Certified Counter-Insider Threat Professional (CCITP) Program

Candidate Handbook

Spring 2021

The Certified Counter-Insider Threat Professional (CCITP) Program is sponsored by the Department of Defense (DoD), Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and National Insider Threat Task Force (NITTF) at the Office of the Director of National Intelligence (ODNI). The CCITP Program is governed by the CCITP Governance Council (CCITP GC), the chair of which is the Director, DoD Counter-Insider Threat (C-InT) Program and the co-chair is the Director, NITTF. The CCITP Program Management Office (CCITP 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 1.4

Spring 2021 CCITP Testing Timeline	
Candidate Registration	Begins February 19, 2021, Ends March 12, 2021
Program Reviewer Approvals	Begins February 19, 2021, Ends April 2, 2021
CCITP Testing Available	Begins April 16, 2021, Ends May 30, 2021

Revisions to Candidate Handbook

Change	Version
Update name of OUSD(I&S) to reflect recent change; change made throughout document.	1.1
Clarified that Certificants will receive a printable PDF certificate in addition to digital badge.	1.1
Update to Terms and Conditions regarding the distribution of conferral lists.	1.1
Clarification that exam content, exam passing standard, and exam results are not eligible for appeals by candidates.	1.1
Updates to include administrative clarifications to improve document utility.	1.2
Updates to include administrative clarifications to improve document utility.	1.3
Updates to include administrative clarifications and Spring 2021 testing window dates.	1.4

Table of Contents

Program Overview

Introduction

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

- 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 (EO) 13587 in 2011. The EO 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 EO also established the National Insider Threat Task Force (NITTF) as the government-wide means for assisting Departments and Agencies as they develop and implement their own C-InT programs. Since the signing of the EO, responses from the Executive Level Departments and Agencies across the U.S. federal government have varied. In 2017, the NITTF began partnering with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) as part of an ongoing effort to bring all Departments and Agencies into compliance with the EO as well as to standardize and professionalize the C-InT workforce across the federal government.

On October 30, 2018, the OUSD(I&S), 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 applies to all C-InT programs within Departments and Agencies across the U.S. federal government. This effort was made possible by the partnership between the Under Secretary of Defense for Intelligence and Security (USD(I&S)) 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&S) and the Director of NCSC serve as the joint conferral authorities for the CCITP Program.

CCITP-F Certification

The CCITP-F certification is a foundational certification designed at the lower levels of Bloom's taxonomy (i.e., Remember and Understand) to measure and assess whether an individual has the

requisite knowledge and skills as annotated within the CCITP-Essential Body of Knowledge (CCITP-EBK) to perform the tasks outlined in the CCITP-Essential Body of Work (CCITP-EBW). The CCITP-F was designed with a target population of those personnel working directly in a C-InT program; however, because each program is unique with 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 organization's Program Manager. The CCITP-F is a pass/fail exam with 115 multiple-choice questions (100 scored, 15 unscored), measuring acceptable performance across the following topic areas:

- Policy and Directives – 25%
- Social and Behavior Science – 10%
- Researching – 30%
- Synthesis & Tools and Methods – 35%

CCITP-A Certification

The CCITP-A certification is an applied certification designed at the middle levels of Bloom's taxonomy (i.e., Apply and Analyze) and establishes a common standard of analytic tradecraft of all who serve and support the C-InT capability; it focuses on the analysis of C-InT information and development of mitigation recommendations. The CCITP-A measures and assess whether an individual has the requisite knowledge and skills annotated in the CCITP-EBK to perform tasks outlined in the CCITP-EBW. The CCITP-A was designed for the target population of those personnel working directly in a C-InT program and performing analysis functions. The CCITP-A is a pass/fail exam with 100 scenario-based multiple-choice questions (85 scored, 15 unscored), measuring acceptable performance across the following topic areas:

- Policy and Directives – 20%
- Social and Behavior Science – 10%
- Researching – 20%
- Synthesis & Tools and Methods – 35%
- Vulnerabilities Assessment – 15%

Certification Benefits

Benefits of obtaining a CCITP certification include:

For Individuals:
- Fosters understanding of the concepts and principles deemed critical to perform C-InT 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 Governance Council (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 GC 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 chaired by the Director, DoD C-InT Program who represents the interests of the DoD, and co-chaired by the Director, NITTF, who represents the interests of the broader U.S. government. The Chair and Co-Chair are supported by a group of twelve (12) voting members comprised of senior-level stakeholders from across the federal government, along with one CCITP Certified Member and one Public Member.

The Chair and Co-Chair 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 executed. The CCITP Program Management Office (CCITP PMO) assists the Chair, the Co-Chair and the CCITP GC as a whole to ensure that the 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 conducted 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 Chair, the Co-Chair and all current active voting members. Closed meetings are designed to discuss sensitive programmatic or administrative decisions (e.g., exam specific issues, waiver/appeal requests, disciplinary issues, etc.). Open Meetings are designed to discuss general program updates and provide a forum for non-voting stakeholders to bring issues or suggestions to the CCITP GC.

Exam Development

The CCITP Program exams, the CCITP-F and CCITP-A, were developed using a two-stage process. Stage one included conducting a practice analysis to codify the C-InT community's skill standard. The C-InT community's skill standard is characterized by two documents, the CCITP-EBW and the CCITP-EBK. The CCITP-EBW describes what C-InT professionals need "to do" and the CCITP-EBK describes what they need "to know." Stage two involved executing the criterion-referenced test development (CRTD) process. The CRTD process involved five phases of exam developed:

> (1) generate a certification blueprint using the results of the practice analysis (i.e., the final CCITP skill standard),

(2) developing draft exam questions that assess mastery of content identified in the exam's blueprint,

(3) reviewing the drafted exam questions,

(4) pilot testing an "Alpha" version of the exam and generating a production exam version, and

(5) establishing the exam's cut-score.

Each phase of the CRTD process was performed under the guidance of Industrial/Organizational (I/O) psychologists and psychometricians (i.e., exam development experts). The CCITP-F and CCITP-A blueprints and exam questions were developed by a team of Subject Matter Experts (SMEs) from the C-InT enterprise (including federal government and DoD departments, agencies, and components) to assess the candidate's mastery of the knowledge and skill requirements, identified by the practice analysis, and defined and described in the CCITP-EBK. Following the development of the exam blueprints and draft exam questions, the team of SMEs reviewed all exam questions for accuracy and relevance to the content outlined in the CCITP-EBK. This process ensured questions and answers were correct, had the appropriate difficulty for the respective exam (i.e., CCITP-F or CCITP-A), contained neither trivia nor 'trick questions,' and were appropriate for both federal government and DoD audiences. Finally, two over-length exams were pilot tested by a large group of C-InT professionals. After the pilot exams were complete, exam development experts analyzed each exam and their corresponding questions to identify the best questions for the final versions of each exam. These final exam versions were presented to a group of SMEs representative of the C-InT enterprise to develop the passing scores, and ultimately presented to the CCITP GC for approval. The CCITP GC approved exams and passing scores were adopted by the CCITP Program and launched in fall 2019.

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 CCITP PMO also assists in making adjustments to the exam questions, as necessary. The CCITP PMO's I/O psychometricians will regularly review the performance of each exam and its questions to ensure that the questions are performing well and that the exam as a whole is performing effectively. During the review of each exam, additional questions may be generated and reviewed in order to bolster exam performance and ensure the exam content is current.

Determining Passing Score

The Modified Angoff method, a widely used standard-setting approach in exam development, was used to set the minimum passing score for each CCITP exam. The Modified Angoff method has a well-established history of determining credible passing standards for professional certification exam and was easily adopted by the CCITP Program. The process of setting the passing standards for each exam was performed by SMEs, guided by exam development experts, and approved by the CCITP GC.

The Modified Angoff method involves two basic elements: 1) conceptualization of a minimally acceptable candidate and 2) SMEs estimation of whether a minimally acceptable candidate will answer an exam question correctly. Minimally acceptable candidates are those who possess the

minimum qualification and knowledge to perform tasks associated with a job. The SMEs' predictions about the minimally acceptable candidate's performance on each exam question 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 CCITP-F certification are as follows:

- Candidates must be current C-InT Program or Affiliated Personnel Only
- Candidates must have a minimum of six (6) months experience working in/with a C-InT Program
- Candidates must complete a minimum of ten (10) hours of C-InT related training
- Candidates must receive Program Manager approval

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

Scoring the CCITP-F Exam

The CCITP-F exam is electronically delivered and 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 exam. While the CCITP-F exam has 115 multiple-choice question, a candidate's final overall score is only based on the 100 scored questions. The remaining 15 questions are unscored and added for piloting purposes; performance on these questions does not affect a candidate's overall score. Each question (scored and unscored) has only one correct answer that was validated during exam development by a representative group of SMEs from the C-InT Enterprise.

Candidates will have 130 minutes, or two (2) hours and ten (10) minutes to complete the 115 multiple-choice questions. The CCITP-F exam questions are linked to one of five (5) different topic areas that align to the CCITP-EBK.

CCITP-F Topic Areas:

- Topic Area 1: Policy and Directives – 25%
- Topic Area 2: Social and Behavioral Science – 10%
- Topic Area 3: Researching – 30%
- Topic Areas 4 & 5: Synthesis & Tools and Methods – 35%

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 two sections of information.

Section 1 provides information on a candidate's overall exam performance compared to the passing standard. Candidates are provided the passing standard (known as the performance threshold), their exam score, and a pass/did not pass result. Candidates exam score and pass/did not pass results are based on their performance on the 100 scored questions only.

Section 2 provides information on candidate performance on the exam's topic areas. To increase the reliability of feedback provided to candidates, topic areas are grouped into the following feedback groups:

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

Candidates should not view the feedback provided in Section 2 of their score report as definitive due to the small number of questions per section. Rather, candidates should use this as additional information to decide what next steps should be taken for professional development.

Following testing, candidates will have two methods of retrieving their results. Candidates will 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). Candidate's pass/did not pass result will also be recorded in their candidate profile on the candidate registration system within 24 hours of testing.

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. The candidate will also be required to apply as a new candidate and complete the registration process again (completing the application, receiving approval and prioritization from the candidate's organization's Program Manager, submitting a request to the test center of choice) each time they attempt to retest.

Use of CCITP-F Credentials

Candidates who pass the CCITP-F exam and are officially conferred will receive a letter, a printable PDF certificate, 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 GC 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 purpose of the CCITP-F maintenance requirements are to ensure that certificants maintain and/or improve the level of knowledge and skill in the C-InT mission which they initially demonstrated by passing the CCITP-F exam. The requirements listed below support this purpose by ensuring that certificants continue to participate in activities that are designed to keep them up to date on changes within the profession (specifically those changes related to policy, technology, and tradecraft). Each of the CCITP-F maintenance requirements were developed and recommended by a group of senior C-InT SMEs who believed that these requirements were appropriate and sufficient to allow certificants the flexibility to choose the maintenance activities that they felt best suited their individual and professional development needs while also ensuring that certificants participated in a variety of maintenance activities sufficient to stay current in all of the areas of the profession where changes may have occurred. These requirements were then reviewed and approved by the CCITP GC prior to the launch of the program.

The CCITP-F certification is valid for a period of two (2) years[1] 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 obtain 100 PDUs over the course of their 2-year maintenance cycle in order to successfully maintain their CCITP-F certification. 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.

---

[1] If a candidate has CCITP-A, then CCITP-F will follow CCITP-A certification maintenance timeline.

Recertification

In order for a certificant to adequately demonstrate that they have met the CCITP-F maintenance requirements, a certificant must submit a PDU Tracking Form to the CCITP PMO prior to the last day of their maintenance cycle. The CCITP PMO will review all CCITP-F PDU Tracking Forms to ensure that they are complete and will audit between ten and twenty percent (10 - 20%) of all CCITP-F PDU Tracking Forms submitted each cycle to ensure that the activities documented were actually attended/completed by the individuals claiming credit for them. The CCITP-F PDU Tracking Form can be found on the CCITP website here: https://dodcertpmo.defense.gov/Counter-Insider-Threat/Resource-Documents/.

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 CCITP-A certification are as follows:

- Certificants must currently hold the CCITP-F certification
- Certificants must be current C-InT Program Personnel
- Certificants must have a minimum of 12 months working in a C-InT Program
- Certificants must complete a minimum of 40 hours of Analysis-related training
- Certificants must complete a minimum of eight (8) hours of UAM policy and/or tool-related training
- Certificants must review at least ten (10) Case Studies
- Candidates must receive Program Manager approval

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

Scoring the CCITP-A Exam

The CCITP-A exam is electronically delivered and 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. While the CCITP-A exam has 100 multiple-choice questions, a candidate's final overall score is only based on the 85 scored questions. The remaining 15 questions are unscored added for piloting purposes; performance on these questions does not affect a candidate's overall score. Each question (scored and unscored) has only one correct answer that was validated during exam development by a representative group of SMEs from the C-InT Enterprise.

Candidates will have 160 minutes or two (2) hours and forty (40) minutes to complete 100 scenario-based multiple-choice questions. The CCITP-A exam questions are linked to one of six (6) different topic areas that align to the CCITP-EBK.

CCITP-A Topic Areas:

- Topic Area 1: Policy and Directives – 20%
- Topic Area 2: Social and Behavioral Science – 10%
- Topic Area 3: Researching – 20%
- Topic Areas 4 & 5: Synthesis & Tools and Methods – 35%
- Topic Area 6: Vulnerabilities Assessment – 15%

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 two sections of information.

Section 1 provides information on a candidate's overall exam performance compared to the passing standard. Candidates are provided the passing standard (known as the performance threshold), their exam score, and a pass/did not pass result. Candidates exam score and pass/did not pass results are based on their performance on the 85 score questions only.

Section 2 provides information on candidate performance on the exam's topic areas. To increase the reliability of feedback provided to candidates, topic areas are grouped into the following feedback groups:

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

Candidates should not view the feedback provided in Section 2 of their score report as definitive due to the small number of questions per section. Rather, candidates should use this as additional information to decide what next steps should be taken for professional development.

Following testing, candidates will have two method of retrieving their results. Candidates will 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). Candidate's pass/did not pass result will also be recorded in their candidate profile on the candidate registration system within 24 hours of testing.

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. The candidate will also be required to apply as a new candidate and complete the registration process again (completing the application, receiving approval and prioritization from the candidate's organization's Program Manager, submitting a request to the test center of choice) each time they attempt to retest.

Use of CCITP-A Credentials

Candidates who pass the CCITP-A exam and are officially conferred will receive a letter, a printable PDF certificate, 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 GC 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 purpose of the CCITP-A maintenance requirements are to ensure that certificants maintain and/or improve the level of knowledge and skill required to perform the analytic function of the C-InT mission which they initially demonstrated by passing the CCITP-A exam. The requirements listed below support this purpose by ensuring that certificants continue to participate in activities that are designed to keep them up to date on changes within the profession (specifically those changes related to policy, technology, and tradecraft). Each of the CCITP-A maintenance requirements were developed and recommended by a group of senior C-InT SMEs who believed that these requirements were appropriate and sufficient to allow certificants the flexibility to choose the maintenance activities that they felt best suited their individual and professional development needs while also ensuring that certificants participated in a variety of maintenance activities sufficient to stay current in all of the areas of the profession where changes may have occurred. These requirements were then reviewed and approved by the CCITP GC prior to the launch of the program.

The CCITP-A certification is valid for a period of three (3) 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 obtain 100 PDUs over the course of their 3-year maintenance cycle in order to successfully maintain their CCITP-A certification. The 100 PDUs are 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.

Recertification

In order for a certificant to adequately demonstrate that they have met the CCITP-A maintenance, a certificant must submit a PDU Tracking Form to the CCITP PMO prior to the last day of their maintenance cycle. The CCITP PMO will review all CCITP-A PDU Tracking Forms to ensure that they are complete and will audit between ten and twenty percent (10 - 20%) of all CCITP-A PDU Tracking Forms submitted each cycle to ensure that the activities documented were actually attended/completed by the individuals claiming credit for them. The CCITP-A PDU Tracking Form can be found on the CCITP website here: https://dodcertpmo.defense.gov/Counter-Insider-Threat/Resource-Documents/.

Registration and Application

Candidates interested in taking either CCITP 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 registration system and complete 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 application within the candidate registration system. The application will then be sent to the candidate's organization's C-InT Program Manager for validation and approval. Once approved by the candidate's organization's C-InT Program Manager, candidates will be contacted by the CCITP PMO with approval to test and instructions for scheduling an exam.

NOTE 1: Candidate or certificant information, to include personally identifiable information (PII) is not shared with anyone outside of the specified CCITP Program personnel except in aggregate as part of the program's exam analysis and performance reporting, unless specifically authorized in writing by the candidate/certificant specifying what information they want shared and with whom.

NOTE 2: The Program Manager 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 Program Manager, they should first contact their Program Manager and discuss the issue with them. If they are unable to resolve the issue with their Program Manager, the candidate may submit an appeal to the CCITP PMO in writing (for further details on this process, see the Appeals Policy).

The exams are delivered electronically 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 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 either of the CCITP exams, they must 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 exam 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 must 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 administering the exam for the requesting party.

The CCITP PMO, along with the test center 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 and statement of reasons of 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. Furthermore, the CCITP Program is not based on nor measures organization-specific operations or procedures. Participation in the CCITP Program 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 the CCITP-EBK for the respective certification they are considering. The CCITP-EBK contains a listing of the knowledge areas a practitioner within the C-InT workforce is expected to possess. Appendix B contains the knowledge domains within the CCITP-EBK relevant to the CCITP-F exam along with all relevant sources. Appendix C contains the knowledge domains within the CCITP-EBK relevant to the CCITP-A exam along with all relevant sources.

<u>Testing Tips:</u>
Consider the following when preparing for one of the CCITP exams:

- Relax before the exam.

- 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., CCITP-EBK and exams) 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 session 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 the scheduled exam sessions. For more information on how to submit a waiver, see the Waiver Policy section.

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 two (2) original (no copies or digital IDs), valid (unexpired) forms of identification with them to the testing center; one must be a primary form of identification (government-issued with a full name, photo, and signature) and a second form of identification, containing a full name and signature, or full name and photo. Candidates will not be permitted to take an exam without proper identification. Test center proctors will verify candidate identification, to include U.S. citizenship (e.g., U.S. passport, or a birth certificate and a government-issued photo ID). 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 questions 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 questions, 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 (NDA) and a brief system tutorial. The exams will be offered electronically at any Pearson VUE testing center during selected testing 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 the exam session and to provide directions for taking the exam at the outset of the exam session but are not allowed to help candidates read or comprehend exam questions. During the administration of the exam, talking to anyone other than a proctor or administrator is not permitted. In addition, candidates are not permitted to discuss exam 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, the CCITP Program 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 processes 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 exams are For Official Use Only and are not authorized for public release.

Candidate and Certificant Confidentiality

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 exam 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 exam studies or reports will be aggregated and PII redacted.

The CCITP PMO provides, on a periodic basis, conferral lists to participating organizations. Conferral lists include certificant name, relevant certification, and conferral date. In addition, the CCITP PMO responds to conferral verification requests that are made in writing and provides 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.

Terms and Conditions

Each candidate who is registering to participate in the CCITP Program is required to accept the program's Terms and Conditions. The Terms and Conditions is presented to the candidate prior to submitting their program application, and states the following:

"Your participation in the Certified Counter-Insider Threat Professional (CCITP) Program is subject to the following terms and conditions.

The CCITP Program exams (including, without limitation, questions, answers, datasets, files, designs, or content in or related to the CCITP exam) are the property of the U.S. Department of Defense and access is reserved to authorized users only. The exams are for internal U.S. government use only and is not publicly releasable. By accessing and participating in the CCITP Program, you accept the responsibility to protect the integrity of the CCITP exams by not disclosing, disseminating, copying, publishing, or transmitting any parts of the exams in any form to any person without the expressed permission of the CCITP Program Management Office. You may be subject to disciplinary actions under agency or component standards of

conduct, disqualified from participating in the CCITP Program, and your CCITP certification may be revoked if you:

1. Participate in the CCITP Program under false identity.
2. Knowingly submit false information in this registration process.
3. Circumvent or violate the CCITP Program's procedures or security mechanisms."

Candidates refusing to accept the Terms and Conditions will not be permitted to move forward with their application and will not be able to participate in the CCITP Program.

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 the 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 meet program requirements. To be recommended for conferral, candidates must successfully meet all the certification eligibility requirements and meet or exceed the exam qualifying score. Candidates who meet these requirements will be conferred within 30 days of the close of their testing window. The CCITP PMO will notify the new certificants via email and award them their credentials. Certificants are responsible for ensuring that they complete all of their maintenance requirements starting from the official date of their conferral to the end of their maintenance period – two years for CCITP-F certificants, and three years for CCITP-A certificants (see the Maintenance sections for each CCITP certification above for the specific maintenance requirements). Certificants who complete their maintenance requirements within the allotted maintenance window will be re-conferred for another period, and their new maintenance window will reset and begin on the new conferral date.

Letters, printable PDF certificates, and digital badges will be issued to signify the CCITP credential. Information on how to access the certificant's digital badge is 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 maintains a record of the digital badges with attendant metadata. This metadata includes the issuer's names (the USD(I&S) 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 also specifies 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). 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 with whom the certificant provides his/her unique badge URL. The badge serves as proof of the certificant's conferral status.

The CCITP PMO maintains 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 apply as a new candidate and meet all of the requirements in place at the time of re-application, to include retaking both 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 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 organization's Program Manager to deny a candidate's admission to the CCITP Program, to terminate participation at any stage throughout the conferral process, or to invalidate the result of an exam. In the case of a certificant, the individual may have their certification(s) revoked and be barred from re-entry into the CCITP 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 exam; obtaining or attempting to obtain copies of the exam 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 exam.
2. **Exam compromise**. Actions that compromise the integrity of the CCITP exams, including but not limited to unauthorized possession of or access to real exam questions;

copying any portion of a CCITP 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 and/or maintain 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 using the Suspected Violation Report in Appendix G by any interested party to the test proctor, the organization Program Manager, 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 Program Manager 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 certification.
- 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, exams, and other registration/exam-related certification issues or challenges.

Grounds for Appeal

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

- Candidate registration protocols (that is determination of eligibility).
- 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:

- Examination results and/or criteria for obtaining a passing score on CCITP exams
- Certification waiver decisions
- Employment policy
- Eligibility criteria for identifying billets or individuals requiring CCITP certification
- Exam content

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

Appeals Process

Individuals have up to 15 business days from the date of receiving an appealable decision or after completing the exam, 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 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 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 CCITP GC 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. • 10 hours C-InT specific Training • Program Manager/Hub Chief Approval	Pass the Exam	2 years	PDUs: • 75 - C-InT specific • 25 -Personal & Professional Growth Categories (with set Minimums & Maximums): • Training, Education, & Presentations • Giving back to the Community, • Unique Work Experiences
CCITP-A Certification	• Passed C-InT Fundamentals • Hub/Prog. Personnel only	• 12 months working in Hub/Prog. • 40 hours (minimum) Analysis-related training • 8 hours (minimum) User Activity Monitoring (UAM) policy and/or tool-related training • Review 10 Case Studies from 5 different categories • Program Manager/Hub Chief Approval	Pass the Exam	3 years	PDUs: • 50 - C-InT specific • 50 -Personal & Professional Growth Categories (with set Minimums & Maximums): • Training, Education, & Presentations • Giving back to the Community, • Unique Work Experiences

Appendix B: CCITP-Essential Body of Knowledge for the CCITP-F Exam

The CCITP-Essential Body of Knowledge (CCITP-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 CCITP-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 questions for the CCITP-F exam.

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

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

Topic Area	References
Topic Area 3 cont'd: Researching (30%) Sub-Topic Areas: • Information Protection • Investigative and Operational Viability • Counterintelligence (CI) Pillar • Cyber Pillar • Human Resources (HR) Pillar • Law Enforcement (LE) Pillar • Legal Pillar • Behavioral Science Pillar • Security Pillar	• CDSE: Counterintelligence Awareness Job Aid, Foreign Collection Methods • Executive Order 12333, US Intelligence Activities • FBI: Elicitation Techniques • National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov 2012 • CDSE: Cybersecurity for Security Personnel, Sept 2017 • DoD 5220.22-M, National Industrial Security Program Operating Manual, May 2016 • DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, Jul 2017 • CDSE: Establishing an Insider Threat Program for Your Organization • Stiennon, R. (2013). Grasping the Problem with Privileged Accounts. • DoDI 1400.25, Vol 431, DoD Civilian Personnel Management System: Performance Management and Appraisal Program, Jul 2019 • CDSE: Insider Threat Records Checks INT230.16 • Band et al., (2006). Comparing insider threat IT sabotage and espionage: A model-based analysis.
Topic Areas 4 & 5: Synthesis & Tools and Methods (35%) Sub-Topic Areas: • All-Source Insider Threat Assessment • All-Source Insider Threat Referral Triage • All-Source Insider Threat Trend Analysis • Analytic Communication • Critical Thinking Techniques • Databases and Data Feeds • DITMAC System-of-Systems (DSoS) • Structured Analytic Techniques	• EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information • Why employee training matters: negligent users are top insider threat • CDSE: Developing a Multidisciplinary Insider Threat Capability • Intelligence Community Directive 203: Analytic Standards • 2017 Insider Threat Guide • Splunk: Quick Reference Guide • A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis • NIST Special Publication 800-160, Systems Security Engineering • NIST Special Publication 800-64, Information Security • CDSE: Insider Threat Records Checks: Student Guide, 2017

Topic Area	References
Topic Areas 4 & 5 cont'd: Synthesis & Tools and Methods (35%)	• CDSE: DoD Insider Threat Management Analysis Center (DITMAC): Student Guide, 2016 • DCSA: DoD Insider Threat Management and Analysis Center (DITMAC) • Privacy Act of 1974: System of Records

UNCLASSIFIED

Appendix C: CCITP-Essential Body of Knowledge for the CCITP-A Exam

The CCITP-Essential Body of Knowledge (CCITP-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 CCITP-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 questions for the CCITP-A exam.

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

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

Topic Area	References
Topic Area 3 cont'd: Researching (20%) Sub-Topic Areas: • Information Protection • Investigative and Operational Viability • Counterintelligence (CI) Pillar • Cyber Pillar • Human Resources (HR) Pillar • Law Enforcement (LE) Pillar • Legal Pillar • Behavioral Science Pillar • Security Pillar	• Executive Order 12333, US Intelligence Activities • FBI: Elicitation Techniques • National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov 2012 • CDSE: Cybersecurity for Security Personnel, Sept 2017 • DoD 5220.22-M, National Industrial Security Program Operating Manual, May 2016 • DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, Jul 2017 • CDSE: Establishing an Insider Threat Program for Your Organization • Stiennon, R. (2013). Grasping the Problem with Privileged Accounts. • DoDI 1400.25, Vol 431, DoD Civilian Personnel Management System: Performance Management and Appraisal Program, Jul 2019 • CDSE: Insider Threat Records Checks INT230.16 • Band et al., (2006). Comparing insider threat IT sabotage and espionage: A model-based analysis.
Topic Areas 4 & 5: Synthesis & Tools and Methods (35%) Sub-Topic Areas: • All-Source Insider Threat Assessment • All-Source Insider Threat Referral Triage • All-Source Insider Threat Trend Analysis • Analytic Communication • Critical Thinking Techniques • Databases and Data Feeds • DITMAC System-of-Systems (DSoS) • Structured Analytic Techniques	• EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information • Why employee training matters: negligent users are top insider threat • CDSE: Developing a Multidisciplinary Insider Threat Capability • Intelligence Community Directive 203: Analytic Standards • 2017 Insider Threat Guide • Splunk: Quick Reference Guide • A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis • NIST Special Publication 800-160, Systems Security Engineering • NIST Special Publication 800-64, Information Security • CDSE: Insider Threat Records Checks: Student Guide, 2017

Topic Area	References
	• CDSE: DoD Insider Threat Management Analysis Center (DITMAC): Student Guide, 2016 • DCSA: DoD Insider Threat Management and Analysis Center (DITMAC) • Privacy Act of 1974: System of Records •
Topic Area 6: Vulnerabilities Assessment and Management (15%) Sub-Topic Areas: • Insider Threat Mitigation: Individual • Insider Threat Mitigation: Organizational	• CDSE: Insider Threat Mitigation Responses INT210.16 • CDSE: Insider Threat Mitigation Responses: Student Guide, 2017 • 2017 Insider Threat Guide • Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats.

UNCLASSIFIED

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)
(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.

Submit no later than:

Comments:

CCITP 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:	

☐ Candidate Registration/Eligibility	☐ Certification maintenance and professional development units (PDUs)
☐ Test-Taking Protocols	☐ Certification disciplinary matters
☐ 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:
     ☐ Insufficient ground for appeal
     ☐ 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) 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

Appendix G: Suspected Violation Report

COMPLAINTANT INFORMATION				
Full Name				
Employer				
Address				
City/State/Zip				
Email		Telephone #		
Signature		Date		
SUSPECTED INDIVIDUAL INFORMATION				
Full Name				
Address				
City/State/Zip				
Email Address		Telephone #		
Unit (if applicable)				
Employer		Employer POC		
Employer POC Email		Employer POC Telephone #		

REASON FOR VIOLATION REPORT	
Date of Violation Event	
☐ Cheating	☐ Misrepresentation or false statements
☐ Test Compromise	☐ Non-Compliance
☐ Request by the Certificant's parent organization	

EXPLAIN THE BASIS OF THE SUSPECTED VIOLATION (Limit 1,000 words)

WITNESS INFORMATION			
Full Name			
Address			
City/State/Zip			
Email Address		Telephone #	

FOR GOVERNANCE COUNCIL USE ONLY
Notes: