Certified Counter-Insider Threat Professional (CCITP) Program Candidate Handbook

SPēD PROGRAM MANAGEMENT OFFICE

CDSE Center for Development of Security Excellence

March 2025

CONTENTS

STARTING YOUR JOURNEY

Congratulations on your decision to pursue a Certified Counter-Insider Threat Professional (CCITP) certification!

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

PURPOSE OF THE HANDBOOK

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

NON-DISCRIMINATION STATEMENT

The CCITP program does not discriminate on the basis of age, race, color, ethnicity, religion, marital status, sex, national origin, handicapping condition, religion, political affiliation, or sexual orientation.

CONTACT INFORMATION

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

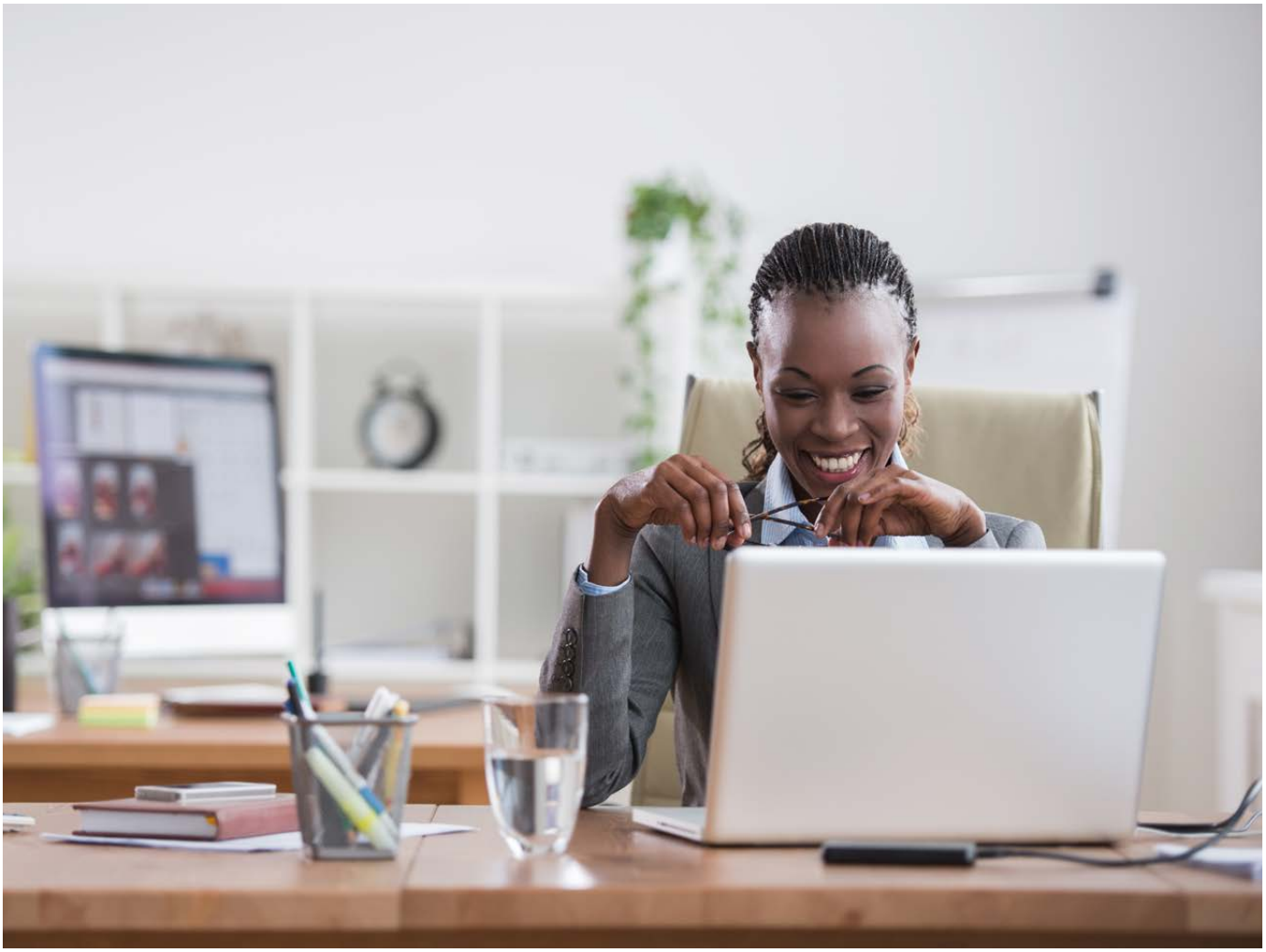
CCITP Program webpage:
https://www.cdse.edu/Certification/Certified-Counter-Insider-Threat-Professional-CCITP-Program/

CCITP Program Candidate Support:
dcsa.ncr.cdse.mbx.ccitp@mail.mil

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

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

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



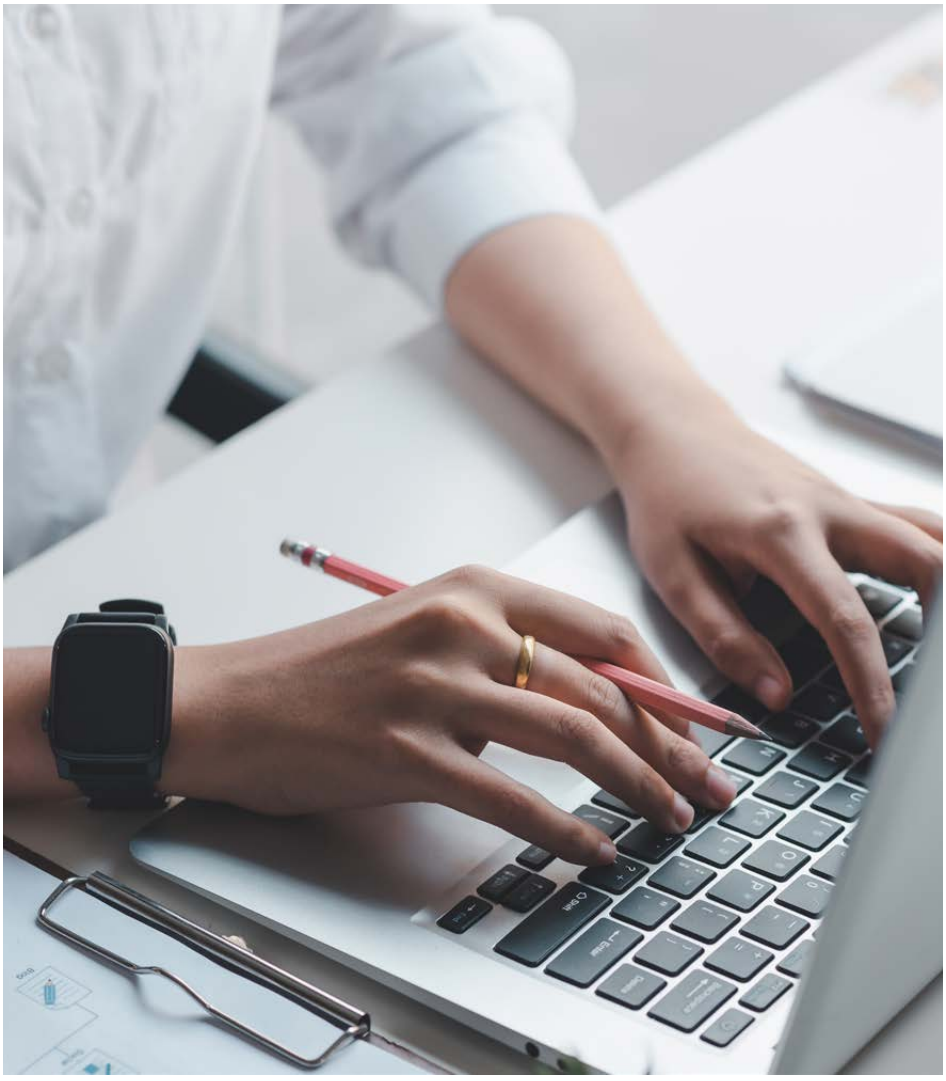
CCITP PROGRAM OVERVIEW

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 promote 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.



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

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.

Specifically regarding CCITP governance, the CCITP GC is responsible for:

- Certification administration oversight
- Technical development oversight
- Certification governance

CCITP-F CERTIFICATION

ELIGIBILITY AND PREREQUISITES

Eligibility defines who is allowed to participate in the program and challenge the exam. Prerequisites define what those individuals must do prior to being authorized to participate in the program or challenge the exam.

The Eligibility and Prerequisite 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 months experience working in/with a C-InT Program
- Candidates must complete a minimum of 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 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 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 110 multiple-choice question, a candidate's final overall score is only based on the 100 scored questions. The remaining 10 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 hours and ten minutes to complete the 110 multiple-choice questions. The CCITP-F exam questions are linked to one of five 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.

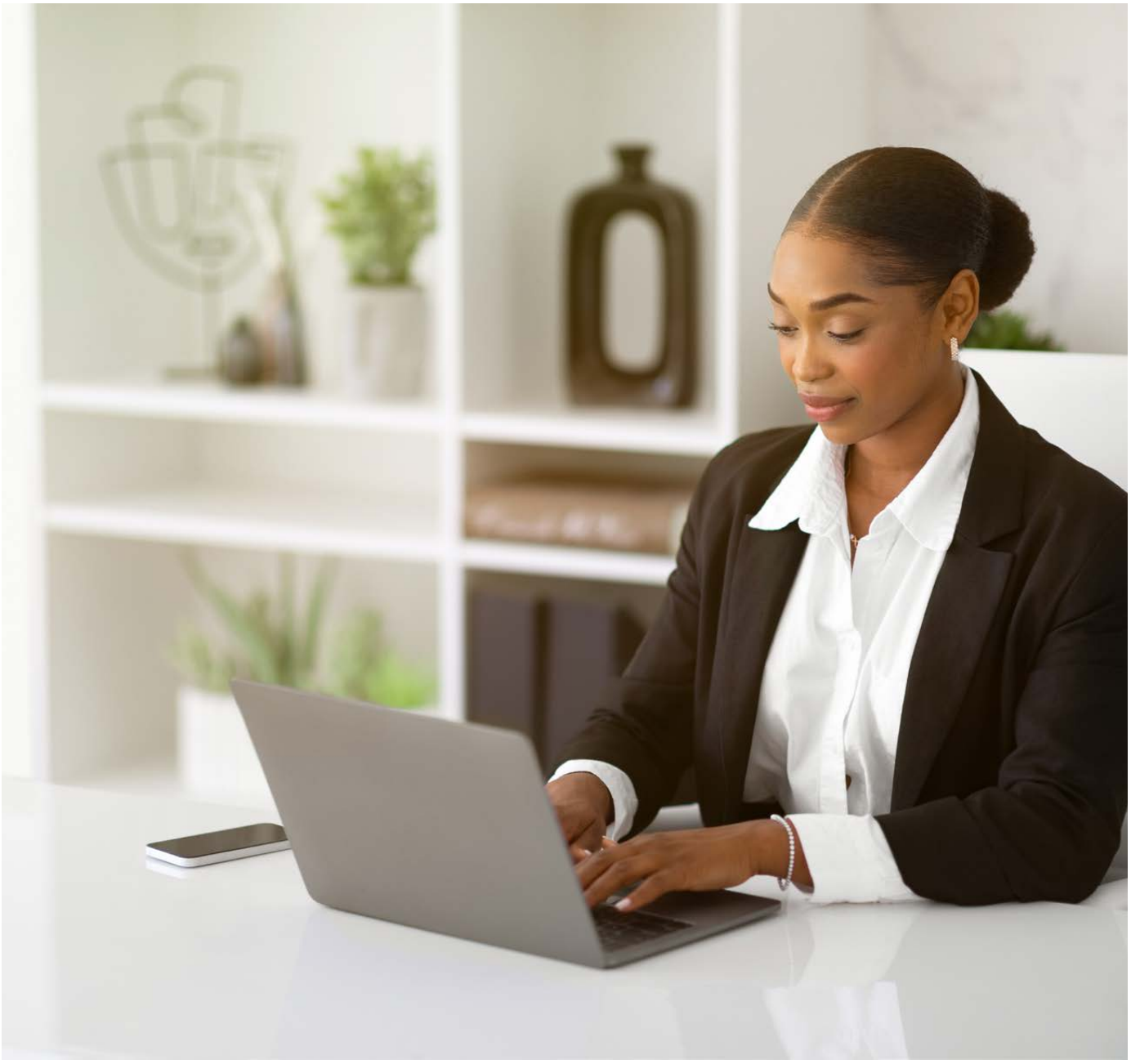
Section 1 provides information on a candidate's overall exam performance compared to the passing standard. Candidates are provided the passing standard (known as the performance threshold), their exam score, and a pass/did not pass result. Candidates' exam scores and pass/did not pass results are based 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). Candidates' pass/did not pass result will also be recorded in their candidate profile on the candidate registration system within 24 hours of testing.



CCITP-A CERTIFICATION

ELIGIBILITY AND PREREQUISITES

Eligibility defines who is allowed to participate in the program and challenge the exam. Prerequisites define what those individuals must do prior to being authorized to participate in the program or challenge the exam. The Eligibility and Prerequisite 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 hours of UAM policy and/or tool-related training
- Certificants must review at least 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 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 86 multiple-choice questions, a candidate's final overall score is only based on the 74 scored questions. The remaining 12 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 135 minutes or 2 hours and 15 minutes to complete 86 scenario-based multiple-choice questions. The CCITP-A exam questions are linked to one of six 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 scores 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 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). Candidates' pass/did not pass result will also be recorded in their candidate profile on the candidate registration system within 24 hours of testing.

CERTIFICATION AND CREDENTIALING

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 development:

1. generating 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 CCITPEBK. 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 SPēD 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. The SPēD 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 exams 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.

CERTIFICATION AND CREDENTIALING PROCESS

CANDIDATE MANAGEMENT PLATFORM

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

DEFENSE ACQUISITION UNIVERSITY (DAU)

CREATE AN ACCOUNT

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

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

ACCOUNT LOG IN

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

UPDATE USERNAME AND EMAIL ADDRESS

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

UPDATE ACCOUNT INFORMATION

1. Login to your DAU account at https://dau.csod.com/.
2. Hover your mouse over the Home tab at the top left and select Universal Profile.
3. Once the page loads, select the Edit User Record Form link at the top.
4. Locate the Organization section and click on the box with the "X." This will clear the field.
5. Select the box again and enter your agency in the search box and select the search button.
6. Results will display on the screen. Select the title associated with your organization and it will automatically be entered on your profile.
   NOTE: If no results populated after your search, select, "Cancel." Select the box again by Organization and use the page numbers and arrows at the bottom right to scroll through all of the available organizations. You will not be able to save your profile until an Organization has been selected.
7. Once complete, select "Submit" to save the changes.
8. Hover your mouse over the Home tab at the top left and select "Welcome" to return to the main screen.

RESET YOUR PASSWORD

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

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

PREPARING FOR AN ASSESSMENT

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 SPēD PMO is firewalled from participating in the design, development, or implementation of education, training, and similar content-focused programs. Candidates are advised that the SPēD 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.

ASSESSMENT-TAKING TIPS

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

ASSESSMENT ADMINISTRATION

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

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

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

Candidates will be provided with the following materials:

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

The following personal items are not permitted in testing rooms:

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

CERTIFICATION AND CREDENTIAL ENROLLMENT

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

SCHEDULE AN ASSESSMENT

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

1. Log in to your DAU account at https://dau.csod.com/.
2. Hover over the Learning tab and select "View Your Transcript."
3. On your Active tab, certifications and credentials that you are enrolled in will appear. Select "Manage" next to your certification to view all of the information.
4. Under "PearsonVue Exam" locate the certification or credential you wish to schedule and select "Launch."
5. Once the assessment launches, select "Next".
6. Read all of the information on the page and within 24 hours you will receive an email from Pearson Vue to schedule your assessment.
   NOTE: If the assessment does not appear on your transcript, wait 24 hours from your enrollment to allow the assessment authorization to process.

CANCEL OR RESCHEDULE AN ASSESSMENT

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

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

NO-SHOW

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

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

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

ACCOMMODATIONS FOR DISABILITIES

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

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

Accommodation types:

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

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

Candidates are responsible for seeking reasonable accommodations when completing the assessment enrollment form. Candidates should only select the reasonable accommodation that have been granted with supporting documentation. The supporting documentation should be sent directly to the CCITP Mailbox. Once the documentation for reasonable accommodation has been received, reviewed, and approved, the candidate will receive a confirmation email from DAU to schedule their assessment.

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

The SPēD PMO may request documentation from an appropriate health care or rehabilitation professional about a candidate's disability and functional limitations when the disability and need for accommodation is not obvious. Appropriate professionals include, but are not limited to, doctors (including psychiatrists), psychologists, nurses, physical therapists, vocational rehabilitation specialists, and licensed mental health professionals.

The need for, and the ability to, provide any specific accommodation is determined on an individual basis, depending on the unique circumstances involved and taken into consideration for a specific disability and the existing limitations in completing the certification process.

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

RETAKING AN ASSESSMENT

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

SCORING

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

FEEDBACK

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

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

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

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

These indicators also allow candidates to see which topic area(s) they performed well on, and which topic area(s) they can improve on. While this feedback may be helpful to candidates, it is suggested that candidates pursue improvement in all topic areas since this comparative performance metric is not definitive and subject to change based on those who take the assessment.

FEES ASSOCIATED
At this time, there are no fees associated with taking any CCITP assessments.

ASSESSMENT SECURITY AND CONFIDENTIALITY
CCITP assessment questions and answers are not subject to public release.

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

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

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

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

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

AFTER THE ASSESSMENT

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

USING CERTIFICATION OR CREDENTIAL ACRONYMS
Security Professionals who possess a CCITP Certification Program certification may use the appropriate acronym designation (CCITP-F or CCITP-A) on business cards, resumes, and signature lines. Designations can only be used while holding an active certification or credential.

DIGITAL CREDENTIALING

PLATFORM

Credly is the platform for all digital certifications and credentials.

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

ACCEPTING A DIGITAL BADGE

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

SHARING A DIGITAL BADGE

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

PRINTING A DIGITAL BADGE

Free Printing Option:

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

For Purchase Option:

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

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

GOVERNMENT AND PERSONAL EMAIL ADDRESSES

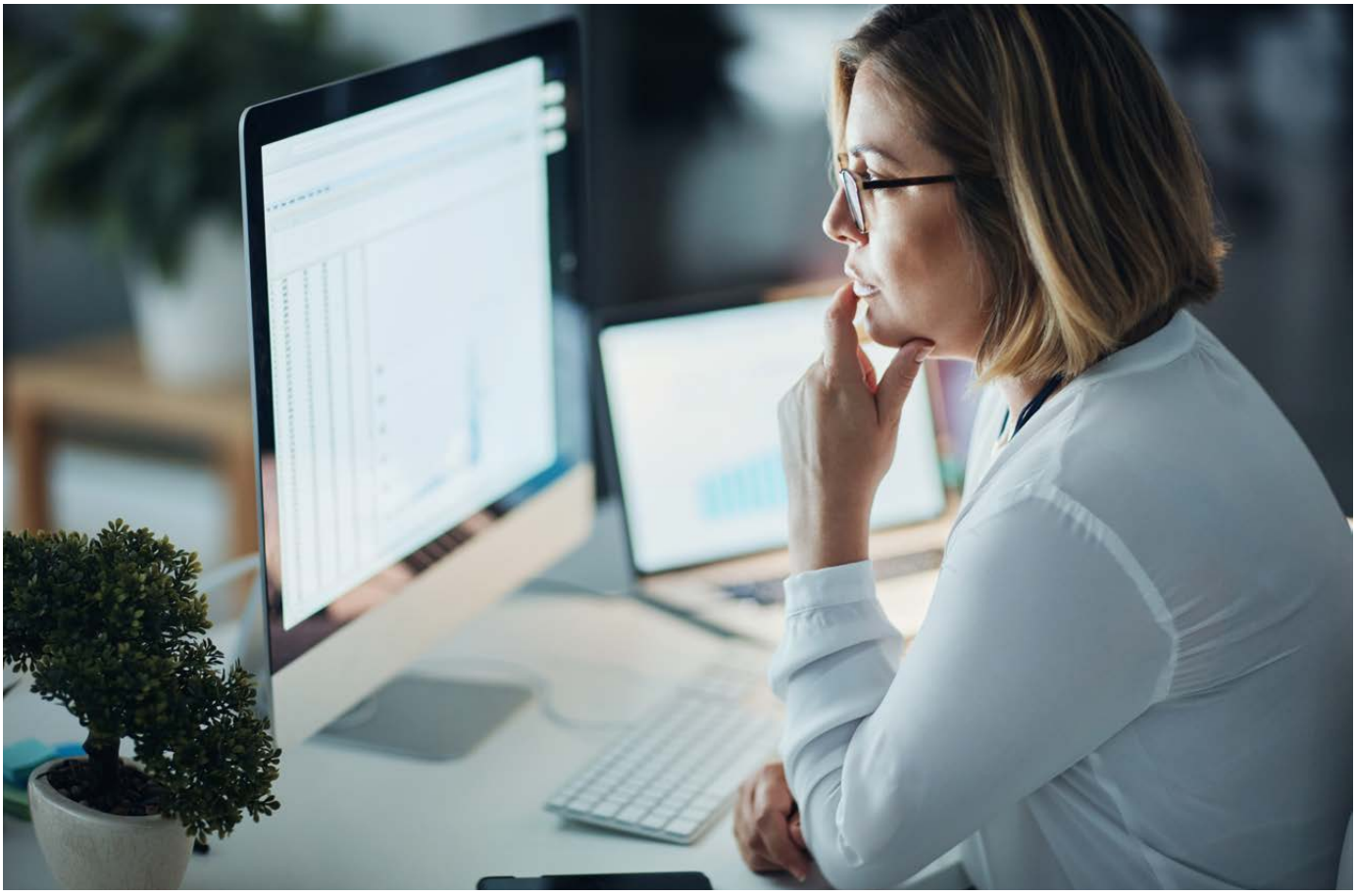
Certificants should ensure both government and personal emails are linked to your Credly account to receive all digital credentials within a DAU account. To link emails:

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

MERGE ACCOUNTS

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

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



MAINTAINING YOUR CERTIFICATION AND CREDENTIAL

CERTIFICATION RENEWAL PROGRAM

The purpose of the CCITP 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 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 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. This also ensures certificants participate 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 are then reviewed and approved by the CCITP GC prior to the launch of the program. CCITP certifications are valid for a period of two years from the date of conferral or most recent renewal activity.

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

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

The purpose of the Certification Renewal Program is to:

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

CERTIFICATION MAINTENANCE STANDARDS

1. The SPēD PMO manages the CCITP certification maintenance program and holds the below policies requiring a certification holder to:

   a. Maintain a certification by:
      - Maintaining an active and up-to-date DAU account
      - Successfully acquiring at least 100 PDUs within their two-year certification maintenance period , 50 of which must be C-InT related

   b. Coordinate waiver review and validation with employing Component, agency, or company to request a reasonable extension for reasons that could prohibit a certification holder from meeting certification maintenance requirements (e.g., deployments, hospitalization/medical leave, or other extraordinary reasons). All waivers must be submitted to the CCITP mailbox.
      - There will be no waivers submitted, accepted, or approved after expiration.

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

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

   a. Upon conferral of a new CCITP certification submission, and approval of the CRP, the new expiration date will update for all currently held certifications and credentials selected during the renewal process to the date of the most recently conferred certification.

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

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

   d. At least 50 of the 100 PDUs must be Counter Insider Threat (C-InT) related. The remaining PDUs do not have to be aligned with C-InT; however, they must satisfy one or more of the professional development categories identified in the PDU table.

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

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

Professional Development Unit (PDU) Categories

Category 1: Complete a Certification or Credential Program	
Category 1a: Obtain CCITP-A	• CCITP-F Certificants can receive 100 PDUs for being conferred a Obtain CCITP-A during their two-year certification maintenance cycle.
Category 1b: Obtain new security-related certification	• Certification holders can claim credit for up to 50 PDUs for each new security-related certification. All certifications must be security focused, nationally accredited, and gained during their two-year certification maintenance cycle. • A copy of the certificate must be uploaded as supporting documentation to receive PDUs in this category.
Category 2: Security-related Training, Certificate Programs, and/or Higher Education	
Category 2a: Security-related eLearning training courses	Consists of an organized series of planned learning experiences developed and delivered in an e-Learning environment, to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area. • Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training). • Awards a certificate of completion. • Certification holders can receive 1 PDU for each hour associated with an approved non-credit bearing training (all minutes past a full hour are rounded up to the next whole number, for example: anything under an hour rounds up to 1, 1 hour + 15 mins/1hour + 30 mins/1 hour + 45 mins are all rounded up to 2). • Certificants can claim credit for up to 100 PDUs in this category. • Annual training can only be used once per each two-year maintenance renewal window. • A certificate of completion must be uploaded to receive PDUs in this category.

Category 2b: Security-related instructor-led or virtually-led training courses	Consists of an organized series of planned learning experiences developed and delivered either in-person or virtually led, to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area.
	• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training).
	• Awards a certificate of completion.
	• Certification holders can receive 10 PDUs for each full-day (4 or more hours) for each day of instruction, or 5 PDUs for each half-day (1-4 hours) associated with an approved non-credit bearing training course.
	  ◦ VILT versions of an ILT will be awarded the same PDUs as that of the ILT version.
	  ◦ VILTs that do not currently have an ILT version will be awarded PDU based on the hours of the course length divided by 8 (example: 40 hours would equal 5 ILT days = 50 PDUs).
	• Certificants can claim credit for up to 100 PDUs in this category.
	• A certificate of completion must be uploaded to receive PDUs in this category.

Category 2: Security-related Training, Certificate Programs, and/or Higher Education (cont.)	
Category 2c: Security related Higher Education	A college or university security-related, credit-bearing course (to include educational courses delivered by CDSE) that: • Consists of an organized series of planned learning experiences (e-Learning, instructor-led, instructor-facilitated online, self-paced, etc.) designed and developed to aid participants in acquiring knowledge, skills, and/or competencies associated with a coherent body of study within a discipline or set of related disciplines. • Is delivered by a nationally accredited academic institution. • Results in academic credits granted and recognized by accredited academic institutions. • Certification holders can receive 10 PDUs per week of an approved security-related, credit-bearing college or university course. • Certificants can claim credit for up to 100 PDUs in this category. • A copy of supporting documentation, such as a transcript, indicating completion and length of the higher education course must be uploaded to receive PDUs in this category.
Category 3: Non-Security related Training, Certificate Programs, and/or Higher Education	
Category 3a. Non-security related e-Learning training courses	Consists of an organized series of planned learning experiences developed and delivered in an e-Learning environment, to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area. • Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency delivers the training). • Awards a certificate of completion. • Certification holders can receive 1 PDU for each hour associated with an approved non-credit bearing training (all minutes past a full hour are rounded up to the next whole number, for example: anything under an hour rounds up to 1, 1 hour + 15 mins/1 hour + 30 mins/1 hour + 45 mins are all rounded up to 2). • Certificants can claim credit for up to 50 PDUs in this category. • A certificate of completion must be uploaded to receive PDUs in this category

Category 3b: Non-security related instructor-led or virtually-led training courses	Consists of an organized series of planned learning experiences developed and delivered either in-person or virtually led, to aid participants in acquiring specific knowledge, skills, and/or competencies associated with a topic area
	• Is delivered by an accredited training or education institution or is facilitated in-house (i.e., an agency or organization delivers the training)
	• Awards a certificate of completion
	• Certification holders can receive 10 PDUs for each full-day (4 or more hours) for each day of instruction, or 5 PDUs for each half-day (1-4 hours) associated with an approved non-credit bearing training course.
	  • VILT versions of an ILT will be awarded the same PDUs as that of the ILT version.
	  • VILTs that do not currently have an ILT version will be awarded PDU based on the hours of the course length divided by 8 (example: 40 hours would equal 5 ILT days = 50 PDUs).
	• Certificants can claim credit for up to 50 PDUs in this category.
	• A certificate of completion must be uploaded to receive PDUs in this category.

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

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

Category 5b: Non-SPēD PMO Security Related Projects	Certification holders may receive PDUs for successfully completing short-term non-SPēD PMO security related projects that require application of security subject matter expertise. **Participation in projects is voluntary in nature. PDUs cannot be accrued for projects for which participation is inherently part of the participant's job and/or assigned duties.* • Certificants can receive 3 PDUs per contact hour for each separate and distinct project • Certificants can receive 2 PDUs for each completed homework assignment for each separate and distinct project • Certificants can claim credit for up to 50 PDUs in this category • A copy of an endorsed letter (PDF) by the project champion, outlining overall contact hours and any completed homework assignments for each project effort, must be uploaded to receive PDUs in this category. NOTE: PDU hours are determined by the formula stated above and are not determined by the project champion.
Category 6: Other Voluntary Professionalization Activities	
Category 6: Other Voluntary Professionalization Activities	Certification holders can receive PDUs for involvement in verifiable professional development, whether security related or not. Examples of professional development activities include, but are not limited to: Leadership Development, Professional Advisory Boards, and career services. • Certification holders can receive 2 PDUs per contact hour for each separate and distinct professionalization activity associated with the professional development experience. • A maximum of 50 PDUs can be earned in this category for each professionalization activity. • Certificants can claim credit for up to 50 PDUs in this category. • A copy of supporting documentation indicating certification holders participated in the project (i.e., email confirmation or official letter of program/activity completion and associated hours of effort) must be uploaded to receive PDUs in this category.

FAILING TO MAINTAIN CERTIFICATIONS AND CREDENTIALS

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

APPEALS PROCESS AND PROCEDURES

GROUNDS FOR APPEAL

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

Appeals may be filed challenging the following:

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

DECISIONS NOT ELIGIBLE FOR APPEAL

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

- Employment policy
- Eligibility criteria

Certificants can contact the CCITP mailbox with questions or appeals of decisions.

APPEAL SUBMISSION

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

APPEAL REVIEW

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

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

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

Appeals may be filed challenging the following:

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

APPEAL DECISION AND NOTIFICATION

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

APPEAL WITHDRAWAL

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

WAIVER PROCESS AND PROCEDURES

CIRCUMSTANCES FOR WAIVER

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

WAIVER REQUEST SUBMISSION

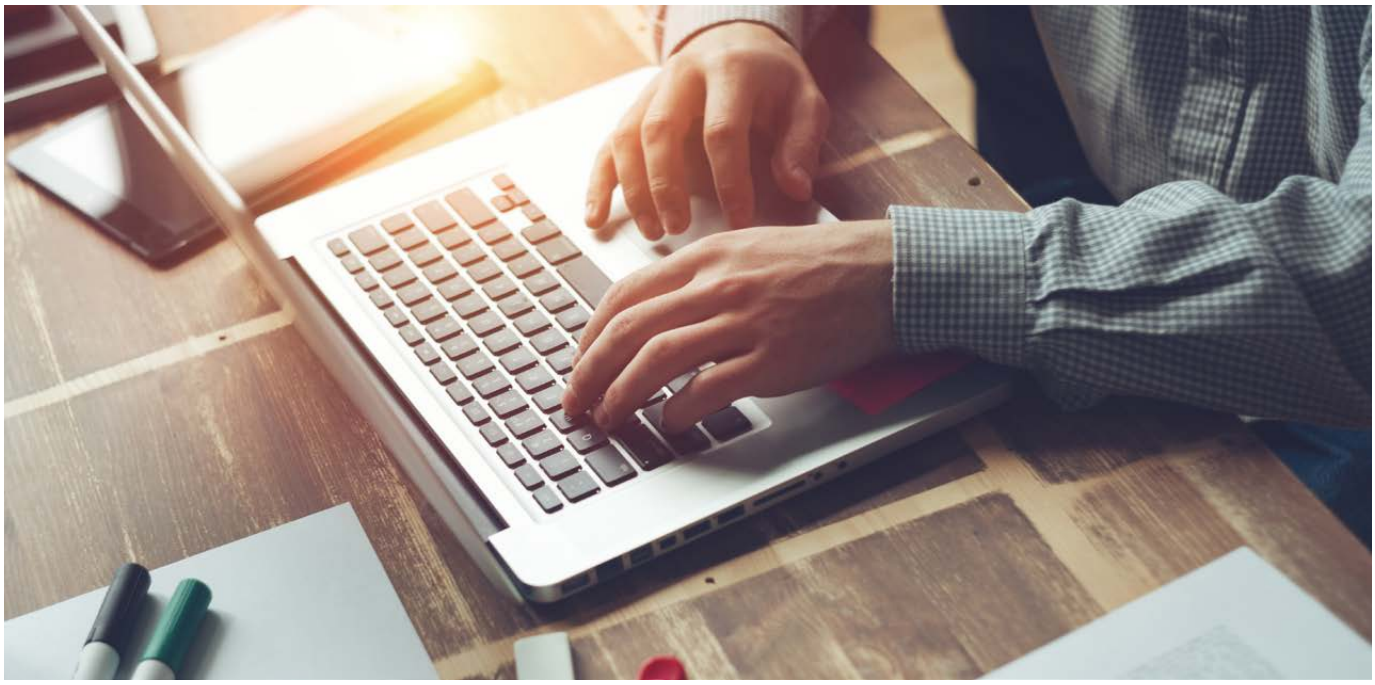
All waiver requests must use the Waiver Request Form (https://www.cdse.edu/Portals/124/Documents/certification/waiver_form.pdf?ver=rkSsN3zJLX7HKWPsc7oVSg%3d%3d) and be sent to the SPēD PMO (dcsa.ncr.cdse.mbx.ccitp@mail.mil).

WAIVER DECISION AND NOTIFICATION

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

APPROVED WAIVERS TIME FRAME

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



GLOSSARY

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

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

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

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

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

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

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

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

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

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

ACRONYMS

ADA	Americans with Disabilities Act
AoE	Areas of Expertise
CAC	Common Access Card
CCITP	Certified Counter-Insider Threat Professional
CCITP GC	CCITP Governance Council
C-InT	Counter Insider Threat
CPT	Competency Preparatory Tool
CRP	Certification Renewal Package
CRTD	Criterion-Referenced Test Development
DAU	Defense Acquisition University
DOD	Department of Defense
DS3	DOD Security Skill Standards
D-SEBOK	Defense Security Essential Body of Knowledge
EBK	Essential Body of Knowledge
EBW	Essential Body of Work
EO	Executive Order
I/O	Industrial/Organizational
IC	Intelligence Community
NCSC	National Counterintelligence and Security Center
NDA	Nondisclosure Agreement
NITTF	National Insider Threat Task Force
ONDI	Office of the Director of National Intelligence
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PDA	Personal Digital Assistant
PDU	Professional Development Unit
SME	Subject Matter Expert
SSO	Single Sign On
TA	Topic Area
USG	Unite States Government