Process | Exam Weight: 36% |
| Pertinent Statutes, Executive Orders, and Regulations Governing the Personnel Security Process | Exam Weight: 7% |

## ASSESSMENT INFORMATION

The DPAPC is a foundational assessment designed to assess a candidate's ability to demonstrate they have mastered the foundational knowledge and skills critical to the performance of the due process adjudication function. The assessment has a total of 60 multiple-choice questions that are either associated with a scenario or a stand-alone question. For each scenario, the candidate is required to read and evaluate the scenario options and courses of action, then answer multiple-choice questions based on the scenario. Both the stand-alone and scenario-based questions are designed to measure the candidate's competence in the DPAPC Areas of Expertise. All 60 questions on the DPAPC are scored, meaning they count toward the candidate's pass/fail result. Questions are dichotomously scored, meaning there are only two scoring options – correct and incorrect. For each correct answer, candidates receive one point toward their total score. Candidates are encouraged to answer all questions because any unanswered questions are marked as incorrect. Candidates have two hours to complete the assessment.

## PREPARING FOR ASSESSMENT

To take the DPAPC assessment, candidates must meet training, experience, and testing requirements for credentialing. Preparing for the DPAPC assessment by gaining additional training, education, or experience in the topic areas may prove beneficial.

## COMPETENCY PREPARATORY TOOLS

CPTs (https://www.cdse.edu/Certification/Prepare-for-Certification/) provide candidates with the means to gauge personal experience and knowledge of the security competencies tested in the DPAPC assessment. Outside of CPTs, there are no other official training materials or courses for SPeD Certifications or Credentials. Candidates should be cautious of any entities offering such products.

Candidates are also invited to familiarize themselves with courses addressing the topics noted in the DPAPC Areas of Expertise. CDSE provides diverse security courses and products to DOD personnel, DOD contractors, employees of other federal agencies, and selected foreign governments. Training is presented through a variety of learning platforms and is streamlined to meet performance requirements.

Before taking the DPAPC assessment, candidates must first complete the following training courses provided by CDSE, or equivalent instruction as determined by CDSE on behalf of the Director, DCSA:

- Introduction to National Security Adjudications (PS001.18)
- Fundamentals of National Security Adjudications (PS101.10)
- Advanced National Security Adjudications (PS301.10)

To view available CDSE-offered training, visit https://www.cdse.edu/Training/.

CDSE has established a program of advanced and graduate-level courses specifically to broaden DOD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. All of the courses are tuition free and are offered in a virtual instructor-led environment.

To view available CDSE-offered education, visit https://www.cdse.edu/education/index.html.

# CERTIFICATION AND CREDENTIALING

## ASSESSMENT DEVELOPMENT

The initial step in developing a fair and objective SPēD Certification and APC assessment was to conduct a job/practice analysis. A job/practice analysis was conducted to assure that the knowledge and skills identified were representative of those required by professionals across the DOD, including tasks and functions performed by civilian, military, and contractor personnel. The job/practice analysis, divided into four phases, was designed and facilitated by DCSA contractors, DOD leaders, and subject matter experts (SMEs) from the uniformed services and multiple DOD agencies. These phases included a detailed review of previous studies, defining specific work performed and required knowledge and skills necessary to perform that work, verifying the results with SMEs, and approval by the appropriate governance board.

The job/practice analysis led to the creation of the DOD Security Skill Standards (DS3), which clarifies DOD expectations of what personnel security professionals must know and successfully perform to support DOD security functions. This information was then used to generate the certification test outline (blueprint) that specifies objectives associated with the knowledge and skill topics and sub-topics measured by each specific SPēD Certification and APC Program assessment.

## DETERMINING PASSING SCORES

The Angoff method was used to set the minimum passing score for the SPēD certification and credential assessments. The Angoff method has a well-established history of determining credible passing standards for multiple-choice examinations and is easily adapted by the SPēD certification, APC, and credential assessments.

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 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 item on the assessment.

A panel of SMEs made predictions for each item (represented as a percentage) and used the average of the ratings on the items to set 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.

## CERTIFICATION AND CREDENTIALING PROCESS

# CANDIDATE MANAGEMENT PLATFORM

**NOTE:** Profile changes in the Virtual Campus may take up to two hours before they are reflected within the system.

## DEFENSE ACQUISITION UNIVERSITY (DAU)

### CREATE AN ACCOUNT

1. Create new DAU account at https://saar.dau.edu. Using Microsoft Edge or Google Chrome is recommended.
2. Under "Request/Reestablish DAU Platform Access", select either "Department of Defense Agency" or "Other Federal Agency (Non-DOD), whichever is applicable.
3. Read the Warning Notice and select "Continue" if you agree.
4. Select your authentication certificate when using your DOD Common Access Card (CAC).
5. Read the information regarding your DAUID and answer the question accordingly.
6. Select "Virtual Campus (Online Training)".
7. Enter the reason you are requesting access to the system, i.e. "to obtain a SPēD certification and/or credential."
8. Complete all of the demographic information.
9. Read and accept the User Agreement
10. Enter the Security Code and select "Submit".

You will receive a "Welcome" email within 24 hours. Be sure to check your junk mailbox. If you do not receive an email within 24 hours, contact the DAU Help Desk at (866) 568-6924 for assistance.

### ACCOUNT LOG IN

1. Log in to your DAU account at https://dau.csod.com/.
2. The login window will pop up. Select the "Sign in with CAC" button at the bottom of the screen.
3. If you do not use your CAC, enter your Username (government email address) and Password.
4. If "Select a Certificate" appears on the screen, use the authentication option.
5. Once you have completed the single sign on (SSO) process, DAU should open up with your agency logo in the upper left corner.

### UPDATE USERNAME AND EMAIL ADDRESS

1. Log in to your DAU account at https://dau.csod.com/.
2. Hover your most over the Home tab at the top left and select "Universal Profile".
3. Once the page loads, select "Update User Record Form" at the top.
4. Locate the email field and enter your new email address. This email address will also be your DAU Username.
5. After you have finished making updates, select "Submit" to save the changes.
6. Hover your mouse over the Home tab at the top left and select "Welcome" to return to the main screen.

## UPDATE ACCOUNT INFORMATION

1. Login to your DAU account at https://dau.csod.com/.
2. Hover your mouse of the Home tab at the top left and select Universal Profile.
3. Once the page loads, select the Edit User Record Form link at the top.
4. Locate the Organization section and click on the box with the "X". This will clear the field.
5. Select the box again and enter your agency in the search box and select the search button.
6. Results will display on the screen. Select the title associated with your organization and it will automatically be entered on your profile.

   **NOTE:** If no results populated after your search, select, "Cancel". Select the box again by Organization and use the page numbers and arrows at the bottom right to scroll through all of the available organizations. You will not be able to save your profile until an Organization has been selected.
7. Once complete, select "Submit" to save the changes.
8. Hover your mouse over the Home tab at the top left and select "Welcome" to return to the main screen.

## RESET YOUR PASSWORD

1. Select the "Need help signing in" and then "Forgot password" buttons.
2. The reset password window will pop up. Enter the email address associated with your DAU account.
3. Select "Reset via SMS" (if a mobile number has been configured) or "Reset via email".
4. You will receive an email to reset your password. Follow the instructions within the email. If you do not receive the reset password email in your inbox, check your junk mailbox.

Contact the DAU Help Desk at (866) 568-6924 if you require assistance resetting your password.

# PREPARING FOR AN ASSESSMENT

## COMPETENCY PREPARATORY TOOLS (CPTS)

CPTs help you prepare for your SPēD certification and credential assessment. CPTs and their references are aligned with the April 2023 DOD Security Skill Standards (DS3) and the Defense Security Essential Body of Knowledge (D-SEBOK), which is the DOD security community's expectations of what security professionals need to know to perform various aspects of their jobs. The D-SEBOK is an exhaustive list of topics the security professional must know; however, the SPēD assessments test for a subset of topics according to the Areas of Expertise.

The CPTs provide an overall scope of what may be covered by an assessment, but users should not assume that every CPT topic will be on the assessment. Topic Areas (TA) and/or Areas of Expertise (AoE) that may be covered by an assessment are thoroughly vetted by Subject Matter Experts (SME)s throughout the DOD security community on a scheduled or as needed basis as required by National Accreditation Standards.

To access and use the CPTs, users should log-in to their STEPP account at cdse.usalearning.gov/ and search "CPT" and follow enrollment instructions.

## ASSESSMENT-TAKING TIPS

- Relax before the assessment.
- Check out the test center location in advance.
- Arrive early.
- Keep a positive attitude throughout the entire assessment session.
- Trust your first impression.
- Read the entire question carefully.
- Do not overanalyze the questions or answers.
- Skip questions you are uncertain about and return to them later.
- Do not look for answer patterns.
- Do not select an answer just because of its length.
- Pace yourself.
- Use your time wisely.
- Answer all questions; there is no penalty for guessing.

## ASSESSMENT ADMINISTRATION

After scheduling an assessment, candidates will receive a confirmation email with information about the test center's admission, rescheduling, and cancellation policies.

Arrive at the test center at least 30 minutes before a scheduled assessment time. Candidates may be refused admission if they are late for their assessment.

Provide two forms of identification as directed in the testing confirmation email.

Candidates will be provided with the following materials:

- Blank paper or whiteboards and appropriate writing instruments. These materials are for your benefit during the testing session and will be collected by your proctor upon the completion of your test.
- Computer to take the assessment

The following personal items are not permitted in testing rooms:

Cellular phones, hand-held computers/personal digital assistants (PDAs) or other electronic devices (including smartwatches and Fitbits), pagers, watches, wallets, purses, hats, bags, coats, books, and notes. These items must be left outside of the test center or stored in a secured area designated by the test center administrator.

## CERTIFICATION AND CREDENTIAL ENROLLMENT

1. Locate and select the certification or credential enrollment form on the CDSE website at https://www.cdse.edu/Certification/Request-to-take-an-Assessment/.
2. Complete all required fields, to include assessment accommodations request, if applicable.
   **NOTE:** The 'State' field must contain two characters.
3. Select the new SPēD certification or credential that you are requesting enrollment for.
   **NOTE:** Certifications and credentials that you hold or are already pursuing will already be selected. **DO NOT** remove the checkmark.
4. Select 'Next' at the bottom of the form.
5. Attach all required supporting documentation, if applicable.
6. Select 'Submit for Approval' at the bottom of the form.
7. Your form will be reviewed for approval within seven business days by your CSR.

## SCHEDULE AN ASSESSMENT

Before scheduling a SPēD certification or credential assessment, you must submit an assessment request with required supporting documentation (if required), to your CSR to obtain authorization to take a SPēD assessment.

1. Log in to your DAU account at https://dau.csod.com/.
2. Hover over the Learning tab and select "View Your Transcript".
3. On your Active tab, certifications and credentials that you are enrolled in will appear. Select, "Manage" next to your certification to view all of the information.
4. Under "PearsonVue Exam" locate the certification or credential you wish to schedule and select "Launch".
5. Once the assessment launches, select "Next".
6. Read all of the information on the page and within 24 hours you will receive an email from Pearson Vue to schedule your assessment.

**NOTE:** If the assessment does not appear on your transcript, wait 24 hours from your enrollment to allow the assessment authorization to process.

## CANCEL OR RESCHEDULE AN ASSESSMENT

Candidates may cancel or reschedule an assessment without penalty at least 24 hours prior to their assessment test date and time. If candidates cancel their assessment less than 24 hours in advance, they will be placed on a 90-day hold and will not be allowed to reschedule their assessment until that 90-day period expires. Canceling or rescheduling an assessment cannot be made by the SPēD PMO, DOD SPēD CSR, or the test center. **All changes must be made through your DAU or Pearson VUE account**. You may call Pearson VUE at 1-888-477-0284 to cancel or reschedule an assessment, or visit https://home.pearsonvue.com/Test-takers/Customer-service.aspx. If extenuating circumstances warrant an exception, candidates can contact their SPēD Program CSR.

Candidates may reschedule existing appointments within the 90-calendar day authorization allotment.

## NO-SHOW

An assessment "no-show" is defined as a candidate who:

- Does not appear for the exam on the scheduled appointment date
- Cancels exam appointment less than 24 hours before the scheduled appointment date
- Arrives at the testing center after their appointment time
- Arrives at the testing center without proper identification

**Note**: No-show candidates will be placed on a 90-day hold and will not be allowed to reschedule until the 90-day period expires.

## ACCOMMODATIONS FOR DISABILITIES

If requested, SPēD will provide reasonable accommodations in compliance with the Americans with Disabilities Act (ADA), the Rehabilitation Act, and DOD policy.

In general, an accommodation is made when a disability is relieved by an auxiliary aid or a procedural change during assessment administration. Reasonable accommodation will be made for a known physical disability or disability related to a mental health condition.

Accommodation types:

- Extra time – half assessment time
- Extra time – 30 minutes
- Extra time – double assessment time
- Glucose testing supplies
- Separate room
- Separate room and reader
- Separate room and recorder
- Separate room and sign language interpreter
- Sign language interpreter – communication only

A request for a reasonable accommodation is a verbal or written statement from a candidate requesting an adjustment or change for a reason related to a disability. A request does not have to use any jargon, such as "reasonable accommodation," "disability," or "Rehabilitation Act." If candidates have a disability, they may request a reasonable accommodation, even if they have not previously disclosed the existence of a disability.

Candidates are responsible for seeking reasonable accommodations when completing the assessment enrollment form. Candidates should only select the reasonable accommodation that have been granted with supporting documentation. The supporting documentation should be sent directly to the candidates CSR. The CSR should review the assessment enrollment form, to include the supporting documentation associated to the selected reasonable accommodations prior to approving the assessment enrollment form. If the candidate does not provide supporting documentation the CSR should contact the candidate. Once the CSR has verified the request and supporting documentation, the CSR should approve the assessment enrollment form. The candidate will receive a confirmation email from DAU to schedule their assessment.

- Candidates can refer to Pearson VUE Comfort Aid List (https://home.pearsonvue.com/Test-takers/Accommodations/Pearson-VUE-Comfort-Aid-List-PDF.aspx) for pre-approved items that do not require reasonable accommodations.

The SPēD PMO may request documentation from an appropriate health care or rehabilitation professional about a candidate's disability and functional limitations 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 need for, and the ability to, provide any specific accommodation is determined on an individual basis, depending on the unique circumstances involved and taking into consideration for a specific disability and the existing limitations in completing the certification process.

The SPēD PMO, along with the testing location, will make reasonable efforts to accommodate a candidate's request by offering an alternative means to take the certification assessment. If it would impose an undue burden to provide the required testing environment, candidates will be notified with a written explanation of the denial and a statement of the reasons for the denial. Grievances regarding accommodations may be brought to the DCSA Office of Equal Employment Opportunity at DCSA.quantico.DCSA-hq.mbx.eeo@mail.mil or 571-305-6737.

## RETAKING AN ASSESSMENT

If candidates do not obtain a passing score, are a no-show, or do not complete the assessment, they can schedule to retake the same assessment or credential after the required waiting period. The waiting period for the APC and DPAPC assessment is 45 days after the first sitting (or attempt), and 90 days for each sitting after. The waiting period for all other SPēD certifications or credentials is 90 days after each sitting. This waiting period is applied after each attempt, regardless of whether candidates completed the assessment. "Sitting for the assessment" occurs when candidates log on to the testing workstation. Candidates have a limit of a total of 8 sittings (or attempts) per single certification or credential.

## SCORING

Candidates must earn a score equal to, or higher than, the cut score to pass the assessment. Preliminary pass/fail results are provided on a printout once candidates complete their assessment and later in their DAU account history.

## FEEDBACK

After completing and submitting the assessment, candidates will receive a feedback report including two sections of information.

Section 1 provides information regarding the candidate's test performance compared to the Performance Threshold (i.e., passing score). Each score provided is a scaled score (100-800). A scaled score is the total number of correctly answered scored questions (raw score) converted into a consistent and standardized scale. For all SPēD assessments, the converted raw passing score is 650 on a scale of 100 to 800. Scaled scores are used to provide more meaningful information to candidates while maintaining consistency between assessment forms. As assessments evolve, scaled scores guarantee that the meaning of a score translates to the same level of performance no matter what form a candidate receives.

Section 2 provides information regarding how the candidate performed on the assessment topic areas compared to other candidates who have taken the assessment. Candidates are provided three indicators:

- The average topic area score received by individuals who failed the assessment
- The average topic area score received by individuals who passed the assessment
- The candidates' topic area score

These indicators also allow candidates to see which topic area(s) they performed well on, and which topic area(s) they can improve on. While this feedback may be helpful to candidates, it is suggested that candidates pursue

improvement in all topic areas since this comparative performance metric is not definitive and subject to change based on those who take the assessment.

### FEES ASSOCIATED

At this time, there are no fees associated with taking any SPēD or APC Program assessments.

### ASSESSMENT SECURITY AND CONFIDENTIALITY

SPēD and APC Program assessment questions and answers are not subject to public release.

To take the SFPC, SAPPC, SPIPIC, ISOC, PSC, SPSC, ATC, APC, or DPAPC assessments, candidates must sign a Nondisclosure Agreement (NDA), and therefore accept the terms and conditions for participating in the SPēD and/or APC Program. Candidates are not authorized to release any information about a SPēD or APC Program assessment to peers, supervisors, study groups, or anyone else. The call-out box to the right is an excerpt of the NDA, which explains to candidates their responsibilities to protect the integrity of the assessments.

> "By accessing and participating in the SPēD Program, you accept the responsibility to protect the integrity of these assessments by not disclosing, disseminating, copying, publishing, or transmitting any parts of the assessment in any form to any person without prior written consent of the DOD SPēD PMO."

SPēD and APC Program assessments are proctored and delivered in secured environments. These measures are in place to protect the integrity of a candidate's results, the SPēD Program, the APC Program, and to ensure consistent testing environments.

Except as described in this handbook, the personal information candidates provide and their assessment results are confidential and will not be disclosed without their written consent unless when necessary to comply with a compulsory, legally-authorized demand or court order of a court of competent jurisdiction. To allow DCSA to release personal or assessment information to a third party other than as described in this handbook, the candidate must authorize DCSA to do so in writing. Any such written authorization must state the specific information that may be released and specifically identify the third party to receive the information. Data gathered and distributed as part of assessment studies or reports will be aggregated and personal identifying information will be redacted.

Any feedback or questions about assessment content on the assessment must be directed to the SPēD PMO at dcsa.spedcert@mail.mil. All terms of the signed NDA apply to assessment-related discussion.

## AFTER THE ASSESSMENT

### CERTIFICATION AND CONFERRAL REVOCATION

DODM 3305.13 authorizes the USD(I&S) to accept and approve certification conferral recommendations made by the Director, DCSA. As the conferral official and upon recommendation from the Director, DCSA, the USD(I&S) is also the authority to revoke certification credentials.

### USING CERTIFICATION OR CREDENTIAL ACRONYMS

Security Professionals who possess a SPēD or APC Certification Program certification or credential may use the appropriate acronym designation (SFPC, SAPPC, SPIPC, ISOC, PSC, SPSC, ATC, APC and/or DPAPC) on business cards, resumes, and signature lines. Designations can only be used while holding an active certification or credential.

# DIGITAL CREDENTIALING

## PLATFORM

Credly is the platform for all digital certifications and credentials.

Log into (or create an account) Credly (https://www.credly.com/earner/earned).

## ACCEPTING A DIGITAL BADGE

After successfully passing and being conferred for a certification or credential, certificants will receive an email from Credly giving them access to their newly earned digital badge. Certificants should click the Accept button below the badge icon and they will be redirected to the Credly login page (URL). The certificant should then log in or create a Credly account to claim the digital badge. Once a certificant claims their digital badge, they will have the option to make it viewable to the public or keep it private.

## SHARING A DIGITAL BADGE

Once certificants have accepted and claimed their digital badge, they will be redirected to the Share Badge screen. From here, they can share their digital badge from Credly to their social media platforms (e.g., LinkedIn, Twitter, Facebook, etc.) and via email. Certificants can also download the badge visual, a free printable badge, and embed their digital badge on a personal website.

## PRINTING A DIGITAL BADGE

**Free Printing Option:**

1. Log into Credly (https://www.credly.com/earner/earned).
2. Certificants will be redirected to the Share your badge page after receiving and accepting a digital badge. From here, certificants will have the option to share their badge directly from the Credly platform to various social media platforms and print earned certification and credential certificate(s) for free.
3. On the Share your badge page, certificants will see the print icon located on the far right. Clicking the print icon allows certificants to download and print certification and credential certificates.
4. Certificants may also select the certification or credential digital badge that they earned and then select the Share button to view their sharing and printing options.

**For Purchase Option**:
Certificants have the option to purchase a printed copy of their certification or credential certificate through American Registry, a third-party vendor. To purchase a certificate, complete the following steps:

1. Log into Credly (https://www.credly.com/earner/earned).
2. After receiving a digital badge on the Credly platform, click the Recommendation's link on the digital badge metadata page.
3. You will be redirected to the American Registry (http://www.americanregistry.com/dcsa) login page. From this page, you select which digital badge you would like to purchase a printed certificate for.
4. After the first visit to the American Registry website, you will be given a unique URL to directly order future earned badges. All future earned badges can be ordered by using this unique URL or following the above steps again.

## GOVERNMENT AND PERSONAL EMAIL ADDRESSES

Certificants should ensure both government and personal emails are linked to your Credly account to receive all digital credentials within a DAU account. To link emails:

1. Sign into Credly (https://www.credly.com/earner/earned) and update your email address by selecting the "Settings" tab located on the navigation bar.
2. On the left-hand navigation panel, click "Account."
3. Under "Email Addresses," select "Add an email address."
4. Insert government and/or personal email and click "Add."
5. You will then receive an email verification from Credly's platform.

### MERGE ACCOUNTS

If a certificant has a digital credential linked to separate accounts, both accounts must be merged to view digital credentials in a single account. To merge accounts:

1. Sign into Credly (https://www.credly.com/earner/earned) and update your email address by selecting the "Settings" tab located on the navigation bar.
2. On the left-hand navigation panel, click "Account."
3. Under "Merge Accounts," select "Merge an account."
4. Insert government or personal email address and password of the account you would like to merge and click "Next."
5. You will receive an activation code from Credly.
6. Insert the activation code to make sure accounts have merged successfully. If at any time you have further questions or are experiencing issues with your Credly account, visit the Credly Help Center (https://support.credly.com/hc/en-us).

## MAINTAINING YOUR CERTIFICATION AND CREDENTIAL

### CERTIFICATION RENEWAL PROGRAM

Obtaining a certification or credential is a significant achievement in a candidate's career. A certification or credential indicates the certificant possesses the knowledge and skills associated with the competencies necessary to successfully carry out DOD-defined security functional tasks.

The DOD has a professionalization goal of establishing a systematic approach for fostering learning and professional growth of the security workforce. Certification renewal is the long-term strategy for meeting this goal.

This approach allows the DOD, DSTC, the ACGB and DCSA to meet both National Intelligence Strategy (NIS) Enterprise Objective (EO) 6 and USD(I&S) Human Capital Goals and Objectives for the security workforce. NIS EO 6 focuses on developing the workforce and strives to "attract, develop, and retain a diverse, results-focused, and high-performing workforce capable of providing the technical expertise and exceptional leadership necessary to address our Nation's security challenges."

The Certification Renewal Program (https://www.cdse.edu/Certification/Certification-Maintenance/) supports certificants' ongoing educational and professional development. The PDU requirement provides opportunity for certificants to enhance job-related skills and knowledge, as well as become familiar with new regulations and technological advances in related security areas to meet security objectives.

Upon submission of your CRP please email the SPēD PMO office at dcsa.quantico.cdse.mbx.spedcert@mail.mil in order to ensure timely processing of your renewal. All submitted CRPs are subject to audit and review by SPēD PMO personnel at any time within the two-year renewal period. These audits assist in the compliance verification and integrity of certification maintenance standards as described below.

The SPēD PMO retains authority for all final determinations regarding submitted Certification Renewal Packages (CRPs) and the disposition of renewal approvals. Certificants may submit an appeal regarding dispositions of determinations made by SpēD PMO via an appeal form sent to dsca.spedcert@mail.mil consistent with the appeals process and procedures described below in this handbook.

The purpose of the Certification Renewal Program is to:

- Enhance continuing subject matter competence
- Recognize and encourage learning opportunities
- Maintain and grow mastery-level knowledge of critical security skills
- Offer a standardized and objective mechanism for obtaining and recording professional development activities
- Sustain the global recognition and value of SPēD certifications and credentials

## CERTIFICATION MAINTENANCE STANDARDS

1. The SPēD PMO manages the certification maintenance program. In accordance with the authority of DODI 3305.13, "DoD Security Education, Training, and Certification" and DODM 3305.13, "DoD Security Accreditation and Certification", these policies require a certification and credential holder to:

   a. Maintain a certification by:

      - Maintaining an active and up-to-date DAU account
      - Successfully acquiring at least 100 PDUs within their two-year certification maintenance period

   b. Maintain the ATC and ISOC by:

      - Maintaining an active and up-to-date DAU account
      - Successfully acquiring at least 75 PDUs within their two-year certification maintenance period

   c. Coordinate waiver review and validation with employing Component, agency, or company to request a reasonable extension for reasons that could prohibit a certification holder from meeting certification maintenance requirements (e.g., deployments, hospitalization/medical leave, or other extraordinary reasons). Individuals in industry, without a CSR, must send their waiver request directly to the SPēD PMO for final determination.

      - There will be no waivers submitted, accepted, or approved after expiration.

   d. Meet the certification holder's two-year certification maintenance requirements or all earned SPēD and APC certifications and credentials will expire, resulting in the loss of all rights and privileges that come with holding a SPēD and/or APC certifications and credentials. Certification and credential holders whose certification(s) and/or credentials have expired must re-establish each certification and/or credential by testing and being conferred to meet all certification and/or credential maintenance requirements.

2. Certification expiration dates are based on the initial conferral date or date of latest CRP submission and approval.

   a. Upon conferral of a new SPēD or APC certification (not credential) submission, and approval of the CRP, the new expiration date will update for all currently held certifications and credentials selected during the renewal process to the date of the most recently conferred certification.

b. Upon submission and approval of CRPs, the new expiration date will align across all held certifications and credentials and will expire two years from date of CRP approval.

c. The certificant must submit a single CRP to capture all PDUs (each category of PDU being claimed must have separate and independent supporting documentation) and select which certifications/credentials they are renewing. Only currently conferred certifications and credentials will be identified on the form as renewable.

   - At least 100 PDUs are required for renewal of the following certifications: SFPC, SAPPC, SPIPC, PSC, and APC.
   - At least 75 PDUs are required for renewal of the following credentials: ISOC, SPSC, DPAPC, and ATC.
   - SPSC and DPAPC are not standalone credentials and can only be renewed once the prerequisite certification (either SFPC or APC) has met the 100-PDU threshold.

d. At least 50 of the 100 PDUs must be security related. The remaining PDUs do not have to be aligned with security; however, they must satisfy one or more of the professional development categories identified in the PDU table on page 41.

e. To maintain an active SPēD and/or APC certification or credential, a certification holder must, in conjunction with a valid CRP submission, do one of the following within their two-year certification maintenance period:

   - Obtain at least 100 PDUs through approved professional development activities
   - Obtain at least 75 PDUs through approved professional development activities (ATC and ISOC only)
   - Be conferred a new SPēD or APC certification
   - Be conferred a new SPēD or DPAPC credential (each valued at 75 PDUs) in conjunction with 25 additional PDUs (do not have to be security related)

Qualifying Professional Development Activities: To accrue PDUs, a certification holder must participate in and successfully complete professional development activities that fall under one or more of the approved professional development categories (listed on the next page).

*Additional details about category requirements and specific PDU supporting documentation needed are available in the Certification Maintenance Guidelines at: https://www.cdse.edu/Portals/124/Documents/certification/sped program-certification-maintenance-guidelines.pdf?ver=7bL3shje1RYHiWf6XasVlQ%3d%3d.*

## Professional Development Unit (PDU) Categories

| Category 1: Complete a Certification or Credential Program | |
|---|---|
| Category 1a: Obtain a new SPēD or APC Certification | • Certificants can receive 100 PDUs for being conferred a new SPēD certification during their two-year certification maintenance cycle |
| Category 1b: Obtain a SPēD Credential or the DPAPC | • Certificants can receive 75 PDUs for being conferred a new SPēD credential or the DPAPC (credential) during their two-year certification maintenance cycle |
| Category 1c: Obtain a non-SPēD Certification | • Certificants can claim credit for up to 50 PDUs for each non-SPēD certification. All certifications must be security focused, nationally accredited, and gained during their two-year certification maintenance cycle<br>• A copy of the certificate must be uploaded as supporting documentation to receive PDUs in this category |

| Category 2: Security-related Training, Certificate Programs, and/or Higher Education | |
|---|---|
| Category 2a: Security-related eLearning training courses | Consists of an organized series of planned learning experiences developed and delivered in an eLearning environment, to assist participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area<br>• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training)<br>• Awards a certificate of completion<br>• Certificants can receive 1 PDU for each hour associated with an approved non-credit bearing training (all minutes past a full hour are rounded up to the next whole number. For example: anything under an hour rounds up to 1, 1 hour + 15 mins/1hour + 30 mins/1 hour + 45 mins are all rounded up to 2)<br>• Certificants can claim credit for up to 100 PDUs in this category<br>• Annual training can only be used once per each 2-year maintenance renewal window<br>• A certificate of completion must be uploaded to receive PDUs in this category |
| Category 2b: Security-related instructor-led or virtually-led training courses | Consists of an organized series of planned learning experiences developed and delivered either in person or virtually led, to assist participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area<br>• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training)<br>• Awards a certificate of completion<br>• Certificants can receive 10 PDUs for each full-day (4 or more hours) for each day of instruction, or 5 PDUs for each half-day (1-4 hours) associated with an approved non-credit bearing training course<br>• Certificants can claim credit for up to 100 PDUs in this category<br>• A certificate of completion must be uploaded to receive PDUs in this category |
| Category 2c: Security-related Higher Education | A college or university security-related, credit-bearing course (to include educational courses delivered by CDSE) that:<br>• Consists of an organized series of planned learning experiences (eLearning, instructor-led, instructor-facilitated online, self-paced, etc.) designed and developed to aid participants in acquiring knowledge, skills, and/or competencies associated with a coherent body of study within a discipline or set of related disciplines<br>• Is delivered by a nationally-accredited academic institution<br>• Results in academic credits granted and recognized by accredited academic institutions<br>• Certificants can receive 10 PDUs per week of an approved security-related, credit-bearing college or university course<br>• Certificants can claim credit up to 100 PDUs in this category<br>• A copy of supporting documentation, such as a transcript, indicating completion and length of the higher education course must be uploaded to receive PDUs in this category |

| Category 3: Non-Security related Training, Certificate Programs, and/or Higher Education | |
|---|---|
| Category 3a. Non-security related eLearning training courses | Consists of an organized series of planned learning experiences developed and delivered in an eLearning environment, to assist participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area<br>• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training)<br>• Awards a certificate of completion<br>• Certificants can receive 1 PDU for each hour associated with an approved non-credit bearing training (all minutes past a full hour are rounded up to the next whole number. For example: anything under an hour rounds up to 1, 1 hour + 15 mins/1 hour + 30 mins/1 hour + 45 mins are all rounded up to 2)<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A certificate of completion must be uploaded to receive PDUs in this category |
| Category 3b: Non-security related instructor-led or virtually-led training courses | Consists of an organized series of planned learning experiences developed and delivered either in person or virtually led, to assist participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area<br>• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training)<br>• Awards a certificate of completion<br>• Certificants can receive 10 PDUs for each full-day (4 or more hours) for each day of instruction, or 5 PDUs for each half-day (1-4 hours) associated with an approved non-credit bearing training course<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A certificate of completion must be uploaded to receive PDUs in this category |
| Category 3c: Non-security related Higher Education | A college or university non-security related, credit-bearing course that:<br>• Consists of an organized series of planned learning experiences (eLearning, instructor-led, instructor-facilitated online, self-paced, etc.) designed and developed to assist participants in acquiring knowledge, skills, and/or competencies associated with a coherent body of study within a discipline or set of related disciplines<br>• Is delivered by a nationally-accredited academic institution<br>• Results in academic credits granted and recognized by accredited academic institutions<br>• Certification holders can receive 10 PDUs per week of an approved non-security related, credit-bearing college or university course<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of supporting documentation, such as a transcript, indicating completion and length of the higher education course must be uploaded to receive PDUs in this category |

| Category 4: Attend Security Conferences | |
|---|---|
| Category 4a: Security Conference - Participant | A conference is an in-person or virtual meeting with main presenters to brief participants on a wide range of related issues/topics<br>Certification holders can receive up to 8 PDUs for each full day (i.e., 1 PDU per hour of the conference) of participation in an approved conference<br>• A maximum of 40 PDUs can be earned in a 5-day event<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of supporting documentation indicating certificant attended a conference (i.e., email confirmation of attendance following the conference or certificate of attendance) must be uploaded to receive PDUs in this category |
| Category 4b: Security Conference – Presenter | If a certificant presents at an approved conference, they can receive an additional 5 PDUs for each presentation<br>• A maximum of 25 PDUs can be earned for presenting at one event<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of supporting documentation indicating certification holders presented at a conference (i.e., email confirmation as a speaker, verification from the conference organizer, or copy of conference agenda with the certificant's name listed as a presenter) must be uploaded to receive PDUs in this category |
| **Category 5: Security-Related Projects** | |
| Category 5a: SPēD Certification Projects | Certificants may receive PDUs for successfully completing short-term certification projects (i.e., subject matter expert (SME) work on item development or certification preparatory tool or resource, participation in DSTC or ACGB working groups) that require application of security subject matter expertise.<br>*Participation in projects is voluntary in nature. PDUs cannot be accrued for projects for which participation is inherently part of the participant's job and/or assigned duties.<br>• Certificants can receive 3 PDUs per contact hour for each separate and distinct project<br>• Certificants can receive 2 PDUs for each completed homework assignment for each separate and distinct project<br>• A maximum of 50 PDUs can be earned in this category for each SPēD certification project<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of the SPēD PMO endorsed letter (PDF) outlining PDUs awarded for each project effort must be uploaded to receive PDUs in this category |
| Category 5b: Non-SPēD Security-Related Projects | Certificants may receive PDUs for successfully completing short-term non-SPēD security-related projects that require application of security subject matter expertise.<br>**Participation in projects is voluntary in nature. PDUs cannot be accrued for projects for which participation is inherently part of the participant's job and/or assigned duties.*<br>• Certificants can receive 3 PDUs per contact hour for each separate and distinct project<br>• Certificants can receive 2 PDUs for each completed homework assignment for each separate and distinct project<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of an endorsed letter (PDF) by the project champion, outlining overall contact hours and any completed homework assignments for each project effort, must be uploaded to receive PDUs in this category. NOTE: PDU hours are determined by the formula stated above and are not determined by the project champion. |

| Category 6: Other Voluntary Professionalization Activities | |
|---|---|
| Category 6: Other Voluntary Professionalization Activities | Certificants can receive PDUs for involvement in verifiable professional development, whether security related or not.<br>Examples of professional development activities include, but are not limited to: Leadership Development, Professional Advisory Boards, and career services.<br>• Certificants can receive two PDUs per contact hour for each separate and distinct professionalization activity associated with the professional development experience<br>• A maximum of 50 PDUs can be earned in this category for each professionalization activity<br>• Certificants can claim credit for up to 50 PDUs in this category<br>• A copy of supporting documentation indicating certificants participated in the project (i.e., email confirmation or official letter of program/activity completion and associated hours of effort) must be uploaded to receive PDUs in this category |

### FAILING TO MAINTAIN CERTIFICATIONS AND CREDENTIALS

Failure to obtain the required PDUs within the two-year certification maintenance cycle or failure to submit the CRP will result in a certification status deemed as non-compliant and all SPēDor APC certifications and credentials will expire.

## APPEALS PROCESS AND PROCEDURES

### GROUNDS FOR APPEAL

The SPēD and APC Program appeals policy governs the process for reviewing decisions made about registration, eligibility, assessments, and other certification issues.

**Appeals may be filed challenging the following:**

- Examination results
- Candidate registration
- Test-taking protocols
- Eligibility decisions related to alleged cheating, alleged violation of professional rules of conduct or the law, or inaccurate information on the application
- Certification maintenance and PDUs
- Certification disciplinary matters

### DECISIONS NOT ELIGIBLE FOR APPEAL

Matters not described in the Grounds for Appeal section are not within the purview of the SPēD and APC Program and are not appealable, such as the following DOD Component decisions:

- Employment policy
- Eligibility criteria for identifying billets or individuals for SPēD certifications
- DOD Component affiliation

Certificants can contact their CSR with questions or appeals of decisions outside the purview of the SPēD PMO.

## APPEAL SUBMISSION

Certificants have up to 90 calendar days from the date of receiving an appealable decision or after completing their assessment, whichever occurs first, to submit an appeal. All appeals must use the Appeal Request Form (https://www.cdse.edu/Portals/124/Documents/certification/appeals_form.pdf) and be sent to the SPēD PMO at dsca.spedcert@mail.mil.

## APPEAL REVIEW

The SPēD PMO conducts a preliminary review of all appeals within 15 duty days of receipt to make certain the appeal is timely, contains all required and pertinent information, and is based on allowable grounds.

- If a candidate's appeal is not received within the 90-day window, or is not based on allowable grounds, their appeal will be dismissed without referral to the Certification Appeals Board, and their PMO will be notified in writing of the dismissal.
- If a candidate's appeal package does not contain all required and pertinent information, they will be notified and given the opportunity to resubmit an appeals package within the 90-calendar day window.

Allowable appeals are forwarded to the Certification Appeals Board for a decision on the appeal.

Appeals may be filed challenging the following:

| Appeals Type | Examples of Allowable Appeals | Examples of Non-Allowable Appeals |
|---|---|---|
| Examination Results | Candidate requests verification that examination score was accurately recorded and calculated. | Candidate challenges content and/or validity of examination questions, scenarios, and/or answer options.<br>Candidate challenges method used for examination cut-score. |
| Candidate Registration | N/A | N/A |
| Test-taking Protocols | Candidate has a valid documented complaint associated with incident(s) at testing center. | Candidate challenges time allowed to complete examination. |
| Eligibility decisions related to inaccurate information on the application form or alleged cheating or alleged violation of professional rules of conduct or the law. | Candidate appeals eligibility denial based on alleged cheating, inaccurate information on the application form, or violation of professional rules of conduct or the law. | N/A |
| Certification maintenance and PDUs | Candidate appeals number of PDU credits awarded to activities. | Candidate improperly uses Certification Renewal Package (CRP).<br>Candidate is unable to verify submission of CRP.<br>Candidate does not maintain their DAU account in accordance with instructions in DOD Certification and Credentialing Handbook.<br>Candidate challenges two-year renewal time frame. |
| Certification disciplinary matters | Candidate appeals determination made by Certification Discipline Board. | N/A |

### APPEAL DECISION AND NOTIFICATION

Certification Appeals Board decisions are made by majority vote. The Certification Appeals Board will provide its decision to the candidate's CSR, the candidate, and the SPēD PMO. The Certification Appeals Board is the final decision authority and there are no further appeals.

### APPEAL WITHDRAWAL

Candidates may withdraw an appeal claim at any time before a Certification Appeals Board decision. Candidates must do so in writing to the SPēD PMO.

## WAIVER PROCESS AND PROCEDURES

### CIRCUMSTANCES FOR WAIVER

Certification waiver decisions are determined by the Component issuing or rejecting the waiver, and are not appealable to the SPēD PMO Candidates may request a waiver for an extension to their certification expiration date due to reasons such as deployment, hospitalization/medical leave, and other extraordinary reasons prohibiting an individual from meeting SPēD certification and credential maintenance requirements. There will be no waivers submitted, accepted, or approved after expiration.

### WAIVER REQUEST SUBMISSION

All waiver requests must use the Waiver Request Form (https://www.cdse.edu/Portals/124/Documents/certification/waiver_form.pdf?ver=rkSsN3zJLX7HKWPsc7oVSg%3d%3d) and be sent to the candidate's appropriate authority.

- If candidates are an employee or contractor for the DOD or one of its Components, agencies, or companies, submit the Waiver Request Form to their CSR.
- If candidates are an employee or contractor for DCSA, Industry, or other participating agency without a CSR, submit the Waiver Request Form to the SPēD PMO at dcsa.spedcert@mail.mil.

### WAIVER DECISION AND NOTIFICATION

Candidates will receive notification of their waiver decision within 10 duty days of receipt of their waiver request by the appropriate authority.

### APPROVED WAIVERS TIME FRAME

The amount of time permitted for approved waivers is determined by the specific circumstance. No waiver will exceed 180 days.

# GLOSSARY

### ADJUDICATOR CERTIFICATION GOVERNANCE BOARD
The authority for the governance and policy for the APC Program rests with the USD(I&S). The ACGB serves as an advisory group for the USD(I&S). The ACGB is the sole authority for the APC Program and represents the interests of all parties concerned with the certification program design, management, and maintenance. The ACGB serves as the ultimate decision-making body for certification policy coordination and oversight of the APC Program.

### APPLICANT
An individual with an established and up-to-date DAU account is eligible to take a SPēD or APC Program assessment.

### CANDIDATE
An individual scheduled to take an APC Program or SPēD assessment.

### CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
The nationally-accredited, award-winning directorate within DCSA providing security education, training, and certification products and services to a broad audience supporting the protection of national security and professionalization of the DOD security enterprise.

### CERTIFICANT
An individual who fulfilled conditions outlined in the policy matrix for certification and conferred by the USD(I&S).

### CERTIFICATION RENEWAL PACKAGE
An online tool to record PDUs earned during a two-year certification maintenance and renewal cycle.

### COMPETENCY PREPARATORY TOOLS (CPTs)
CPTs are references that are aligned with the DOD Security Skill Standards (DS3) and the Defense Security Essential Body of Knowledge (D-SEBOK), which is the DOD security community's expectations of what security professionals need to know to perform various aspects of their jobs. CPTs indicate what may be covered by an assessment, but it cannot be assumed that every topic will be on the assessment.

### DOD SECURITY SKILL STANDARDS
Establishes DOD expectations of what security professionals must know and successfully perform to support DOD security functions relative to each SPēD Program certification or credential. DOD Security Skill Standards also provide certification blueprints specifying objectives associated with the knowledge and skill topics and sub-topics measured by each assessment.

### ELIGIBLE APPLICANT
An individual eligible to apply to take a SPēD or APC Program assessment after gaining approval from their employing agency or the SPēD PMO.

### FOURTH ESTATE
Components of the United States DOD that are not considered to be affiliated with armed services, Intelligence Community (IC) agencies, or Combatant Commands (CCMD), to include the defense agencies and other DOD field activities.

## DEFENSE ACQUISITION UNIVERSITY

The system of record for the SPēD and APC Program and the gateway to testing and managing a certification and/or credential. An applicant's DAU account must be active and up to date to register for or maintain certifications and credentials (https://dau.csod.com/).

## NATIONAL COMMISSION FOR CERTIFYING AGENCIES

The Commission responsible for reviewing professional certification programs and determining whether they meet certification standards for program development, implementation, and maintenance while guaranteeing health, welfare, and safety of the public. Commission reviews programs to determine whether their practices are consistent with the Standards for the Accreditation of Certification Programs.

## PROFESSIONAL DEVELOPMENT UNITS

Professional development activities falling under approved professional development categories. A certification holder is responsible for obtaining 100 PDUs before the end of their two-year maintenance cycle. At least 50 of the 100 PDUs must be acquired through approved security-related professional development activities.

## SECURITY TRAINING, EDUCATION, AND PROFESSIONALIZATION PORTAL

STEPP is the learning management system where DOD employees are able to access the CDSE course catalog and view their course transcripts. These courses are intended for use by DOD and other U.S. Government personnel and contractors within the National Industrial Security Program. (https://cdse.usalearning.gov/login/index.php).

## SPĒD PROGRAM MANAGEMENT OFFICE

Establishes and implements policies and procedures to manage and support the SPēD and APC Program, including the application process, certification and credential assessments and testing protocols, candidate record retention, the DS3, and national accreditation through the NCCA. The SPēD PMO acts as the CSR for Industry, contractors (such as Facility Security Officers), as well as for agencies that do not have a CSR in the SPēD or APC programs.

# ACRONYMS

| | |
|---|---|
| **AAA** | Access Approval Authority |
| **ACGB** | Adjudicator Certification Governance Board |
| **ADA** | Americans with Disabilities Act |
| **APC** | Adjudicator Professional Certification |
| **AT** | Antiterrorism |
| **ATC** | Antiterrorism Credential |
| **ATO** | Antiterrorism Officer |
| **CDSE** | Center for Development of Security Excellence |
| **CPT** | Competency Preparatory Tool |
| **CRP** | Certification Renewal Package |
| **CSR** | Component Service Representative |
| **DAU** | Defense Acquisition University |
| **DCSA** | Defense Counterintelligence and Security Agency |
| **DCSA AVS** | DCSA Adjudication and Vetting Services |
| **DHRA** | Defense Human Resources Activity |
| **DIA** | Defense Intelligence Agency |
| **DOD** | Department of Defense |
| **DOD IC** | DOD Intelligence Community |
| **DODI** | DOD Instruction |
| **DODM** | DOD Manual |
| **DOHA** | Defense Office of Hearings and Appeals |
| **DPAPC** | Due Process Adjudicator Professional Credential |
| **DS3** | DOD Security Skill Standards |
| **DSTC** | DOD Security Training Council |
| **EO** | Enterprise Objective |
| **FOCI** | Foreign Ownership, Control, or Influence |
| **FS** | File Series |
| **FSO** | Facility Security Officer |
| **IC** | Intelligence Community |
| **IS** | Information Security |
| **ISOC** | Industrial Security Oversight Credential |
| **IT** | Information Technology |
| **NCCA** | National Commission for Certifying Agencies |
| **NDA** | Nondisclosure Agreement |
| **NGA** | National Geospatial-Intelligence Agency |
| **NID** | National Interest Determination |
| **NIS** | National Intelligence Strategy |
| **NISP** | National Industrial Security Program |
| **NSA** | National Security Agency |
| **OPSEC** | Operations Security |
| **OUSD(I&S)** | Office of the Under Secretary of Defense for Intelligence and Security |
| **PDA** | Personal Digital Assistant |
| **PDU** | Professional Development Unit |
| **PMO** | Program Management Office |
| **PPB&E** | Planning, Programming, Budgeting, and Execution |

| | |
|---|---|
| **PSC** | Physical Security Certification |
| **PSP** | Personnel Security Program |
| **RMF** | Risk Management Framework |
| **SAPPC** | Security Asset Protection Professional Certification |
| **SAP** | Special Access Program |
| **SAPCO** | SAP Central Office |
| **SAPF** | SAP Facility |
| **SAPNP** | SAP Nomination Process |
| **SCI** | Sensitive Compartmented Information |
| **SFPC** | Security Fundamentals Professional Certification |
| **SME** | Subject Matter Expert |
| **SPēD** | Security Professional Education Development |
| **SPIPC** | Security Program Integration Professional Certification |
| **SPSC** | Special Program Security Credential |
| **STEPP** | Security Training, Education, and Professionalization Portal |
| **TPI** | Two-Person Integrity |
| **USD(AT&L)** | Under Secretary of Defense for Acquisition, Technology, and Logistics |
| **USD(I&S)** | Under Secretary of Defense for Intelligence and Security |
| **SOR** | Statement of Reasons |