# Certified Counter-Insider Threat Professional Program

Candidate Handbook

2019

The Certified Counter-Insider Threat Professional (CCITP) Program is co-sponsored by the Under Secretary of Defense for Intelligence (USD(I)) and the Director of the National Counterintelligence and Security Center (D, NCSC). The CCITP Program is governed by the CCITP Governance Council (CCITP-GC), which is co-chaired by a representative from the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) and a representative from the National Insider Threat Task Force (NITTF). The CCITP Program Management Office (PMO) executes all CCITP programmatic functions on behalf of the CCITP-GC.

Questions or concerns regarding this handbook or the CCITP Program can be directed to the CCITP PMO: OSD.CINT-Certification@mail.mil (NIPRnet)

To obtain more information about the CCITP Program or to download a copy of this handbook, please visit https://dodcertpmo.defense.gov/Counter-Insider-Threat/.

Version 1.0

## Table of Contents

# Program Overview

## Introduction

The Certified Counter Insider Threat Professional (CCITP) Candidate Handbook provides candidates and other interested parties with information on program intent, eligibility and maintenance requirements, details the steps required to take the certification exam, along with other program policies and procedures. Currently the CCITP Program has two certifications:

- CCITP – Fundamentals (CCITP-F)
- CCITP – Analysis (CCITP-A)

## CCITP Program History and Purpose

With the rise of classified information being released into the public domain and causing great damage to the interests and activities of U.S. and Allied forces across the world, the President of the United States signed Executive Order 13587 in 2011. The Executive Order created a mandate that every Executive Level Department and Agency have a Counter-Insider Threat (C-InT) Program capable of *deterring, detecting and mitigating* against actions by employees who present a threat to national security. The Executive Order also created the National Insider Threat Task Force (NITTF) as the Government-wide means for assisting Departments and Agencies as they develop and implement their own insider threat programs. Since the signing of the Executive Order, responses from the Executive Level Departments and Agencies across the U.S. Federal Government have varied. In 2017, the NITTF began partnering with OUSD(I) as part of an ongoing effort to bring all Departments and Agencies into compliance with the Executive Order as well as to standardize and professionalize the C-InT Workforce across the Federal Government.

On October 30, 2018, the OUSD(I), along with the NITTF, facilitated the first meeting of C-InT professionals from across the Federal Government to discuss the vision and scope of what would become the CCITP Program. This group would eventually evolve to become the CCITP-Governance Council (CCITP-GC). The goal of the CCITP-GC is to create a certification program that will establish workforce credibility, foster a professional identity, and catalyze professional development.

The CCITP Program is the first certification program within the U.S. Federal Government to be developed jointly by representatives from both the Department of Defense (DoD) and the broader U.S. Government (USG). Because of this joint effort, the scope and applicability of the CCITP Program is able to cut across all C-InT Programs within Departments and Agencies across the U.S. Federal Government. This effort was made possible by the partnership between the USD(I) and the Director of the National Counterintelligence and Security Center (NCSC) (a senior agency who manages the NITTF and reports to the Office of the Director of National Intelligence (ODNI)). Together the USD(I) and the Director of NCSC serve as the joint conferral authorities for the CCITP Program.

## CCITP-F Certification

The CCITP-F Certification is designed to measure and assess whether an individual has the requisite knowledge and skills as annotated within the CCITP-F Essential Body of Knowledge (EBK) to perform the tasks outlined in the CCITP-F Essential Body of Work (EBW), as identified by the C-InT Community. The CCITP-F Certification was designed with a target population of those personnel working directly in a C-InT Program, however, because each program is unique and has different needs and constraints, the CCITP-F Certification is open to anyone who works within or is affiliated with a C-InT Program, as determined by each Program Manager.

## CCITP-A Certification

The CCITP-A Certification is designed to measure and assess whether an individual has the requisite knowledge and skills as annotated within the CCITP-A Essential Body of Knowledge (EBK) to perform the tasks outlined in the CCITP-A Essential Body of Work (EBW), as identified by the C-InT Community. The CCITP-A Certification was designed with a target population of those personnel working directly in a C-InT Program and performing analysis functions; however, because each program is unique and has different needs and constraints, the CCITP-A Certification is open to anyone who works within a C-InT Program, as determined by each Program Manager.

## Certification Benefits

Benefits of obtaining a CCITP credential include:

**For Individuals:**

- Fosters understanding of the concepts and principles deemed critical to perform Counter-Insider Threat activities
- Identifies the individual as a certified C-InT professional regardless of position or employing organization
- Promotes professional development

**For Organizations/Employers:**

- Provides metrics for employee and workforce performance management
- Provides reliable and valid metrics for employment decision-making (e.g., hiring, promotion, transfer out of a work role)
- Provides certified C-InT individuals to enhance workforce competency

**For the Profession:**

- Provides summary information about workforce strengths and weaknesses
- Provides valuable information that can be used to integrate workforce initiatives and align supporting capabilities (e.g., training and education) to a common set of skill standards
- Provides shared understanding by creating common standards to measure C-InT professionals

# CCITP Program Governance and Development

## Governance

The CCITP-GC is the governing body for the CCITP Program. The CCITP-GC is an autonomous body comprised of senior-level stakeholders from across the Federal Government with equities in the C-InT workforce (i.e., civilian, military, and contractors). The CCITP is responsible for discussing and coordinating policies, standards, and professional development metrics; making all essential certification administration decisions; as well as ensuring each of the certifications within the program meet and maintain third-party accreditation standards.

The CCITP-GC is led by two co-chairs, one from the OUSD(I) representing the interests of the DoD, and one from the NITTF, representing the interests of the broader U.S. Government. They are supported by a group of voting members comprised of senior-level stakeholders from across the Federal Government, along with one CCITP Certified Member and one Public Member.

The two co-chairs are non-voting members of the CCITP-GC and are responsible for leading all CCITP-GC meetings, presenting the CCITP-GC with program updates and any essential administrative actions that require a vote, and ensuring that all CCITP-GC programmatic decisions are carried out. A Program Management Office (PMO) also exists to help Co-Chairs and the CCITP-GC as a whole to ensure that program runs in accordance with their guidance and according to accreditation standards. All other CCITP-GC members, to include the Certified Member and the Public Member are voting members and are responsible for ensuring that the CCITP Program is run in a fair manner and serves to meet the overall goals and benefits of the program as described above.

The CCITP-GC is required to convene at least two times annually. The CCITP-GC has two types of meetings, Closed Meetings and Open Meetings. Closed meetings are for the CCITP-GC Co-Chairs and all current active voting members. Closed meetings are designed to go over sensitive programmatic or administrative decisions (e.g., test specific issues, waiver/appeal requests, disciplinary issues, etc.). Open Meetings are designed to go over general program updates and provide a forum for non-voting stakeholders to bring issues or suggestions to the CCITP-GC.

## Assessment Development

Under the guidance of psychometricians, the CCITP Fundamentals and Analysis exam questions were developed based on their respective Essential Bodies of Knowledge (EBK). Draft questions were designed by a team of Subject Matter Experts (SMEs) from the C-InT Enterprise to assess the candidate’s mastery of the knowledge and skill requirements, identified by the job/practice analysis, and defined and described in the EBK. The team of SMEs from across the USG C-InT Enterprise reviewed each exam question for accuracy and relevance to the objectives set forth within the EBK. This process ensured questions and answers were correct, had the appropriate difficulty, and contained neither trivia nor ‘trick questions.’ Finally, two oversized exams were piloted by a large group of C-InT professionals. After the pilot tests were complete, a representative group of SMEs, working in conjunction with psychometric data covering each item and each exam, developed the final versions of each CCITP exam.

The CCITP PMO monitors “change factors” (e.g. policy change, doctrinal change, platform or system capability change) on a continuous basis to identify those changes that could affect exam questions. Based on the change factors, the PMO also assists in making adjustments to the exam questions necessary. The psychometricians will regularly review exams and test item performance to ensure that the items are performing correctly and that the exam as a whole is performing effectively. The items are reviewed by analyzing the test-level statistics. During these reviews, additional items may be generated and reviewed in order to bolster exam performance and ensure content is current.

## Determining Passing Score

The Angoff method, a widely used standard-setting approach in test development, was used to set the minimum passing score for each CCITP exam. The Angoff method has a well-established history of determining credible passing standards for professional certification examinations and was easily adapted by the CCITP exams.

The Angoff method involves two basic elements: 1) conceptualization of a minimally competent examinee and 2) SMEs estimation of whether a minimally competent examinee will answer an item correctly or incorrectly. Minimally competent examinees are those who possess the minimum qualification and knowledge to perform tasks associated with a job. The SMEs’ predictions about the minimally competent candidate’s performance on each test item are averaged and the resulting passing standard (or provisional cut-score) is thereby established. The provisional cut-score is then validated using empirical data collected during the pilot test phase to establish an operational cut-score for post pilot testing.

# CCITP-F Certification

## Eligibility and Pre-Requisites

Eligibility defines *who* is allowed to participate in the program and challenge the exam. Pre-Requisites define *what* those individuals must do prior to being authorized to participate in the program or challenge the exam. The Eligibility and Pre-Requisite requirements for the Fundamentals certification are as follows:

- Candidates must be current Hub/Program or Affiliated Personnel Only
- Candidates must have a minimum of 6 months experience working in/with a C-InT Hub/Program
- Candidates must complete a minimum of 10 hours of C-InT related training
- Candidates must receive Program Manager/Hub Chief Approval

These requirements will be documented in the candidate registration system and must be approved by the Candidate's organization's Hub/Program leadership prior to the Candidate scheduling the exam.  Approval by the Candidate's Hub/Program leadership indicates that leadership has reviewed the application and validated that it was complete and accurate.

## Scoring the CCITP-F Certification Exam

The CCITP-F Certification Exam is electronically scored, and a single overall score is computed. Candidates will be required to achieve a score of 650 or higher (out of a possible 800) on the CCITP-F Certification Exam. Candidates will have 130 minutes, or two (2) hours and ten (10) minutes to complete 115 multiple choice questions.  The questions are divided into five (5) different topic areas that align to the CCITP-F EBK.

Topic Areas:

- Topic Area 1: Policy and Directives
- Topic Area 2: Social and Behavioral Science
- Topic Area 3: Researching
- Topic Area 4: Synthesis
- Topic Area 5: Tools and Methods

The online score report does not constitute a final conferral decision. See CCITP Conferral for additional information on conferral.

## Feedback

A score report will be generated immediately upon completion of the exam. The report includes a pass/did not pass result, as well as a summary of performance. Candidates will also receive a copy of their score report via email (Note: This email is not the notice of certification conferral; the communication of conferral will occur separately.).

The score report will also provide feedback based on the Candidate's performance in the following combined topic areas.

- Group 1: Topic Area 1

- Group 2: Topic Areas 2 & 3
- Group 3: Topic Areas 4 & 5

## Retesting

A Candidate who does not pass the CCITP-F exam must wait a minimum of ninety (90) days, or until the next testing window occurs to take the exam again, whichever is longer.

## Use of CCITP-F Credentials

Candidates who pass the exam and are officially conferred will receive a letter and a digital badge. Conferred Certificants are authorized to use the designation "CCITP-F" or "Certified Counter-Insider Threat Professional – Fundamentals," as well as display their digital badge. This designation signifies that the Certificant has met all of the requirements for the CCITP-F Certification. Certificants may use this credential on business cards, resumes, and signature lines for as long as they maintain their certification. "CCITP-F" and "Certified Counter-Insider Threat Professional - Fundamentals" are the only designations approved for use and should appear after a comma following the certificant's name. No other designator and no other usage are approved.

**Examples of correct use:**

- Jessica A. Smith, CCITP-F
- Joseph A. Smith, Certified Counter-Insider Threat Professional - Fundamentals

If a Certificant allows their certification to expire, they will no longer be allowed to use the designation until he or she has recertified. Use of these credentials beyond the authorized period (without complying with recertification requirements) constitutes unauthorized use of the credential. The CCITP Governance Council may also revoke the use of this designation if an individual exhibits signs of misconduct or violation of policies. (See Disciplinary Policy and Procedures for more information).

## Certification Maintenance

The CCITP-F Certification is valid for a period of two years from the date of conferral. In order to prevent the certification from lapsing, Certificants must meet the following recertification requirements:

**Professional Development Units (PDUs):**

Certificants are required to complete 100 PDUs over the course of their 2-year maintenance cycle in order to successfully maintain their CCITP-F Credential. The 100 PDUs are divided between C-InT specific activities and professional growth activities in the following manner:

- 75 PDU: C-InT specific
- 25 PDU: Professional Growth

**Categories:**

There are three (3) general categories in which a Certificant can earn PDUs:

- Unique work experiences (e.g., special projects, job shadowing/rotations, achievements, professionalization projects)
- Training, education, additional Certification(s)
- Giving back to the community (e.g., leadership in teaching, mentoring, conferences, workshops, papers)

Refer to Appendix F for the PDU reference table that outlines the number of PDUs awarded for PDU activities required for certification maintenance.

# CCITP-A Certification

## Eligibility and Pre-Requisites

Eligibility defines *who* is allowed to participate in the program and challenge the exam. Pre-Requisites define *what* those individuals must do prior to being authorized to participate in the program or challenge the exam. The Eligibility and Pre-Requisite requirements for the Analysis certification are as follows:

- Certificants must Currently hold the CCITP-F Credential
- Certificants must be current Hub/Program Personnel
- Certificants must have a minimum of 12 months working in Hub/Program
- Certificants must complete a minimum of 40 hours of Analysis-related training
- Certificants must complete a minimum of 8 hours of UAM policy and/or tool-related training
- Certificants must review at least 10 Case Studies
- Candidates must receive Program Manager/Hub Chief Approval

These requirements will be documented in the candidate registration system and must be approved by the Candidate’s organization’s Hub/Program leadership prior to the Candidate scheduling the exam. Approval by the Candidate’s Hub/Program leadership indicates that leadership has reviewed the application and validated that it was complete and accurate.

## Scoring the CCITP-A Assessment

The CCITP-A Certification Exam is electronically scored, and a single overall score is computed. Candidates will be required to achieve a score of 650 or higher (out of a possible 800) on the CCITP-A Exam. Candidates will have 160 minutes or two (2) hours and forty (40) minutes to complete 100 multiple choice scenario-based questions. The questions are divided into six (6) different topic areas that align to the CCITP-A EBK.

**Topic Areas:**

- Topic Area 1: Policy and Directives
- Topic Area 2: Social and Behavioral Science
- Topic Area 3: Researching
- Topic Area 4: Synthesis
- Topic Area 5: Tools and Methods
- Topic Area 6: Vulnerabilities Assessment

The online score report does not constitute a final conferral decision. See CCITP Conferral for additional information on conferral.

## Feedback

A score report will be generated immediately upon completion of the exam. The report includes a pass/did not pass result, as well as a summary of performance. Individuals will also receive a copy of their score report via email (Note: This email is not the notice of certification conferral; the communication of conferral will occur separately.).

The score report will also provide feedback based on the Candidate's performance in the following combined topic areas

- Group 1: Topic Area 1
- Group 2: Topic Areas 2 & 3
- Group 3: Topic Areas 4 & 5
- Group 4: Topic Area 6

## Retesting

A candidate who does not pass the CCITP-A exam must wait a minimum of ninety (90) days, or until the next testing window occurs to take the exam again, whichever is longer.

## Use of CCITP Credentials

Candidates who pass the exam and are officially conferred will receive a letter and a digital badge. Conferred Certificants are authorized to use the designation "CCITP-A" or "Certified Counter-Insider Threat Professional - Analysis" as well as display their digital badge. This designation signifies that the Certificant has met all of the requirements for the CCITP-A Certification. Certificants may use this credential on business cards, resumes, and signature lines for as long as they maintain their certification. "CCITP-A" and "Certified Counter-Insider Threat Professional - Analysis" are the only designations approved for use and should appear after a comma following the certificant's name. No other designator and no other usage are approved.

**Examples of correct use:**

- Jessica A. Smith, CCITP-A
- Joseph A. Smith, Certified Counter-Insider Threat Professional - Analysis

If a certificant allows their certification to expire, they will no longer be allowed to use the designation until he or she has recertified. Use of these credentials beyond the authorized period (without complying with recertification requirements) constitutes unauthorized use of the credential. The CCITP Governance Council may also revoke the use of this designation if an individual exhibits signs of misconduct or violation of policies. (See Disciplinary Policy and Procedures for more information).

## Certification Maintenance

The CCITP-A Certification is valid for a period of three years from the date of conferral. In order to prevent the certification from lapsing, Certificants must meet the following requirements:

**Professional Development Units (PDUs) (100 total):**
Certificants are required to complete 100 PDUs over the course of their 3-year maintenance cycle in order to successfully maintain their CCITP-A Credential. The 100 PDUs a divided between C-InT specific activities and professional growth activities in the following manner:

- 50 PDU: C-InT specific
- 50 PDU: Professional Growth

**Categories:**
There are three (3) general categories in which a Certificant can earn PDUs:

- Unique Work Experiences (e.g., special projects, rotations, achievements, professionalization projects)
- Training, Education, additional Certification(s)
- Giving back to the Community (e.g., leadership in teaching, mentoring, conferences, workshops, papers)

Refer to Appendix F for the PDU reference table that outlines the number of PDUs awarded for PDU activities required for certification maintenance.

## Registering for the Exams

Candidates interested in taking either CCITP Certification Exam must first register online via the following link https://cint-gsx.learningbuilder.com. Candidates will be required to create an account within the candidate management system and complete of a series of demographic questions. After completing the demographic questions, Candidates will have to answer a series of questions demonstrating how they have met both the eligibility and pre-requisite requirements in order to proceed. Candidates will then submit their registration within the candidate management system. The registration request will then be sent to the Candidate's Program Manager/Hub Chief (PM/HC) for validation and approval. Once approved by the PM/HC, Candidates will be contacted by the CCITP PMO with approval to test and instructions for scheduling an exam.

NOTE: The PM/HC has final approval authority over a candidate's eligibility. If a candidate feels that they have met the eligibility and all of the other prerequisites but are for some reason not being approved by their PM/HC, they should first contact their PM/HC and discuss the issue with them. If they are unable to resolve the issue with their PM/HC, the candidate may submit an appeal to the CCITP PMO in writing (for further details on this process, see the Appeals section of this Handbook).

The exams are delivered at all Pearson VUE Testing Centers worldwide. With 5,600 locations throughout the United States, Europe, Asia and the Middle East, Pearson VUE is able to meet the needs of most members of the USG C-InT Workforce. Additionally, testing centers are located on over 100 U.S. military installations and in numerous cities throughout multiple countries.

Candidates should ensure familiarization with the No-Show Policy.

### Requests for Reasonable Accommodations

If a Candidate feels that they require any special accommodations in order to take any of the CCITP Certification Exams, they need to contact the CCITP PMO to request those accommodations. If requested, the CCITP PMO will work with testing centers to 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 accommodations will be made for known physical or mental limitations if the Candidate is a qualified individual with a disability.

A request for a reasonable accommodation is a 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 specific words, such as “reasonable accommodation,” “disability,” or “Rehabilitation Act.” If a Candidate has a disability, he/she may request a reasonable accommodation, even if the Candidate has not previously disclosed the existence of a disability.

It is the responsibility of the Candidate to seek accommodations in advance of his/her exam date. Candidates must provide verification of the disability and a statement of the specific type of assistance needed to the CCITP PMO at least 30 days prior to the desired exam date. Requests are to be sent to the CCITP PMO at osd.CINT-Certification@mail.mil.

The CCITP PMO may request documentation from an appropriate health care or rehabilitation professional about a 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 a specific disability and the existing limitations in completing the certification process. The ability to provide a specific accommodation is also based on the capabilities available at the testing center providing the exam for the requesting party.

The CCITP PMO, along with the exam location, will make reasonable efforts to accommodate each request. If it would impose an undue burden to provide the required testing environment, the Candidate will be notified with a written explanation of the denial and a statement of the reasons for the denial.

Grievances regarding denied accommodations may be appealed to the CCITP PMO, who will then coordinate a response with the employing organization’s Equal Employment Opportunity Office.

## Preparing for the CCITP Exams

The CCITP exams are training-agnostic, meaning they do not require Candidates to participate in any specific course or group of courses to prepare for the exams. It also does not require membership in any association and does not require the purchase of any product or service. The CCITP PMO is an independent organization that operates as a third party and is firewalled from participating in the design, development, or implementation of education, training, and similar content-focused programs. Candidates are advised that the CCITP PMO does not offer courses or materials to prepare Candidates for the exams, nor does it currently accredit any educational/training programs or courses of study leading to eligibility or certification.

Candidates are instead encouraged to review the information provided for each of the knowledge domains covered in their respective EBKs for the certification they are considering. Each EBK contains a listing of the knowledge areas a practitioner within the C-InT workforce is expected to possess. Appendix B contains the CCITP-F EBK along with all relevant sources. Appendix C contains the CCITP-A EBK along with all relevant sources.

**Testing Tips:**
Consider the following when preparing for one of the CCITP exams:

- Relax before the assessment.
- Find the test center location in advance.
- Arrive early.
- Keep a positive attitude throughout the entire testing session.
- Trust your first impression.
- Read the entire question carefully.
- Do not overanalyze the questions or answers.
- Pace yourself.
- 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.
- Use your time wisely.
- Answer all questions; there is no penalty for guessing.
- The body of material covered on the exam cannot be memorized in its entirety.

All CCITP Program content (i.e., EBKs and examinations) is UNCLASSIFIED and based on publicly-available source documentation (e.g., Executive Orders, Federal laws and statutes, DoD policy, and Intelligence Community Directives, etc.; however, they do not incorporate individual organization requirements, nor does it incorporate organization-specific standard operating procedures).

## No Show Policy

If a candidate does not cancel or reschedule a confirmed exam at least 48 hours prior to the scheduled exam and does not show up for their scheduled exam, the USG will still be charged an exam seat fee as if the candidate sat for the exam. PLEASE make every effort to make your scheduled exam date or reschedule in time to meet the Pearson VUE Deadline. If an individual is a no-show for two exam iterations, he or she will not be able to participate in the CCITP program. Individuals may appeal by submitting a waiver request explaining why they were unable to make scheduled exam sessions.

# Taking the Exam

Candidates should arrive at the test center at least 30 minutes prior to the scheduled exam time. Candidates who arrive more than 15 minutes later than the scheduled exam start time will be refused admission.

Candidates must bring evidence of identity. Candidates will not be permitted to take an exam without proper identification. Test center proctors will verify candidate identification, including U.S. citizenship (e.g., U.S. passport or a birth certificate and a government-issued photo ID), driver's license (except from MN and MO), military ID card, or another ID card issued by a federal, state, or local government agency as long as it contains a photograph or information such as name, date of birth, gender, height, eye color and address. Test center proctors and administrators will read instructions to candidates and for online testing, provide each candidate with a unique testing system log-in.

Test centers will execute requests for reasonable accommodations as appropriate and possible for those who submitted a request for such accommodations at least 30 days prior to the exam.

The CCITP-F Exam consists of 115 multiple choice items and Candidates will have 130 minutes (2 hours and 10 minutes) to complete the exam. The CCITP-A Exam consists of 100 scenario-based multiple-choice items, and Candidates will have 160 minutes (2 hours and 40 minutes) to complete the exam. An additional 15 minutes will be allotted for instructions, the signing of a Non-Disclosure Agreement and a brief system tutorial. The tests will be offered at any Pearson Vue testing center during selected windows.

## Testing Environment

Candidates may not bring any of the following items into the test center:

- Smartphones/Cell Phones
- Laptops
- Hand-held computers or personal electronic devices, including e-readers, tablets, and smart watches
- Calculators
- Tape Recorders
- Pagers
- Notes
- Newspapers
- Books
- Bags
- Hats/Coats
- Purses/wallets

If there is not designated secure storage at the test center, Candidates may bring the items into the testing room, but the items must be placed in an inaccessible location within the room during the exam.

Candidates are expected to conduct themselves in a professional manner in the testing environment. Candidates who do not conduct themselves in such a manner are subject to disciplinary action from CCITP PMO, which can include dismissal from the test center regardless of the Candidate's completion of the exam.

Testing center proctors and administrators are responsible to monitor Candidates during testing and to provide directions for taking the exam at the outset of the testing session but are not allowed to help candidates read or comprehend exam questions. During the administration of the examination, talking to anyone other than a proctor or administrator is not permitted. In addition, Candidates are not permitted to discuss examination content (i.e., questions or answers) with anyone at any time.

## Non-Discrimination Policy

The CCITP Program does not discriminate on the basis of race, color, national origin, sex (including pregnancy or childbirth), religion, age, disability (physical or mental), sexual orientation, marital status, parental status, political affiliation, genetic information, or retaliate for participating in protected activities. The CCITP Program complies with all applicable jurisdictional laws and regulations related to protection against discrimination in access to CCITP Exams. Additionally, CCITP procedures ensure that all applicants and candidates are treated in an equitable and consistent manner throughout the entire certification process. The eligibility requirements, exam instrument content, exam environment, scoring method, and maintenance and recertification process provide for a fair, impartial, and bias-free certification program.

## Exam Security and Confidentiality

To ensure the integrity of the CCITP Program, all questions and answers developed to create the exam are For Official Use Only and are not authorized for public release.

### Terms and Conditions

The CCITP PMO recognizes the importance and the sometimes sensitive nature of the C-InT work and the individuals performing that work; as such, the CCITP PMO strives to maintain Candidate and Certificant confidentiality as much as possible.  Personally identifiable information (PII) and assessment results are protected and will not be disclosed without the written consent of a candidate, unless when necessary to comply with a compulsory, legally-authorized demand or order of a court of competent jurisdiction.  To allow the CCITP PMO to release personal or conferral information to a third party other than as described in this handbook, the Candidate must authorize such activity 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 PII redacted.

The CCITP PMO also recognizes that there will be times when employing organizations and/or interested third parties may need to verify whether or not an individual possesses a CCITP Credential. Verification requests can be made to the CCIPT PMO in writing and will receive one of the following two (2) responses:

- “Yes, (Individual) currently holds an active CCITP-F/A Credential.”
- “No, (Individual) does not currently hold an active CCITP-F/A Credential.”

Personal scores will not be provided to anyone but the Candidate and are for feedback purposes only.  Also, no information will be provided by the CCITP PMO about those Candidates who take the exam and do not pass.

Candidates refusing to accept the Terms and Conditions will not be permitted to take the exam.

## Non-Disclosure Agreement

All Candidates are required to sign a Non-Disclosure Agreement (NDA) prior to beginning either CCITP exam. This agreement is to ensure the security of the CCITP exams and prohibits the discussion or sharing of all exam-related content.

The CCITP exam shall be conducted in appropriate facilities and in a proctored environment. Proctors are responsible for ensuring consistent testing environments and exam security and will also be required to sign an NDA.

The CCITP exams shall be protected through industry- and government-accepted security protocols. The exams shall not be accessed, copied, printed, or distributed without specific written approval from the CCITP PMO.

## CCITP Conferral

Per National Commission for Certifying Agencies (NCCA) guidance, credentials may only be awarded after a Candidate's knowledge and/or skills are evaluated and determined to be acceptable. To be recommended for conferral, Candidates must successfully meet all the exam eligibility requirements and meet or exceed the certification exam qualifying score. The names of those Candidates who successfully meet the exam eligibility requirements and passing criteria will be submitted to the DoD USD(I) and the Director of NCSC for final adjudication and conferral approval. After conferral recommendations are approved, the CCITP PMO will notify the new Certificants and award them their credentials.

Letters and digital badges will be issued to signify the CCITP Credential. Information on how to access the Certificant's digital badge will be provided in the conferral email sent to the Certificant. Digital badges are tokens that appear as icons or logos on a web page or other online venue signifying accomplishments, such as conferral of a certification or mastery of a skill. The CCITP PMO will maintain a record of the digital badge with attendant metadata. This metadata includes the issuer's names (the USD(I) and the Director of NCSC), the Certificant's name and e-mail address, a link to the certification criteria, and a short description of the badge. It will also specify other details, such as the issue date and the expiration date; the badge will expire at the end of the conferral period unless Certificants renew the certification (as described in the Maintenance sections for each CCITP Certification above). Upon expiration, the badge will no longer appear as active on the web page where it is stored.

Digital badges are viewable by the Certificant and those to whom the Certificant provides his/her unique badge URL. The badge serves as proof of the certificant's conferral status.

The CCITP PMO will maintain a registry of all conferred Certificants. Confirmation of an individual's conferral status will be provided to interested parties upon request, but an individual's score will not be provided.

## Reinstatement of Expired Credentials

Individuals who fail to meet the certification maintenance requirements will receive a notice from the CCITP PMO that their credential has expired. Individuals who allow their CCITP-F credential to expire will automatically lose their right to use the credential and must apply as a new Candidate and meet all of the requirements in place at the time of re-application, to include retaking the exam. Individuals who allow their CCITP-A Credential to expire will automatically lose both their right to use their CCITP-A Credential *and* their CCITP-F Credential and will have to meet all of the requirements in place at the time of re-application, to include retaking the exams.

## Disciplinary Policy and Procedures

The CCITP-GC is the authoritative body for standards of conduct, and policies and procedures governing disciplinary action for the CCITP Certification Program. On disciplinary matters, the CCITP PMO may only address the conferral and certification aspects of the violation as approved by the CCITP GC.

All other disciplinary actions (if any) taken against CCITP Candidates and/or Certificants will be the responsibility of their employer.

Unethical or unprofessional behavior may be cause for the CCITP PMO or PM/HC to deny a candidate's admission to the CCITP Certification Program, to terminate participation at any stage throughout the conferral process, or to invalidate the result of an examination. In the case of a Certificant, the individual may have their certification(s) revoked and be barred from re-entry into the program for a period of up to two (2) years.

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

1. **Cheating**. Cheating on an exam consists of willfully consulting a notebook, textbook, or any other source of information not specifically authorized by the proctor during the exam; willfully aiding, or receiving aid, or attempting to aid or receive aid from another Candidate, Certificant or any other individual during an examination; obtaining or attempting to obtain copies of the examination before it is given; or any act or attempt made with the intent of violating or circumventing the stated conditions governing the administration of an examination.
2. **Test compromise**. Actions that compromise the integrity of the CCITP Certification Exams, including but not limited to unauthorized possession of or access to real exam questions; copying any portion of a CCITP Certification Exam (this includes any portion of the exam questions or answers); or the sharing or the receipt of exam information before, during, or after the exam session that gives any tester an unfair advantage over other Candidates.
3. **Misrepresentation or false statements**. Falsification of information on any document needed to acquire a CCITP Certification. Misrepresentation or false statements regarding an individual's conferral status of a CCITP Credential (i.e., claiming to hold a CCITP credential when the credential has not been conferred, or claiming to hold the credential after it has expired but was not renewed in accordance within the CCITP Certification exam guidelines).

4. **Non-compliance.** Refusal by the Candidate or Certificant to comply with their organization's Code of Ethics, standards of conduct, rules, or professional behavior. This particularly includes any violation of any part of their signed CCITP NDA.
5. **Request by the Certificant's parent organization** that the certification be revoked.

The CCITP PMO will conduct inquiries into suspected violations of the CCITP Certification Disciplinary Policy in direct coordination with the individual Candidate's and/or Certificant's Component.

**Process for Reporting Suspected Violations:** Suspected violations may be submitted by any interested party to the test proctor, the Organization PM/HC, or the CCITP PMO, as appropriate. The Complainant's name, witnesses, and the content of the complaint will remain confidential, unless legal requirements mandate disclosure. Notices of suspected violations will be sent to the Candidate's employing Agency or Organization for investigation. The Organization PM/HC will notify the CCITP PMO of their determination and action taken so that the CCITP PMO can determine if additional action or information is needed. All investigations into suspected violations will be completed within 60 days.

# Waiver Policy

## Waiver Policy

The waiver policy governs the process for providing a temporary suspension of a policy or procedure. Waivers may be appropriate in cases when circumstances outside of the control of the individual prevent the Candidate/Certificant from meeting specific certification requirements.

Waivers may be filed in cases such as:

- The Certificant requests a time extension due to extenuating circumstances (e.g., military deployment or medical hardship) that would prohibit an individual from meeting the requirement for maintaining a current CCITP Credential.

- The Candidate is being deployed and would like to retake the exam prior to deploying and would like the 90-day waiting period to be waived.

## Waiver Process and Procedures

A waiver may be filed when the Candidate or Certificant is faced with a certification requirement that cannot be met, due to reasons outside his/her control. The individual may request a waiver by submitting a Waiver Request Form (see Appendix D) to the CCITP PMO mailbox (osd.CINT-Certification@mail.mil). Each waiver will be reviewed by the CCITP PMO. All decisions will be made on a case-by-case basis, and a written response will be provided to the individual within 30 days from the request.

# Appeals Policy

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

## Grounds for Appeal

An appeal may be filed based on all decisions relating to:

- Examination results, criteria for obtaining a passing score on the CCITP Exams, or Candidate registration and test-taking protocols.
- Certification renewal requirements, such as completion of approved PDUs or timeliness of completing and reporting PDUs.
- Findings by the CCITP PMO related to alleged cheating, violations of rules of conduct or law, or inaccurate application information.
- Certification status (e.g. date of certification expiration or renewal).

## Decisions Not Eligible for Appeal

Matters not described in "Grounds for Appeal" above are not within the purview of the CCITP Program and are not appealable to the CCITP PMO, including the following Agency/Organization/Component decisions:

- Certification waiver decisions
- Employment policy
- Eligibility criteria for identifying billets or individuals requiring CCITP Certification

Individuals should contact their employing organizations with questions or appeals of decisions outside the purview of the CCITP Certification Program.

## Appeals Process

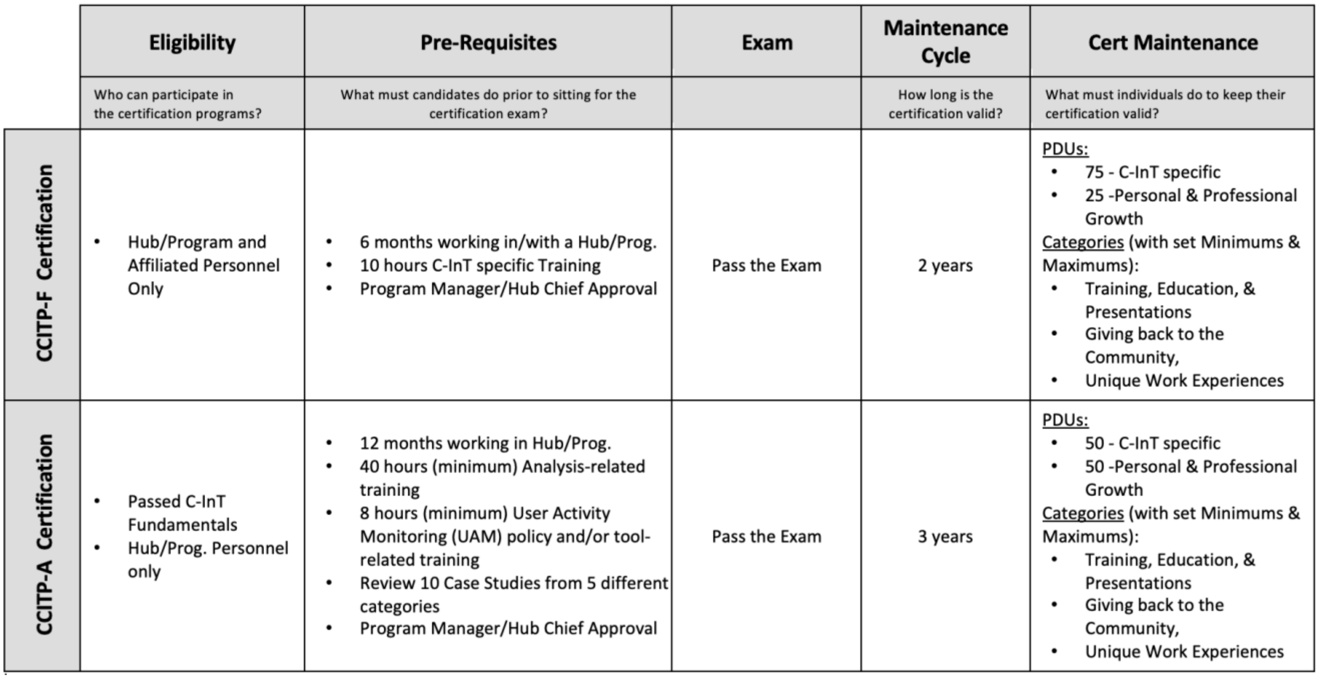
Individuals have up to 15 business days from the date of receiving an appealable decision or after completing the assessment, whichever occurs first, to submit an appeal.  All appeals must be submitted in writing to the CCITP PMO using the Appeals Request Form (Appendix E).  The form must be completed and sent to osd.CINT-Certification@mail.mil.  Individuals submitting an appeal must provide their contact information (unclassified phone number and email address), specific grounds for appeal, and evidence in support of the appeal.

## Appeals Review

The CCITP PMO conducts a preliminary review of all appeals within five (5) business days of receipt to ensure the appeal is timely, contains all required and pertinent information, and is allowable/meets grounds for appeals.  A Certification Appeals Board (CAB) will be created to review all Allowable appeals. The CCITP CAB will consist of the Chief of the CCITP PMO and two (2) CCITP-GC members (unaffiliated with individual or the organization involved in the appeal).

- Appeals that are not allowable or are received outside the 15-business day window, will be dismissed without referral to the CAB. The Candidate and their PM/HC will be notified in writing of the dismissal.
- Appeals that require additional information will be referred back to the appealing individual to provide further information before a determination on the validity of the appeal is made.
- Upon receipt of a valid appeals request, the CAB shall have 30 days to review relevant information, request additional information from the individual, and make a determination. The CAB may grant or deny the appeal request. CAB decisions shall be made by consensus; if consensus is unattainable, a majority vote by CAB members shall prevail. The CAB shall provide a written response to the individual documenting the basis for the decision.
- If, after the CAB review, the individual would like a second appeal, the individual has 15 business days from when they receive their initial verdict to submit a second appeal in writing to the CCITP PMO.
- Upon receipt of the second appeal, the CCITP PMO will inform the CCITP-GC Chair, who will ensure that the appeal is on the agenda at the next regularly-scheduled CCITP-GC meeting. If there is not a CCITP-GC meeting scheduled within a reasonable timeframe, the CCITP-GC Chair will direct the CCITP PMO to distribute all evidence to CCITP-GC members and facilitate a remote (i.e., electronic) review and vote on the appeal.
- The CCITP GC may grant or deny a second appeal. Appeals decisions by the CCITP-GC shall be made by consensus; where consensus is not attainable, decisions supported by at least 60% of the Governance Council voting members shall prevail. The second appeal constitutes the final decision, and no further consideration will be given to the appeal.

# Appendix A: Final Policy Requirements for CCITP Certification



| | Eligibility | Pre-Requisites | Exam | Maintenance Cycle | Cert Maintenance |
|---|---|---|---|---|---|
| | Who can participate in the certification programs? | What must candidates do prior to sitting for the certification exam? | | How long is the certification valid? | What must individuals do to keep their certification valid? |
| **CCITP-F Certification** | • Hub/Program and Affiliated Personnel Only | • 6 months working in/with a Hub/Prog.<br>• 10 hours C-InT specific Training<br>• Program Manager/Hub Chief Approval | Pass the Exam | 2 years | PDUs:<br>• 75 - C-InT specific<br>• 25 -Personal & Professional Growth<br>Categories (with set Minimums & Maximums):<br>• Training, Education, & Presentations<br>• Giving back to the Community,<br>• Unique Work Experiences |
| **CCITP-A Certification** | • Passed C-InT Fundamentals<br>• Hub/Prog. Personnel only | • 12 months working in Hub/Prog.<br>• 40 hours (minimum) Analysis-related training<br>• 8 hours (minimum) User Activity Monitoring (UAM) policy and/or tool-related training<br>• Review 10 Case Studies from 5 different categories<br>• Program Manager/Hub Chief Approval | Pass the Exam | 3 years | PDUs:<br>• 50 - C-InT specific<br>• 50 -Personal & Professional Growth<br>Categories (with set Minimums & Maximums):<br>• Training, Education, & Presentations<br>• Giving back to the Community,<br>• Unique Work Experiences |

# Appendix B: CCITP-F Essential Body of Knowledge

The Essential Body of Knowledge (EBK) is the domain of essential information over which mastery is required for success in the C-InT profession. The list of references contained in the EBK is broad but not exhaustive. Each contains key concepts that a Counter-Insider Threat professional is expected to know and understand, but only a subset of the references was used to generate items for the CCITP-F exam.

| Topic Area | References |
|---|---|
| **Topic Area 1**: Policy and Directives (25%)<br>Sub-Topic Areas:<br>• Insider Threat Policies<br>• Counter-Insider Threat Program<br>• Protecting Civil Liberties | • DoD 5220.22-M, National Industrial Security Program Operating Manual, May 2016<br>• DoDD 5205.16, The DoD Insider Threat Program<br>• DoDI 2000.26, Suspicious Activity Reporting (SAR)<br>• DoDI 5205.83, DoD Insider Threat Management and Analysis Center (DITMAC)<br>• DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information<br>• EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information<br>• 2017 Insider Threat Guide<br>• 1995 Intelligence Authorization Act, Section 811<br>• National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 2012<br>• Security Executive Agent Directive 5, Collection, Use and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications, May 2016<br>• Insider Threat Mitigation Responses, Student Guide, September 2017<br>• National Insider Threat Task Force Mission<br>• FY17 NDAA, Subtitle F, Section 951<br>• Titles I and V of the Americans with Disabilities Act (ADA) of 1990<br>• What is FOIA?<br>• Health Insurance Portability and Accountability Act of 1996<br>• Your Rights Under HIPAA<br>• DoDD 5400.11, DoD Privacy Program<br>• DoDI 7050.01, DoD Hotline Program |

| Topic Area | References |
|---|---|
| **Topic Area 1 cont'd**: Policy and Directives (25%) | • Executive Order 12333, US Intelligence Activities<br>• Privacy Act of 1974<br>• The Privacy Act Handbook<br>• Whistleblower Protection Act of 1989 |
| **Topic Area 2**: Social and Behavioral Science (10%)<br><br>Sub-Topic Areas:<br>• Psychology of Insider Threat | • Perspectives on Threat Management, 2016<br>• Workplace Assessment of Targeted Violence Risk: The Development and Reliability of the WAVR-21<br>• DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy<br>• FBI: Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks<br>• Behavioral Indicators of Insider Threat: Looking Forward<br>• Assessing the Mind of the Malicious Insider, Intelligence and National Security Alliance, 2017<br>• Pathway to Violence<br>• Application of the Critical-Path Method to Evaluate Insider Risks<br>• Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats. |
| **Topic Area 3**: Researching (30%)<br><br>Sub-Topic Areas:<br>• Information Protection<br>• Investigative and Operational Viability<br>• Counterintelligence (CI) Pillar<br>• Cyber Pillar<br>• Human Resources (HR) Pillar<br>• Law Enforcement (LE) Pillar<br>• Legal Pillar<br>• Behavioral Science Pillar<br>• Security Pillar | • DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)<br>• DoDD 5400.11, DoD Privacy Program<br>• Executive Order 12333, US Intelligence Activities<br>• EO 13526, Classified National Security Information<br>• The Freedom of Information Act, 5 U.S.C., Section 552<br>• General Records Schedule 5.6: Security Records<br>• 2017 Insider Threat Guide<br>• M-07-16, Safeguarding Against and Responding to the Breach of PII<br>• Civil Liberties FAQ<br>• Privacy Act of 1974<br>• (U) U.S. Insider Threat Security Classification Guide V.1, Dec 2013<br>• CDSE: DoD Insider Threat Program Best Practices, 1.1. Hub Hiring Rev 2, May 2017<br>• CDSE: Preserving Investigative and Operational Viability in Insider Threat, Sept 2017<br>• CDSE: Counterintelligence Awareness Job Aid, Foreign Collection Methods |

| Topic Area | References |
|---|---|
| **Topic Area 3 cont'd**: Researching (30%)<br>Sub-Topic Areas:<br>• Information Protection<br>• Investigative and Operational Viability<br>• Counterintelligence (CI) Pillar<br>• Cyber Pillar<br>• Human Resources (HR) Pillar<br>• Law Enforcement (LE) Pillar<br>• Legal Pillar<br>• Behavioral Science Pillar<br>• Security Pillar | • Executive Order 12333, US Intelligence Activities<br>• FBI: Elicitation Techniques<br>• National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov 2012<br>• CDSE: Cybersecurity for Security Personnel, Sept 2017<br>• DoD 5220.22-M, National Industrial Security Program Operating Manual, May 2016<br>• DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, Jul 2017<br>• CDSE: Establishing an Insider Threat Program for Your Organization<br>• Stiennon, R. (2013). Grasping the Problem with Privileged Accounts.<br>• DoDI 1400.25, Vol 431, DoD Civilian Personnel Management System: Performance Management and Appraisal Program, Jul 2019<br>• CDSE: Insider Threat Records Checks INT230.16<br>• Band et al., (2006). Comparing insider threat IT sabotage and espionage: A model-based analysis. |
| **Topic Area 4**: Synthesis & Tools and Methods (35%)<br>Sub-Topic Areas:<br>• All-Source Insider Threat Assessment<br>• All-Source Insider Threat Referral Triage<br>• All-Source Insider Threat Trend Analysis<br>• Analytic Communication<br>• Critical Thinking Techniques<br>• Databases and Data Feeds<br>• DITMAC System-of-Systems (DSoS)<br>• Structured Analytic Techniques | • EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information<br>• Why employee training matters: negligent users are top insider threat<br>• CDSE: Developing a Multidisciplinary Insider Threat Capability<br>• Intelligence Community Directive 203: Analytic Standards<br>• 2017 Insider Threat Guide<br>• Splunk: Quick Reference Guide<br>• A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis<br>• NIST Special Publication 800-160, Systems Security Engineering<br>• NIST Special Publication 800-64, Information Security<br>• CDSE: Insider Threat Records Checks: Student Guide, 2017 |

| Topic Area | References |
|---|---|
| **Topic Area 4 cont'd**: Synthesis & Tools and Methods (35%) | • CDSE: DoD Insider Threat Management Analysis Center (DITMAC): Student Guide, 2016<br>• DCSA: DoD Insider Threat Management and Analysis Center (DITMAC)<br>• Privacy Act of 1974: System of Records |

# Appendix C: CCITP-A Essential Body of Knowledge

The Essential Body of Knowledge (EBK) is the domain of essential information over which mastery is required for success in the C-InT profession. The list of references contained in the EBK is broad but not exhaustive. Each contains key concepts that a Counter-Insider Threat professional is expected to know and understand, but only a subset of the references was used to generate items for the CCITP-A exam.

| Topic Area | References |
|---|---|
| **Topic Area 1**: Policy and Directives (20%)<br>Sub-Topic Areas:<br>• Insider Threat Policies<br>• Counter-Insider Threat Program<br>• Protecting Civil Liberties | • National Industrial Security Program Operating Manual<br>• DoDD 5205.16, The DoD Insider Threat Program<br>• DoDI 2000.26, Suspicious Activity Reporting (SAR)<br>• DoDI 5205.83, DoD Insider Threat Management and Analysis Center (DITMAC)<br>• DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information<br>• EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information<br>• 2017 Insider Threat Guide<br>• 1995 Intelligence Authorization Act, Section 811<br>• National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 2012<br>• Security Executive Agent Directive 5, Collection, Use and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications, May 2016<br>• Insider Threat Mitigation Responses, Student Guide, September 2017<br>• National Insider Threat Task Force Mission<br>• FY17 NDAA, Subtitle F, Section 951<br>• Titles I and V of the Americans with Disabilities Act (ADA) of 1990<br>• What is FOIA?<br>• Health Insurance Portability and Accountability Act of 1996<br>• Your Rights Under HIPAA<br>• DoDD 5400.11, DoD Privacy Program<br>• DoDI 7050.01, DoD Hotline Program |

| Topic Area | References |
|---|---|
| **Topic Area 1 cont'd**:<br>Policy and Directives (20%) | - Executive Order 12333, US Intelligence Activities<br>- Privacy Act of 1974<br>- The Privacy Act Handbook<br>- Whistleblower Protection Act of 1989 |
| **Topic Area 2**: Social and Behavioral Science (10%)<br>Sub-Topic Areas:<br>- Psychology of Insider Threat | - Perspectives on Threat Management, 2016<br>- Workplace Assessment of Targeted Violence Risk: The Development and Reliability of the WAVR-21<br>- DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy<br>- FBI: Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks<br>- Behavioral Indicators of Insider Threat: Looking Forward<br>- Assessing the Mind of the Malicious Insider, Intelligence and National Security Alliance, 2017<br>- Pathway to Violence<br>- Application of the Critical-Path Method to Evaluate Insider Risks<br>- Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats. |
| **Topic Area 3**: Researching (20%)<br>Sub-Topic Areas:<br>- Information Protection<br>- Investigative and Operational Viability<br>- Counterintelligence (CI) Pillar<br>- Cyber Pillar<br>- Human Resources (HR) Pillar<br>- Law Enforcement (LE) Pillar<br>- Legal Pillar<br>- Behavioral Science Pillar<br>- Security Pillar | - DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)<br>- DoDD 5400.11, DoD Privacy Program<br>- Executive Order 12333, US Intelligence Activities<br>- EO 13526, Classified National Security Information<br>- The Freedom of Information Act, 5 U.S.C., Section 552<br>- General Records Schedule 5.6: Security Records<br>- 2017 Insider Threat Guide<br>- M-07-16, Safeguarding Against and Responding to the Breach of PII<br>- Civil Liberties FAQ<br>- Privacy Act of 1974<br>- (U) U.S. Insider Threat Security Classification Guide V.1, Dec 2013<br>- CDSE: DoD Insider Threat Program Best Practices, 1.1. Hub Hiring Rev 2, May 2017<br>- CDSE: Preserving Investigative and Operational Viability in Insider Threat, Sept 2017<br>- CDSE: Counterintelligence Awareness Job Aid, Foreign Collection Methods |

| Topic Area | References |
|---|---|
| **Topic Area 3 cont'd**: Researching (20%)<br>Sub-Topic Areas:<br>• Information Protection<br>• Investigative and Operational Viability<br>• Counterintelligence (CI) Pillar<br>• Cyber Pillar<br>• Human Resources (HR) Pillar<br>• Law Enforcement (LE) Pillar<br>• Legal Pillar<br>• Behavioral Science Pillar<br>• Security Pillar | • Executive Order 12333, US Intelligence Activities<br>• FBI: Elicitation Techniques<br>• National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov 2012<br>• CDSE: Cybersecurity for Security Personnel, Sept 2017<br>• DoD 5220.22-M, National Industrial Security Program Operating Manual, May 2016<br>• DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, Jul 2017<br>• CDSE: Establishing an Insider Threat Program for Your Organization<br>• Stiennon, R. (2013). Grasping the Problem with Privileged Accounts.<br>• DoDI 1400.25, Vol 431, DoD Civilian Personnel Management System: Performance Management and Appraisal Program, Jul 2019<br>• CDSE: Insider Threat Records Checks INT230.16<br>• Band et al., (2006). Comparing insider threat IT sabotage and espionage: A model-based analysis. |
| **Topic Area 4**: Synthesis & Tools and Methods (35%)<br>Sub-Topic Areas:<br>• All-Source Insider Threat Assessment<br>• All-Source Insider Threat Referral Triage<br>• All-Source Insider Threat Trend Analysis<br>• Analytic Communication<br>• Critical Thinking Techniques<br>• Databases and Data Feeds<br>• DITMAC System-of-Systems (DSoS)<br>• Structured Analytic Techniques | • EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information<br>• Why employee training matters: negligent users are top insider threat<br>• CDSE: Developing a Multidisciplinary Insider Threat Capability<br>• Intelligence Community Directive 203: Analytic Standards<br>• 2017 Insider Threat Guide<br>• Splunk: Quick Reference Guide<br>• A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis<br>• NIST Special Publication 800-160, Systems Security Engineering<br>• NIST Special Publication 800-64, Information Security<br>• CDSE: Insider Threat Records Checks: Student Guide, 2017 |

| Topic Area | References |
|---|---|
| | • CDSE: DoD Insider Threat Management Analysis Center (DITMAC): Student Guide, 2016<br>• DCSA: DoD Insider Threat Management and Analysis Center (DITMAC)<br>• Privacy Act of 1974: System of Records<br>• |
| **Topic Area 5**: Vulnerabilities Assessment and Management (15%)<br>Sub-Topic Areas:<br>• Insider Threat Mitigation: Individual<br>• Insider Threat Mitigation: Organizational | • CDSE: Insider Threat Mitigation Responses INT210.16<br>• CDSE: Insider Threat Mitigation Responses: Student Guide, 2017<br>• 2017 Insider Threat Guide<br>• Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats. |

# Appendix D: Waiver Request Form

| | | | |
|---|---|---|---|
| Name: | | | |
| Employer: | | | |
| Work Email: | | | |
| Current Expiration Date: | | New Expiration Date Requested: | |
| Date Waiver Submitted: | | | |
| REASON FOR WAIVER | | | |
| □ Medical | □ Military Deployment | □ Other | |
| Explain the reasons for the request for this waiver. (Limit 1,000 words)<br>(Please attach all pertinent documentation with the initial submission so your waiver request can be properly reviewed.) | | | |
| | | | |
| **ACTION TAKEN** (For PMO Only) | | | |
| □ Waiver is approved | | | |
| □ Waiver is rejected | | | |
| □ Return – Incomplete information in the waiver request/additional information is requested.<br>Submit no later than: | | | |
| Comments: | | | |

C-InT PMO Signature: ________________________________________

Date: ____________________

## Appendix E: Appeal Request Form

Date Appeal Submitted:

| | | | |
|---|---|---|---|
| Name: | | | |
| Employer: | | | |
| Work Address: | | | |
| City/State/Zip: | | | |
| Unit (if applicable): | | Work Telephone #: | |
| Work Email: | | Employer POC: | |
| Employer POC Email: | | Employer POC Phone #: | |

| | |
|---|---|
| REASON FOR APPEAL | |
| Date of appealable event: | |
| □ Examination Results | □ Certification maintenance and professional development units (PDUs) |
| □ Candidate Registration/Eligibility | □ Certification disciplinary matters |
| □ Test-Taking Protocols | □ Decisions related to alleged cheating, alleged violation of professional rules of conduct, or inaccurate information on the application form |
| Explain the basis of the appeal. (Limit 1,000 words) | |
| | |
| Attach all pertinent documentation with the initial submission so your appeal can be properly reviewed. (Please indicate the type of documentation submitted – check all that apply. | |
| □ Score Report | □ Disciplinary Violation Report |
| □ Medical Form | □ Alleged Cheating Defense |
| □ Complaint Form | □ Other |
| **ACTION TAKEN** (For PMO Only) | |
| □ Forward to the Certification Appeals Board | |
| □ Reject the appeal:<br>□ Insufficient ground for appeal<br>□ Missed deadline for appeals submission | |
| □ Return – Incomplete information in the appeals submission | |
| | |
| Comments: | |

Reviewer: Date:

# Appendix F: CCITP PDU Reference Table

| Category | Event Type | PDU Rate | Max PDU/Event | Max PDU/Category |
|---|---|---|---|---|
| **Training & Education** | Training Events | 1 PDU per Contact Hour | 45 PDUs per Event | 100 PDUs |
| | Conferences | 1 PDU per Contact Hour | 45 PDUs per Event | 100 PDUs |
| | Certifications: | | | |
| | - Higher CCITP Certification | 100 PDUs per Certification | 100 PDUs per Certification | 100 PDUs |
| | - CCITP related Certification | 45 PDUs per Certification | 45 PDUs per Certification | 100 PDUs |
| | - Non-CCITP related Certification | 45 PDUs per Certification | 45 PDUs per Certification | 25 PDUs (F)<br>50 PDUs (A) |
| **Giving Back to the Community** | Teaching, Training, & Presenting | 3 PDUs per Contact Hour | 45 PDUs per Event | 100 PDUs |
| | Mentoring | 1 PDU per Contact Hour | 45 PDUs per Event | 100 PDUs |
| | Workshops & Working Groups | 1 PDU per Contact Hour | 45 PDUs per Event | 100 PDUs |
| **Unique Work Experiences** | Cross-Hub Experience | 1 PDU per Contact Hour | 45 PDUs per Event | 100 PDUs |
| | Publications: | | | |
| | - Monographs/ Scholarly Book: | 45 PDUs | 45 PDUs | 100 PDUs |
| | - Dissertation/Thesis | 50 PDUs | 50 PDUs | 100 PDUs |
| | - Chapter of a book | 25 PDUs | 25 PDUs | 100 PDUs |
| | - Publication Article | 25 PDUs | 25 PDUs | 100 PDUs |
| | - Book Review | 25 PDUs | 25 PDUs | 100 PDUs |
| | - Newsletter Article | 10 PDUs | 10 PDUs | 100 PDUs |
| | - Newsletter Editor | 5 PDUs | 5 PDUs | 100 PDUs |
| | Special Projects | 1 PDU per Contact Hour | 45 PDUs per Event | 45 PDUs |