PARALLAX CYBER ACADEMY

parallax-cyber.com

Space Systems Security Engineering Professional (S3EP)©

Certification Program Candidate Handbook

Edition: 8 May 2026

Questions: certifications@parallax-cyber.com

This handbook is reviewed and updated annually and upon significant changes.

TABLE OF CONTENTS

SECTION 1 — PROGRAM INTRODUCTION

1. Program Introduction

1.1 Mission Statement

The Parallax Cyber Academy (PCA) Space Systems Security Engineering Professional (S3EP)© Certification Program exists to identify, recognize, and develop professionals who possess verified knowledge, skills, and experience in the cybersecurity of space systems. The program advances national and international security by ensuring that a qualified, credentialed workforce is available to protect the space systems upon which modern society increasingly depends.

1.2 About Parallax Cyber Academy

Parallax Cyber Academy is the credentialing arm of Parallax Cyber, LLC, a specialized branch focused on the intersection of space operations and cybersecurity. The Academy delivers training courses, administers the S3EP certification examinations, and maintains the active registry of certified professionals. The Academy is committed to the highest standards of integrity, fairness, and professional excellence in all certification activities.

1.3 Program Governance

The S3EP program is governed by the PCA Certification Council (the "Council"), composed of senior subject-matter experts, industry practitioners, and an independent public representative. The Council is responsible for:

- Setting and updating certification requirements, exam content, and CPE policies
- Adjudicating appeals, ethics complaints, and credentialing disputes
- Ensuring the program remains aligned with industry standards and workforce needs
- Reviewing this Candidate Handbook and approving revisions on at least an annual basis

Day-to-day administration of the program is conducted by the PCA Certifications Team, reachable at certifications@parallax-cyber.com.

1.4 Industry Alignment

Industry Practice Reference: The S3EP program is designed in alignment with ISO/IEC 17024:2012, the international standard for bodies operating certification of persons, and draws on best practices established by leading certification bodies including (ISC)², ISACA, CompTIA, and EC-Council. Specifically, the CPE maintenance model, ethics framework, and appeals structure described in this handbook are modeled on those established by (ISC)² for its CISSP® credential — widely recognized as the gold standard for professional cybersecurity certification.

NOTE	Completion of PCA-certified courses and the S3EP certification examination demonstrates domain-specific competence in space cybersecurity. The S3EP credential is not a substitute for required government or regulatory clearances, licenses, or occupational authorizations.

1.5 Non-Discrimination and Equal Opportunity Statement

Parallax Cyber Academy is committed to providing equal opportunity in all aspects of its certification program. Certification opportunities are available to all qualified individuals without regard to race, color, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, veteran status, genetic information, marital status, or any other characteristic protected under applicable federal, state, or local law.

All certification decisions are made solely on the basis of meeting the documented requirements described in this handbook. Any individual who believes they have been subjected to discriminatory treatment in connection with the S3EP program may file a complaint in writing to certifications@parallax-cyber.com. Complaints will be reviewed by the PCA Certification Council.

1.6 Privacy and Data Protection

Scope. This section describes how Parallax Cyber Academy collects, uses, stores, and shares personal information submitted in connection with the S3EP certification program. Parallax Cyber, LLC is a U.S.-based entity and handles personal information in accordance with applicable U.S. federal and state law, including but not limited to the California Consumer Privacy Act (CCPA), where applicable, and relevant sector-specific privacy requirements.

Information We Collect. PCA collects personal information necessary to administer the certification program, including: full legal name; contact information (email, phone, mailing address); employment history and job titles; educational credentials and transcripts (where submitted); names and contact information of professional references; exam performance data; CPE submission records; and payment transaction records through a compliant payment vendor.

How We Use Your Information. Personal information is used exclusively to: process and evaluate certification applications; schedule and administer examinations; verify eligibility and references; issue and maintain certification records; process payments and annual maintenance fees; communicate program updates and renewal reminders; and conduct CPE audits.

Sharing with Partners. Parallax Cyber Academy may share applicant and candidate information with authorized third-party partners to support the implementation and continuous improvement of the certification program. Such partners include: (a) exam delivery and remote proctoring service providers, who receive candidate identification and scheduling information necessary to administer secure examinations; (b) PCA-Certified Training Vendors, who may receive confirmation of course completion status for credentialing verification purposes; (c) professional reference contacts, who are contacted by PCA to verify stated experience; and (d) technology service providers supporting

the certification registry, CPE tracking portal, and digital badge issuance. All partners are contractually required to handle personal information in accordance with applicable law and to use it solely for the purposes for which it was shared. PCA does not sell personal information to third parties.

Retention. Certification records, including examination results and CPE submissions, are retained for a minimum of seven (7) years following expiration or revocation of a certification. Application records for applicants who did not achieve certification are retained for three (3) years.

Your Rights. Individuals may request access to, correction of, or deletion of their personal information by submitting a written request to certifications@parallax-cyber.com. PCA will respond to verified requests within forty-five (45) calendar days. Deletion requests may be subject to legal retention requirements and may affect the ability to verify certification status.

Security. PCA employs reasonable administrative, technical, and physical safeguards to protect personal information from unauthorized access, use, or disclosure. Examination data is transmitted over encrypted channels and stored in access-controlled systems.

SECTION 2 — CERTIFICATION LEVELS & REQUIREMENTS

2. Certification Levels and Requirements

2.1 Overview of the S3EP Credential Family

The S3EP program provides a progressive five-tier credentialing pathway that reflects advancing levels of knowledge, practical experience, and professional leadership. Each level builds upon the previous, creating a transparent career development framework for space cybersecurity professionals.

Certification	Exam Required	PCA Courses (or PCA-Certified Vendor)	Experience	Annual CPEs
Associate Space Systems Security Engineering Professional (AS3EP)©	Basic Space Systems Security Engineering Exam	Securing Space Systems from Cyber Attacks©	None	10
Deputy Space Segment Systems Security Engineering Professional (DSS3EP)©	Basic Space Systems Security Engineering Exam	Securing Space Systems from Cyber Attacks© + Defending and Attacking Space Systems in Cyberspace©	2 years	20
Deputy Ground Segment Systems Security Engineering Professional (DGS3EP)©	Basic Space Systems Security Engineering Exam	Securing Space Systems from Cyber Attacks© + Defending and Attacking Space Systems in Cyberspace©	2 years	20
Certified Space Systems Security Engineering Professional (CS3EP)©	Advanced Space Systems Security Engineering Exam	Previous + Engineering Secure Space Systems©	5 years	30
Expert Space Systems Security Engineering Professional (ES3EP)©	Advanced Space Systems Security Engineering Exam	Previous + Engineering Secure Space Systems©	8 years	40

NOTE	Academic equivalency may be substituted for experience requirements during the application process. See Section 2.4 for details. An annual service fee is required to maintain certification. CPE credits are due 60 days before the anniversary of certification award.

2.2 Certification Descriptions

AS3EP© — Associate Level

The entry-level S3EP credential is designed for students, early-career professionals, and individuals transitioning into space cybersecurity from adjacent fields. No prior experience in a space or cybersecurity role is required; successful completion of a PCA-hosted course or a PCA-certified vendor foundational course and the Basic Exam.

DSS3EP© — Deputy Space Segment

Designed for professionals with demonstrated experience in the engineering, operation, or security of space segment systems (satellite bus, payload, on-board software, launch operations). Holders have completed both foundational and intermediate courses and can apply engineering principles to satellite cybersecurity challenges.

DGS3EP© — Deputy Ground Segment

Designed for professionals with experience in ground segment systems—including mission operations centers, ground stations, command and telemetry systems, and data processing infrastructure. Holders have completed both foundational and intermediate courses and can apply engineering principles to ground station cybersecurity challenges, recognize the distinct technical domain of ground segment security.

CS3EP© — Certified Level

A practitioner-level credential for experienced professionals who design, implement, assess, or manage cybersecurity across integrated space systems. Requires five years of qualifying experience and passing an advanced exam. Completion of advanced PCA courses or certified vendor courses, including advanced offensive/defensive courses, support exam readiness.

ES3EP© — Expert Level

The highest S3EP credential, is reserved for senior professionals with eight or more years of qualifying experience who demonstrate mastery across the full technical and leadership domains of space cybersecurity by passing the advanced exam. Expert holders are expected to contribute to the profession through research, publication, mentorship, or standards development, reflected in the increased CPE requirement. Completion of advanced PCA courses or certified vendor courses, including advanced offensive/defensive courses, support exam readiness.

2.3 Eligible Experience — Definition and Qualifying Criteria

"Qualifying experience" for S3EP purposes means paid or unpaid professional work in which the primary responsibilities involve one or more of the following domains:

- Space systems engineering or architecture (satellite, launch vehicle, or ground segment)
- Cybersecurity of space systems, including threat analysis, vulnerability assessment, and incident response in space or ground segment environments
- Secure software development for space systems or embedded systems
- Systems security engineering applied to space systems (applying NIST SP 800-160 or equivalent)
- Mission assurance, risk management, or safety engineering for space programs
- Intelligence analysis, policy, or acquisition related to space systems security
- Academic research with demonstrated application to space cybersecurity (see Section 2.4)

Experience must be accrued after completion of secondary education. The following rules apply:

- Full-time employment: 1 year of experience = 12 months in a qualifying role at 35+ hours/week.
- Part-time employment: Pro-rated at actual hours versus a 40-hour baseline (e.g., 20 hours/week = 0.5 years per calendar year).
- Multiple overlapping roles: Experience may not be double-counted. Concurrent roles are counted once for the period of overlap.
- Contract and freelance work: Eligible when documented by a signed statement from the contracting entity or a qualified reference.
- Internships: May count toward experience if the work falls within qualifying domains and the internship was paid or academic credit-bearing.
- U.S. Military service: Active duty, reserve, or National Guard service in a space, cyber, or intelligence occupational specialty qualifies on a year-for-year basis.
- Government civilian service: Qualifying on the same basis as private sector employment.

INDUSTRY PRACTICE	The experience verification approach used by S3EP mirrors the endorsement and attestation model used by (ISC)² for the CISSP® credential, in which professional references attest to the accuracy of stated experience. References who provide false attestations are subject to removal from PCA-recognized reference status.

2.4 Academic Equivalency

Candidates who hold qualifying academic credentials may substitute academic achievement for up to a defined portion of the experience requirement as follows:

Academic Credential	Experience Substitution	Maximum Substitution
Master's degree in cybersecurity, computer science, electrical engineering, aerospace engineering, or closely related field from an accredited institution	1 year	1 year
Doctoral degree (Ph.D., D.Sc., etc.) in a qualifying field, with dissertation in a space or cybersecurity domain	2 years	2 years
Completion of a PCA-certified training course, fellowship, or advanced training program (as published on the PCA website)	6 months	6 months

Academic substitution does not reduce the requirement for any certification level below 1 year of qualifying experience (except AS3EP, which has no experience requirement). Applicants claiming academic equivalency must submit official or certified copies of transcripts with their application with Social Security Numbers obscured/redacted.

2.5 Recommended Courses

All S3EP certification levels are supported through completion of one or more PCA-certified courses. Courses may be completed through Parallax Cyber-sponsored offerings or through vendors on the PCA Certified Vendor List, published at parallax-cyber.com. Courses must be completed from a PCA-certified vendor to adequately prepare for the certification exam.

At the time of publishing, PCA-sponsored courses include:

- Securing Space Systems from Cyber Attacks© — Relevant to AS3EP. Covers the threat landscape, fundamental security principles, and policy frameworks for space systems.
- Defending and Attacking Space Systems in Cyberspace© — Relevant to DSS3EP, DGS3EP, CS3EP, and ES3EP. Covers defensive and offensive cybersecurity techniques and advanced defensive strategies for space systems.

- Engineering Secure Space Systems© — Relevant to CS3EP and ES3EP. Covers systems security engineering for satellite and ground segment environments.

Courses do not expire, but PCA reserves the right to recommend updated courses if the course content has been substantially revised and the prior completion is more than five (5) years old.

SECTION 3 — APPLICATION PROCESS

3. Application Process

3.1 Step-by-Step Application Instructions

1. Confirm eligibility: Review Section 2 to confirm you meet all course, experience, and any academic equivalency requirements for the desired certification level.
2. Download the application template: The current application template for each certification level is available at parallax-cyber.com or by request from certifications@parallax-cyber.com. Online instructions are kept current if anything changes.
3. Complete the application: Fill in all required fields, including: full legal name and contact information; desired certification level; list of completed courses with completion dates and vendor; employment history for all qualifying experience (dates, employer, role, description of qualifying duties); names and contact information for professional references; and any academic equivalency documentation.
4. Gather supporting documents: Assemble your current resume or CV; course completion certificates for all applicable courses; official or certified transcripts (if claiming academic equivalency); and reference contact information (at least one reference who can attest to the full period of qualifying experience stated, or more references as needed).
5. Submit your application: Email the completed application, resume/CV, and supporting documents to certifications@parallax-cyber.com with the subject line: "S3EP Application - [Your Full Name], [Certification Level]."
6. Pay the application fee: You will receive an invoice for the application processing fee within five (5) business days of submission. Applications are not reviewed until payment is received. Parallax Cyber leverages the Paypal platform which accepts Venmo, credit cards, and Paypal payments.
7. Await review: PCA will review your application and contact your references. See Section 3.4 for processing timelines.
8. Receive exam authorization: If your application is approved, you will receive an Exam Authorization Notice by email with instructions for scheduling your examination.

3.2 Required Documentation

Document	Requirements
Application Form	PCA template; all sections must be completed; incomplete applications will be returned without review
Resume / CV	Current; must reflect all experience claimed in the application; no length limit
Course Completion Certificates	One certificate per required course with course name, completion date, and vendor name

Document	Requirements
Transcripts (if claiming academic equivalency)	Official or certified copies; unofficial transcripts accepted for initial review but official copies required before certification is issued
Reference Contact Information	At least one reference familiar with the full period of qualifying experience; additional references may be required if the single reference cannot cover the entire period

3.3 Reference Requirements

References must be individuals who can attest from direct personal knowledge to the accuracy of the qualifying experience stated in your application. Acceptable references include:

- Current or former supervisors or managers
- Senior colleagues who directly observed the applicant's work in qualifying roles
- Government contracting officers or program managers (for contract work)
- Faculty advisors (for academic research experience only)

References may not be: immediate family members; individuals who have a direct financial interest in the applicant's certification; or current co-applicants for the same certification level.

PCA will contact references directly by email or phone. References will be asked to verify: dates of the applicant's service or employment, the nature of qualifying duties performed, and that the information provided in the application is accurate to the best of their knowledge. References who provide false attestations will be reported to appropriate professional bodies and removed from PCA's approved reference list.

3.4 Application Processing Timeline

PCA is committed to the following processing timelines, measured from receipt of a complete application package (all documents submitted and application fee paid):

Milestone	Standard Timeline	Complex Cases*
Initial completeness review	5 business days	5 business days
Reference contact and response collection	10 business days	15 business days
Application eligibility determination	15 business days	25 business days
Total (approved application to exam authorization)	20–25 business days	30–40 business days

*Complex cases include applications with experience spanning more than five employers; experience claimed in whole or in part through academic equivalency; applications where

references are unresponsive; or cases where the Certifications Team has additional questions about eligibility.

Applicants will be notified of approval, denial, or a request for additional information before the estimated deadline in the table above. If PCA requires additional information, the processing clock is paused until the requested information is received.

SECTION 4 — EXAMINATION

4. Examination

4.1 Exam Blueprints

S3EP Basic Exam (AS3EP, DSS3EP, DGS3EP)

The Basic Exam is a 60-question, multiple-choice, closed-book assessment covering the following domains. Candidates should expect a balanced distribution across all domains, with no single domain representing more than 30% of the total questions.

Domain	Approximate Weight	Question Count (~)
Space Systems Architecture and Engineering Fundamentals	20%	12
Cybersecurity Frameworks and Policy (NIST, NISPOM, ITAR)	20%	12
Space Segment Security (Satellite Bus, Payload, On-board Software)	20%	12
Ground Segment Security (Mission Operations, Ground Stations, Link Security)	20%	12
Threat Intelligence and Risk Management for Space Systems	20%	12
TOTAL	**100%**	**60**

S3EP Advanced Exam (CS3EP, ES3EP)

The Advanced Exam is a 100-question, multiple-choice, closed-book assessment. It tests deeper technical proficiency and includes scenario-based questions that require applied reasoning.

Domain	Approximate Weight	Question Count (~)
Advanced Space Systems Security Architecture & Engineering	20%	20
Offensive Techniques and Adversary Tradecraft in Space Cyber	20%	20
Defensive Operations and Incident Response for Space Systems	20%	20

Domain	Approximate Weight	Question Count (~)
Risk Management, Governance, and Compliance (Advanced)	15%	15
Emerging Threats and Technology (AI, quantum, supply chain)	15%	15
Leadership, Ethics, and Professional Practice	10%	10
TOTAL	**100%**	**100**

4.2 Passing Score

A scaled passing score of 70% is required for the Basic Exam and 72% for the Advanced Exam. Scores are reported as a scaled score on a range of 0–100. PCA reserves the right to apply minor statistical equating adjustments across exam forms to ensure fairness across administrations; the published passing threshold reflects the adjusted standard.

NOTE	Exam results are provided as Pass or Fail only. Specific item-level feedback is not provided to candidates in order to protect the integrity of exam content. A performance summary by domain is provided to candidates who do not pass, to guide remediation study.

4.3 Exam Delivery and Scheduling

S3EP examinations are administered in two formats:

- In-person (paper copy or online)
- Remotely using synchronous proctoring (online)

Exam schedules for the next 90 days are published on the PCA website and updated monthly. Candidates receive exam registration and testing instructions with their Exam Authorization Notice. In-person PCA courses include exam administration when conditions permit (for in-person participants).

4.4 Exam Conduct Rules

All S3EP exams are "closed book." The following are prohibited during the exam:

- Reference materials of any kind (notes, textbooks, online resources)
- Communication with any other person
- Use of artificial intelligence tools, search engines, or any external software assistance
- Recording or photographing the exam screen or content
- Leaving the monitored testing area without authorization

Violation of exam conduct rules will result in immediate exam termination, a score of zero for that attempt, and may result in a permanent bar from future S3EP examination participation. Suspected conduct violations are referred to the PCA Certification Council.

4.5 Exam Retake Policy

Industry Practice Reference: The retake policy imposes mandatory waiting periods and attempt limits to protect exam integrity and encourage adequate preparation between attempts.

Attempt	Policy
1st attempt (initial)	No waiting period; scheduled after Exam Authorization Notice is received
2nd attempt (1st retake)	Minimum 30-day waiting period after the failed attempt date; retake fee applies
3rd attempt (2nd retake)	Minimum 60-day waiting period after 2nd failed attempt; retake fee applies
4th+ attempts	Minimum 90-day waiting period between each subsequent attempt; retake fee applies; a new application is not required unless the original application has expired (2 years from approval date)

Retake exam fees are listed in Section 8 (Fee Schedule). Candidates who do not pass after four attempts within a 24-month period may petition the Certification Council for an extended eligibility period, stating steps taken to remediate knowledge gaps. Such petitions are submitted to certifications@parallax-cyber.com.

4.6 Testing Accommodations

Parallax Cyber Academy is committed to providing equal access to certification examinations for candidates with disabilities. Candidates who require testing accommodations due to a documented disability (as defined under the Americans with Disabilities Act, 42 U.S.C. § 12101 et seq.) may request accommodations by following the process below.

1. Submit a written accommodation request to certifications@parallax-cyber.com at least 21 calendar days before the desired exam date.
2. Include documentation from a licensed healthcare or rehabilitation professional describing: the nature of the disability; the functional limitations relevant to the exam environment; and the specific accommodations recommended.
3. PCA will review the request and documentation and respond within 10 business days with a decision and, if applicable, approved accommodation details.
4. If the request is denied in whole or in part, the candidate may appeal pursuant to Section 7 (Appeals Process).

Available accommodations may include, but are not limited to: extended exam time (typically 50% additional); screen reader compatibility; alternative text formats; a separate testing room; and additional breaks. Accommodations are determined on an individual basis.

SECTION 5 — CERTIFICATION AWARD & MAINTENANCE

5. Certification Award and Maintenance

5.1 Certificate Issuance

Candidates who pass the required examination and hold an approved application will receive their certification within 15 business days of confirmed exam passage. Certification documentation includes:

- A digital certificate of completion bearing the candidate's name, certification level, certification date, and a unique certification number
- A digital badge issued by PCA, suitable for display on LinkedIn, email signatures, and professional profiles. Badges include embedded metadata that allows employers and colleagues to verify authenticity by contacting PCA.
- Inclusion in the PCA Active Certification Registry, a public-facing lookup tool at parallax-cyber.com/verify that allows anyone to confirm a credential holder's name, certification level, and active/inactive status by name or certification number unless the participant selects to not be listed prior to completing the certification exam.

5.2 Certification Validity and Renewal

All S3EP certifications are valid for one (1) year from the date of issue. To maintain certification in active status, holders must, before each anniversary date:

1. Submit the required number of Continuing Professional Education (CPE) credits for their certification level (see Section 5.3).
2. Pay the annual maintenance fee (see Section 8).
3. Certify continued compliance with the S3EP Code of Ethics (see Section 6).

Submissions must be received by PCA no later than 60 calendar days before the anniversary date. A 30-day grace period applies for late submissions, subject to a late fee (see Section 8). Certifications not renewed within the grace period will be suspended. Certifications suspended for more than 180 days without resolution will be revoked.

5.3 Continuing Professional Education (CPE) Requirements

CPE credits are the mechanism by which S3EP holders demonstrate continued professional engagement and currency in the space cybersecurity field. The annual CPE requirements by certification level are:

Certification Level	Annual CPEs Required	3-Year Cumulative
AS3EP©	10	30
DSS3EP© / DGS3EP©	20	60
CS3EP©	30	90
ES3EP©	40	120

INDUSTRY PRACTICE The ES3EP annual CPE requirement of 40 credits is set higher than lower tiers to reflect the expectation that Expert-level holders contribute actively to the profession.

5.4 Eligible CPE Activities

Activity	Credit per Unit	Annual Max
Attending subject-related training courses or bootcamps	1 CPE per contact hour	No limit
Conference attendance (related technical sessions)	1 CPE per session hour	16 CPEs per event
Presenting at a professional conference or webinar	2 CPEs per hour of presentation	No limit
Completing space cybersecurity course (new, not previously completed)	1 CPE per contact hour	No limit
Publishing a technical article, blog post, or whitepaper (space/cyber domain)	5 CPEs each	10 CPEs
Contributing to a standards body, working group, or government advisory panel	1 CPE per meeting hour	20 CPEs
Mentoring a PCA candidate (formal, documented arrangement)	2 CPEs per month of active mentoring	10 CPEs
Self-study (reading technical books, completing online modules)	1 CPE per hour	25% of annual requirement

All CPE activities must relate to space systems, cybersecurity, information technology, or closely related professional domains. Activities must have occurred during the current certification year. Documentation for all CPEs must be retained by the holder for a minimum of two (2) years after submission and must be produced upon request during a CPE audit.

5.5 CPE Submission Process

1. Log CPE activities throughout the year using the PCA CPE Tracking Portal at parallax-cyber.com (login with your certification credentials).
2. For each CPE activity, record: activity title, provider/organizer, dates, number of hours/credits, and a brief description of relevance to the S3EP domain.
3. Upload supporting documentation (certificate, agenda, publication link, etc.) directly in the portal.
4. Submit your annual CPE report through the portal no later than 60 days before your certification anniversary date.

If you are unable to access the portal, email a completed CPE submission form (available on the PCA website) to certifications@parallax-cyber.com.

5.6 CPE Audits

PCA conducts random CPE audits of a sample of holders each year. All holders are subject to audit. If selected for audit, you will be notified by email and given 30 days to produce documentation supporting all CPE credits submitted. Failure to produce adequate documentation will result in disqualification of unsupported credits. If disqualified credits bring your total below the annual requirement, your certification will be suspended pending remediation. Holders who are found to have submitted fraudulent CPE claims are subject to revocation (see Section 5.8).

5.7 Consequences of Non-Renewal

Status	Condition and Consequence
Active	All renewal requirements met on time; certification listed as Active in the public registry
Grace Period	Submission received 1–30 days late; late fee applies; certification remains Active during this period
Suspended	Renewal not received within grace period; certification listed as Suspended; holder may not represent themselves as actively certified. May reinstate within 180 days by completing renewal requirements plus a reinstatement fee.
Revoked	Certification not reinstated within 180 days of suspension, OR revoked for cause (ethics violation, fraudulent application or CPE submission). Revoked certifications are permanently removed from Active status. Reinstatement requires re-application and re-examination.

5.8 Revocation for Cause

In addition to non-renewal, a certification may be revoked for cause upon a finding by the PCA Certification Council that a holder has:

- Violated the S3EP Code of Ethics (see Section 6)

- Submitted false or fraudulent information in a certification application or CPE submission
- Misrepresented certification status (e.g., claiming a higher level than held, claiming an expired certification is active)
- Committed a criminal act relevant to professional trust, including fraud, theft, or computer crimes

Revocation for cause is subject to the appeals process in Section 7. A holder under active investigation may be suspended pending the outcome of the Council's review.

SECTION 6 — CODE OF ETHICS & PROFESSIONAL CONDUCT

6. Code of Ethics and Professional Conduct

Industry Practice Reference: The S3EP Code of Ethics requires holders to act honorably, justly, responsibly, and legally. The S3EP Code is adapted to reflect the unique responsibilities of professionals operating in the national security-relevant domain of space systems cybersecurity.

6.1 The S3EP Professional Code of Ethics

All S3EP credential holders, upon achieving any level of certification, are required to uphold and be bound by the following Code of Ethics as a condition of certification issuance and maintenance. Failure to abide by this Code may result in investigation, suspension, or revocation of certification.

Preamble

> The safety and security of space systems is a matter of national and global importance. S3EP-certified professionals have achieved specialized knowledge of vulnerabilities in systems upon which critical infrastructure, national defense, and daily life increasingly depend. This places upon us an obligation that goes beyond technical competence — an obligation to act with integrity, to protect the public interest, and to uphold the trust placed in us by employers, clients, colleagues, and society at large.

Canon I — Protect Society and the Public Good

S3EP professionals shall place the safety and security of the public, critical infrastructure, and national interests above all other considerations. Professionals shall:

- Disclose known vulnerabilities in space systems through appropriate responsible disclosure channels rather than suppressing or exploiting them
- Decline to participate in activities that they know or have reason to believe will cause harm to the public or to critical space infrastructure
- Report credible threats to space system security to appropriate authorities when legally required or when public safety is at risk

Canon II — Act Honorably, Justly, and Responsibly

S3EP professionals shall conduct themselves with honesty and integrity in all professional activities. Professionals shall:

- Represent their credentials, experience, and expertise truthfully at all times
- Not misrepresent the status of their certification or claim a higher certification level than they currently hold

- Acknowledge mistakes and take responsibility for errors in their professional work
- Treat colleagues, clients, and the public with dignity and respect, without discrimination

Canon III — Protect Sensitive and Classified Information

S3EP professionals frequently have access to sensitive, proprietary, or classified information concerning space system vulnerabilities, architectures, and operations. Professionals shall:

- Handle sensitive and classified information in strict accordance with applicable laws, regulations, and contractual obligations
- Not disclose proprietary, sensitive, or classified information to unauthorized parties
- Comply with applicable export control laws, including International Traffic in Arms Regulation (ITAR) and Export Administration Regulations (EAR), when sharing information related to space systems

Canon IV — Act Within the Law

S3EP professionals shall comply with all applicable federal, state, local, and international laws and regulations governing their professional activities. Professionals shall:

- Obtain appropriate authorization before conducting security assessments, penetration tests, or offensive security activities on any space system
- Not engage in unauthorized access to computer systems, satellites, or space infrastructure
- Comply with privacy laws governing the collection and handling of personal data

Canon V — Advance the Profession

S3EP professionals have a responsibility to contribute to the growth and development of the space cybersecurity field. Professionals shall:

- Share knowledge with colleagues and the broader community through mentoring, publishing, and professional engagement, within the bounds of applicable confidentiality obligations
- Support the development and maintenance of space cybersecurity standards, frameworks, and best practices
- Encourage qualified individuals from diverse backgrounds to enter the space cybersecurity profession

6.2 Ethics Agreement

As a condition of receiving any S3EP certification, all candidates must sign the following attestation, which is incorporated into the certification application:

> "I have read and understand the S3EP Code of Ethics and Professional Conduct. I agree to uphold and be bound by this Code as a condition of receiving and maintaining my S3EP certification. I understand that violation of this Code may result in suspension or revocation of my certification by the PCA Certification Council, following the process described in the S3EP Candidate Handbook."

6.3 Ethics Complaint Process

Any individual—whether a PCA candidate, credential holder, employer, or member of the public—may submit an ethics complaint against an S3EP holder by sending a written complaint to certifications@parallax-cyber.com with the subject line "Ethics Complaint: [Holder Name]."

The complaint must include: the name and certification level of the holder alleged to have violated the Code; a description of the alleged conduct; the specific Canon(s) believed to have been violated; and any supporting documentation available. Anonymous complaints may be accepted but may be more difficult to investigate.

Ethics complaints are reviewed and adjudicated by the PCA Certification Council following the process described in Section 7.

SECTION 7 — APPEALS & GRIEVANCE PROCESS

7. Appeals and Grievance Process

7.1 Overview

Parallax Cyber Academy is committed to fair, consistent, and transparent decision-making. Any candidate, applicant, or credential holder who disagrees with a certification-related decision made by the PCA Certifications Team has the right to appeal that decision to the PCA Certification Council. The Council is the independent governing body of the S3EP program and serves as the final decision-making authority for all appeals.

7.2 Appealable Decisions

The following categories of decisions may be appealed:

- Denial of a certification application on eligibility grounds
- Denial of a testing accommodation request
- Examination scoring dispute (procedural irregularity only—substantive challenges to specific exam questions are not permitted)
- CPE audit determination (disqualification of submitted CPE credits)
- Suspension of certification for failure to renew
- Revocation for cause or ethics violation finding
- Denial of a reinstatement request

7.3 How to Submit an Appeal

All appeals must be submitted in writing. Oral or informal appeals will not be accepted or acted upon. To submit an appeal:

1. Prepare a written appeal statement that includes: your full legal name and certification number (if applicable); the specific decision being appealed and the date it was communicated; a clear statement of why you believe the decision was incorrect or unfair; all supporting evidence and documentation you wish the Council to consider; and the specific remedy or outcome you are requesting.
2. Submit the appeal by email to certifications@parallax-cyber.com with the subject line: "APPEAL: [Your Name], [Type of Decision]."
3. Pay the appeal filing fee (see Section 8). The fee is refunded if the appeal is decided in the appellant's favor.
4. Appeals must be filed within 60 calendar days of the date of the written decision being appealed. Appeals filed after this deadline will not be accepted absent extraordinary circumstances, which must be described in the appeal submission.

IMPORTANT	Submitting an appeal does not automatically stay or reverse the decision under appeal. If you wish to request a stay (temporary pause) of a suspension or revocation pending the outcome of an appeal, you must include a written request for a stay with your appeal submission. The Council will consider stay requests on a case-by-case basis.

7.4 Council Review Process

Upon receipt of a properly submitted appeal, the PCA Certification Council will conduct the following process:

Step	Timeline	Description
1	Within 5 business days of receipt	Acknowledgment: PCA sends written acknowledgment confirming receipt of the appeal and the assigned Council reviewer(s).
2	Within 10 business days of acknowledgment	Completeness Review: The Council verifies the appeal is complete and timely. Incomplete appeals are returned with written notice of what is missing and an opportunity to supplement within 15 days.
3	Within 20 business days of completeness confirmation	Fact Review: The Council reviews the written appeal, all supporting documentation, and the original decision record. The Council may request additional information from the appellant or from PCA staff. Neither party appears in person before the Council unless the Council specifically requests it.
4	Within 30 business days of completeness confirmation	Council Determination: The Council reviews the facts and makes a determination by majority vote of participating Council members. The determination may: uphold the original decision; overturn the original decision; or modify the original decision (e.g., reduce a revocation to a suspension). Recusal: any Council member with a conflict of interest with respect to the appellant must recuse themselves from the determination.
5	Within 5 business days of determination	Written Notice: The Council's written determination is sent to the appellant by email, stating the outcome, the rationale, and any corrective action to be taken. The Council's determination is final and binding within the S3EP program.

7.5 Ethics Complaint Adjudication

Ethics complaints filed pursuant to Section 6.3 follow the same Council review process described in Section 7.4, with the following additional steps:

- The holder against whom the complaint is filed will be notified of the complaint within 10 business days and given 20 business days to submit a written response.

- The Council reviews the complaint, the holder's response, and all supporting evidence before making its determination.
- Possible outcomes include: dismissal of the complaint (no violation found); a formal written warning; suspension of certification pending remediation; or revocation of certification.
- Both the complainant and the subject of the complaint will be notified of the Council's determination in writing.

SECTION 8 — FEE SCHEDULE

8. Fee Schedule

The following fee schedule is effective as of the date of this handbook edition. Fees are subject to change; current fees and payment instructions are always published on the PCA website at parallax-cyber.com. All fees are in U.S. Dollars (USD). PCA accepts payment by Paypal, credit card, Venmo, and organizational purchase order.

8.1 Application and Examination Fees

Transaction	Fee (USD)	Refundable?
Application Processing Fee (all certification levels)	**$60**	No*
Basic Exam Registration Fee (AS3EP, DSS3EP, DGS3EP)	**$75**	Partial**
Advanced Exam Registration Fee (CS3EP, ES3EP)	**$100**	Partial**
Exam Retake Fee — Basic (2nd attempt and beyond)	**$75**	No
Exam Retake Fee — Advanced (2nd attempt and beyond)	**$150**	No

*Application fees are non-refundable once the application has been reviewed, even if the application is denied. Applications withdrawn before review commences may receive a partial refund of $25.

**Exam fees are refundable (minus a $50 processing fee) if cancellation is received more than 7 business days before the scheduled exam date. Cancellations within 7 business days of the exam forfeit the full fee, but the exam may be rescheduled once without additional charge.

8.2 Annual Maintenance Fees

Certification Level	Annual Fee (USD)	Late Fee
AS3EP©	$60	+$25
DSS3EP© / DGS3EP©	$100	+$40
CS3EP©	$125	+$50
ES3EP©	$150	+$60

First annual maintenance fees are due upon the one-year anniversary of certification approval.

8.3 Other Fees

Service	Fee (USD)
Appeal Filing Fee (refunded if appeal succeeds)	$50
Reinstatement Fee (following suspension)	$100
Duplicate Certificate (digital)	$25
Name Change / Certificate Reissue	$50
CPE Late Submission (within grace period)	Per tier (see 8.2)
Organizational / Group Application (5+ candidates, same employer)	10% discount on application and exam fees

All fees must be paid before the associated service is performed. Parallax Cyber does not extend credit. Fee waivers may be available for active-duty and retired U.S. military members and qualifying students enrolled in accredited academic programs; contact certifications@parallax-cyber.com for details.

SECTION 9 — RESOURCES, CONTACT & FAQ

9. Resources and Contact Information

9.1 Key Resources

Resource	Location / Contact
S3EP Main Website	parallax-cyber.com/certification
Certification Registry (Verify a Credential)	parallax-cyber.com/verify
CPE Tracking Portal	parallax-cyber.com/cpe
Exam Scheduling Portal	parallax-cyber.com/schedule
Application Templates	parallax-cyber.com/apply (or email certifications@parallax-cyber.com)
Certified Vendor List	parallax-cyber.com/vendors
Certifications Team Email	certifications@parallax-cyber.com
Accommodations Requests	certifications@parallax-cyber.com — Subject: "Accommodation Request"
Ethics Complaints	certifications@parallax-cyber.com — Subject: "Ethics Complaint"
Appeals	certifications@parallax-cyber.com — Subject: "APPEAL"

9.2 Frequently Asked Questions

Can I apply for multiple certification levels simultaneously?

No. Applications are accepted for one certification level at a time. You may apply for a higher level once you have received your current level and have acquired any additional qualifying experience.

What happens if my reference does not respond?

PCA will make at least two attempts to contact each reference. If a reference is unresponsive after 15 business days, you will be notified and given the opportunity to provide an alternative reference. Your application will remain on hold during this period.

Are PCA-certified courses available online?

PCA-sponsored courses are offered in a variety of formats, including virtual instructor-led, in-person, and self-paced online options. Check the PCA website or contact the certifications team for the current schedule and format availability.

How do I report a change of name, employer, or contact information?

Notify the certifications team at certifications@parallax-cyber.com promptly upon any change. Name changes require supporting documentation (e.g., marriage certificate, court order) and a certificate reissue fee (see Section 8). Contact information updates are made at no charge.

Is the S3EP credential recognized by the U.S. Department of Defense?

PCA is pursuing alignment with DoD Directive 8140 (Cyberspace Workforce Management). Candidates and employers should consult the official DoD 8140 Qualification Matrix for current recognition status. PCA will update this section upon any formal DoD recognition.

Is there an organizational or employer sponsorship program?

Yes. Organizations seeking to sponsor multiple employees may take advantage of group pricing (see Section 8.3) and may contact certifications@parallax-cyber.com to discuss organizational accounts, bulk invoicing, and workforce development partnerships.

My company sponsors space cybersecurity training. How do I have my corporate training verified by Parallax Cyber Academy to meet S3EP exam preparation needs?

Contact certifications@parallax-cyber.com to discuss curriculum review and addition to the PCA-Certified Vendor List. Administrative fees may apply.

APPENDIX — GLOSSARY OF TERMS

Appendix A — Glossary of Terms

Term	Definition
Active Certification	A certification that is current, in good standing, and included in the PCA Active Certification Registry.
Candidate	An individual who has submitted an application for an S3EP certification and whose application has been approved, pending exam completion.
Certification Council (Council)	The governance body of the S3EP program, responsible for policy, appeals, and ethics adjudication.
CPE (Continuing Professional Education)	Activities that demonstrate ongoing professional development and maintenance of competence in the S3EP credential domain.
Ground Segment	The terrestrial components of a space system, including mission operations centers, ground stations, uplink/downlink systems, and data processing infrastructure.
Holder	An individual who currently holds one or more active S3EP certifications.
ITAR	International Traffic in Arms Regulations — U.S. export control regulations governing defense articles and services, including certain space systems.
PCA	Parallax Cyber Academy — the credentialing and training arm of Parallax Cyber, LLC.
PCA-Certified Vendor	A training organization that has been evaluated and approved by PCA to deliver qualifying S3EP courses. Current list at parallax-cyber.com/vendors.
Qualifying Experience	Paid or unpaid professional work in roles whose primary responsibilities fall within the domains defined in Section 2.3 of this handbook.
Revoked Certification	A certification that has been permanently terminated, either for failure to reinstate from suspension or for cause. Revoked holders must re-apply and re-examine to earn any new S3EP credential.
Space Segment	The space-based components of a space system, including satellite bus, payload, on-board computer, and associated flight software.
Suspended Certification	A certification that has been placed in inactive status due to non-renewal or pending investigation. Suspended holders may not represent themselves as actively certified.

Appendix B — Handbook Revision History

Version	Date	Summary of Changes
1.0	May 2026	Initial publication of the S3EP Candidate Handbook.

— End of S3EP Candidate Handbook —

Parallax Cyber Academy | certifications@parallax-cyber.com | parallax-cyber.com