Navy COOL

Credentialing Opportunities On-Line Home COOL Overview About Credentials Agency Resources Costs & Resources <u>Media</u> **Related Sites**

- Licenses & Certifications
- <u>Need Credential?</u>
- Documenting Training/Experience Listing Credentials on JST/SMART
- What's On COOL?
- ٠ **COOL** Organization
- How To Use COOL
- Understanding Search Results
- Resource Icon Overview •
- <u>Navy-Funded Exam Vouchers</u>
- <u>Navy-Funded Exam Reimbursements</u>
- Credentialing Costs
- Credentialing Resources
- Training and Education ٠



Step 4

Report Results

to Navy COOL

Step 3

Apply for Credential & Take Exam

Step 2

Get Exam Voucher

Step 1

Find & Select **Related Credentials**

Click X to close Step 4

| Report I | Results |
|----------|---------|
| to Navv | COOL |

| to Navy COOL | |
|--------------------------------------|---|
| | |
| Step 3 | |
| Apply for Credential & Take Exam | |
| | |
| Step 2 | |
| Get Exam Voucher | |
| | / |
| Step 1 | |
| Find & Select Related Credentials | |
| | |
| Step 4 | |
| Report Results to Navy COOL | |
| | |

Report Your Results

Upon completion of the credential exam, you must provide the results to:

- Credentials Program Office (pass or failure) (within 30 calendar days of taking exam). Please include score when possible. Email (pass or fail) results to: navycool@navy.mil.
- Your supervisor (pass or fail)
- Your local Approving Official (pass or fail)
- Enlisted Passing scores should also be reported to your PSD for service record entry and to the Navy College Office for inclusion into your Joint Service Transcript (JST) (previously known as SMART) and your Electronic Training Jacket (ETJ). You should provide only "Certified True Copies" or "Notarized" copies of your credential completion certificate to the Navy College Office.

To update your JST (Transcript) Contact:

Virtual Education Center 1905 Regulus Avenue, Suite 234 Virginia Beach, VA 23461-2009 Phone: 1-877-838-1659 Fax: 757-492-0595 https://jst.doded.mil/smart/welcome.do

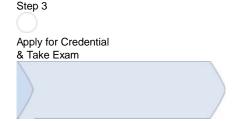
On your fax cover sheet be sure to include:

RANK/RATE: Last 4 of SSN Only: PHONE: E-Mail:

- Officer please ensure entry into OSR/ODC (pass only)
- DON Civilians please ensure copy of certification is provided to your local Human Resources/N1 (pass only)

In most cases, the member must schedule and take the credential exams within 60 calendar days from receipt of your voucher (date the exam was funded). If the member's certification exam process takes longer than 60 days he/she must call or email the Navy's Credentials Program Office (navycool@navy.mil) [(850) 452-6683/6664] in order to request a time waiver for going beyond the 60 calendar day limit. Vouchers not used in the approved timeframe will be recalled and the member will no longer be authorized to use the voucher.

The exam voucher/funding is non-transferable and may only be used by the individual specifically issued, towards the specific exam in which it was funded for. The member may be subject to administrative and/or disciplinary action if he/she attempts unauthorized use of the voucher.



Apply for the Credential and Take the Exam

It is important to note that Navy COOL is **not** a credentialing organization- you do not sign up for or take exams from Navy COOL. Once you have an approved exam voucher, you are responsible for contacting a credential exam test center (i.e. Pearson VUE, ProMetric, New Horizons, LaserGrade, etc...) to schedule the exam. You must schedule and take your exam within 60 days of issue of the Navy-funded voucher or the voucher expires (unless specifically coordinated with the Navy's Credentials Program Office). The following is a list of test vendors. Navy COOL does not endorse any of the following vendors, but lists them here for your convenience.

Test Vendors

- CATS
- <u>Certiport</u>
- <u>Comira</u>
- <u>KRYTERION</u>
- LaserGrade
- <u>Pearson Vue</u> (off-base testing)
- Pearson Vue (military on-base testing)
- Pearson Vue (map of on-base testing locations)
- Prometric

See the Credential Exams Frequently Asked Questions for answers to many questions related to credential exams.

Once you have taken the exam and received your results, see step 4 above, "Report Results to Navy COOL" for information about reporting your results.

Step 2

Get Exam Voucher

Navy-Funded Exam Voucher Requests

After you have chosen a credential, you will need to request an exam voucher. The Navy's Credentials Program Office has a limited amount of certification/license exam voucher funds each year. These vouchers will be issued on a "first-come, first-served" basis.

To receive a certification or license exam voucher:

- 1. Review the Frequently Asked Questions.
- 2. Make sure you are familiar with the detailed Navy-funded Exam Voucher Program information.
- 3. Apply for a voucher, using the Voucher Eligibility tool below.
 - Read the items, and check each box to confirm that you meet each criteria.
 - Click Get Form to download the Voucher Request Form Word document.
 - Open the form in Microsoft Word, fill it out, and save your changes.
 - Request that your Commanding Officer or designated E7 or above Command Representative <u>email</u> the completed form to the Credentials Program Office (navycool@navy.mil), or fax it to the Credentials Program Office - (850) 452-6897.

For further explanation of eligibility rules and the Navy-funded Exam Voucher Program, see the Costs and Resources page.

Once you have an approved exam voucher, go to step 3 above, "Apply for Credential and Take Exam" for instructions on applying to take the exam with the credentialing agency or testing service.

Pre-Approved Reimbursement Requests

For information on obtaining reimbursements for exam fees, see Exam Reimbursement Program information, or refer to the Costs and Resources page.

Navy COOL Voucher Eligibility Tool

You must receive approval for a voucher from the Navy Credentials Program Office BEFORE registering for, scheduling or taking an exam, or taking any other action that requires payment. Failure to receive voucher approval in advance may mean that you have to pay for an exam yourself, without reimbursement from the Navy.

Check off each item below to affirm you are eligible to request a voucher, then click Get Form.

I am enlisted U.S. Navy active duty or Navy Reserve, but not IRR (may be Officer, or DoN Civilian for mandatory Information Assurance Workforce (IAWF) certifications)

I meet one of the following criteria:

- I am in the appropriate Enlisted Rating/Officer Designator/Civil Service Series or collateral duty/out of rate assignment to which the credential is mapped.
- I am currently working in, or have been assigned to a position to which the credential is mapped.
- I have prior documented experience in a position to which the credential is mapped (for credentials outside of my specific rating, the credential has relevance or applicability to the current or future needs of the command or the Navy). Officers and DoN Civilians are currently ONLY funded for IAWF credentialing exams.

I meet the credentialing agency's requirements for this credential.

My Commanding Officer or Command-designated E7 or above approving official (Command IAM for IAWF personnel) will validate, before authorizing the request (note: ALL of the following criteria apply to Active Duty and Reserve personnel. For DoN Civilian IAWF, only the service obligation criteria below apply):

- I have passed my most recent advancement exam.
- I have passed, or been medically waived from, my most recent physical fitness assessment.
- I have not received a judicial or courts martial punishment within the past 6 months.
- I have been recommended for promotion or advancement on my most recent performance evaluation.
- I have, at a minimum, one year remaining on my enlistment or military service obligation at the time I receive the certification for which I am requesting funding. (Special cases will be considered by the Navy's Credentials Program Office, as stated in OPNAVINST 1540.56a)

The credential I want is in a Funded section with a (Navy S) resource icon next to the section heading.

I have verified that the exam I am requesting is offered at a date and location I can attend.

Please ensure you have met all eligibility requirements and check each box before getting the form

Note: If you do not meet the above criteria, you may be eligible for a waiver IAW OPNAVINST 1540.56a. Review Time of Service Info to see if you're eligible.

Get Form

Search for Enlisted

Select an item, then click 'Go.'

| - Select Rating - | Go | |
|---|----|----|
| - Select Collateral Duty/Out of Rate Assignment - | | Go |
| - Select Civilian Career Area - Go | | |
| - Select Apprenticeship - | Go | |
| Credential Name Search | | |
| Agency Name Search | | |
| Hide content | | |
| Search For Enlisted | | |
| Search For Officers | | |

Select an item, then click 'Go.'

| - Select Designator Code - | | Go |
|------------------------------------|----|----|
| - Select Designator Title - | | Go |
| - Select Duty/Assignment - | Go | |
| - Select Civilian Career Area - Go | | |
| Credential Name Search | | |
| Agency Name Search | | |
| Hide content | | |
| Search For Officers | | |
| Search for Dept. of Navy Civilians | | |
| | | |

Select an item, then click 'Go.'

| Select Duty/Assignment | Go |
|-------------------------------------|----|
| Credential Name Search | |
| Agency Name Search | |
| Hide content | |
| Search for Dept. of Navy Civilians | |
| CTN-Cryptologic Technician Networks | |
| Navy Duties | |
| + | |

CTN-Cryptologic Technician Networks

The Cryptologic Technician - Networks branch offers a career in computer Networks. CTN's perform a variety of duties associated with computer network operations across global networks. About 600 men and women serve worldwide in the CTN rating. Advanced training in computer network operations, using state-of-the-art technology is readily available. Within a short period, today's CTN quickly develops highly marketable computer network skills. A combination of technical and analytical computer network skills provides the situational awareness required to plan and execute informational operations (IO) actions/counter-actions. Initial training is located in Pensacola, Florida. For more detailed information, see the <u>Rating Information Card</u>. CTN Jobs

- <u>CTN Global Network Operations Director</u>
- <u>CTN Global Network Operations Manager</u>
- <u>CTN Global Network Operations Technician</u>

Show All / Hide All Related Credentials

CTN-Cryptologic Technician Networks

- <u>National Certifications</u>
- <u>Apprenticeship</u>

i Show Credential Tables / Hide Credential Tables

Navy S Funded Certifications

| Credential | Agency | <u>TypeNavy\$</u> | <u>Gap</u> Analysis | <u>LaDR</u> | <u>GI Bill</u> <u>ANSI</u> | NCCACollege Credit |
|--|---|-------------------|------------------------|-------------|----------------------------|-----------------------|
| Associate Information Technology Coordinato | Professional Standards Institute | S Navy | | | | |
| Associate of ISC2 | International Information Systems Security Certification Consortium, Inc. | S Navy |) | | | |
| Certified Ethical Hacker (CEH) | International Council of E-Commerce Consultants (EC-Council) | S Navy |) | E | 5 ANS | 61 |
| Certified in Disaster Preparedness (CDP-I) | American Board for Certification in Homeland Security (ABCHS) | S Navy |) | EŠ | 600 | |
| <u>Certified in Homeland Security Level I, II, & III</u> (CHS-I, II, & III) | American Board for Certification in Homeland Security (ABCHS) | S Navy |) | | GOD | |
| Certified in Homeland Security Level IV (CHS-IV) | American Board for Certification in Homeland Security (ABCHS) | S Navy |) | E | 600 | |
| <u>Certified in Homeland Security Level V</u> (CHS-V) | American Board for Certification in Homeland Security (ABCHS) | S Navy |) | E | ¢00 | 8 |
| Certified Information Security Manager (CISM | Information Systems Audit and Control Association (ISACA) | n S Navy | • | | GOD ANS | 51 |
| Certified Information Systems Security Professional (CISSP) | International Information Systems Security Certification Consortium, Inc. | S Navy |) | EŠ | GOD ANS | 51 |
| Certified Security Analyst (CSA) | International Council of E-Commerce Consultants (EC-Council) | S Navy |) | | | |
| Check Point Certified Security Principles Associate | Check Point Software Technologies, Inc. | S Navy |) | | | |
| Cisco Certified Network Associate Routing an Switching (CCNA) | ^d Cisco Systems, Inc. | D Navy |) | E¥ | GOD ANS | 51 |
| CompTIA Advanced Security Practitioner (CASP) | Computing Technology Industry Association (CompTIA) | S Navy |) | | ANS | 51 |
| CompTIA Network+ | Computing Technology Industry Association (CompTIA) | D Navy |) | EŬ4 | GOI ANS | 51 |
| CompTIA Security+ | Computing Technology Industry Association (CompTIA) | S Navy |) | | 🗐 ANS | 51 |
| CyberSecurity Forensic Analyst (CSFA) | CyberSecurity Institute | S Navy |) | EŬ | | |
| GIAC Assessing and Auditing Wireless Networks (GAWN) | Global Information Assurance Certification (GIAC) | S Navy |) | E | 5 | |
| GIAC Certified Forensics Analyst (GCFA) | Global Information Assurance Certification (GIAC) | S Navy |) | E | ANS | 51 |

| GIAC Certified Incident Handler (GCIH) | Global Information Assurance Certification (GIAC) | S | Navy S | GII ANSI |
|---|--|---|---------|--------------------|
| GIAC Certified Intrusion Analyst (GCIA) | Global Information Assurance Certification (GIAC) | S | Navy S | E 6 🗐 ANSI |
| GIAC Certified Penetration Tester (GPEN) | Global Information Assurance Certification (GIAC) | S | Navy S | E 0 6 |
| GIAC Security Essentials Certification (GSEC) | Global Information Assurance Certification (GIAC) | S | Navy \$ | E U4 🗐 ANSI |
| GIAC Security Leadership Certification (GSLC) | Olobal Information Assurance Certification (GIAC) | S | Navy \$ | ANSI |
| GIAC Systems and Network Auditor (GSNA) | Global Information Assurance Certification (GIAC) | S | Navy S | ¢D |
| Licensed Penetration Tester (LPT) | International Council of E-Commerce Consultants (EC-Council) | S | Navy \$ | |
| Sensitive Security Information, Certified (SSI) | American Board for Certification in Homeland Security (ABCHS) | S | Navy \$ | |
| Systems Security Certified Practitioner (SSCP) | International Information Systems Security | S | Navy S | GOD ANSI |
| | | | | |

Cther Certifications Related Occupational Opportunities

CTN-Cryptologic Technician Networks

- <u>Civilian</u>
- Federal

Related Civilian Occupational Equivalents

The following civilian occupations are similar to CTN-Cryptologic Technician Networks. These occupations may require additional education, training or experience. For more information about these occupations, click on the civilian equivalent below.

| Civilian Occupational Equivalents Civilian Job | Bright OutlookGreen OccupationLocal Salary InfoFind Jobs |
|---|--|
| Computer and Information Systems Managers | find local salary find jobs |
| Network and Computer Systems Administrator | s 🤤 find local salary find jobs |
| Additional Information, Continuing Education | |
| | |

CTN-Cryptologic Technician Networks

- Additional Information
- <u>Continuing Education</u>
- <u>Collateral Duty/ Out of Rate Assignments</u>

Additional Information

Additional information pertaining to CTN-Cryptologic Technician Networks can be found below.

Department of Defense (DOD) 8570.01-M

<u>DoD</u> 8570.01-M, signed 19 Dec 2005, mandates Cyberspace (CS)/Information Assurance (IA) identification, tracking, and reporting of personnel within the Cyberspace/Information Assurance Workforce (CSWF/IAWF) and use of commercial certifications to validate <u>DoD</u> baseline knowledge and skills. Some Sailors may have these <u>CSWF/IAWF</u> responsibilities and will need to meet the 8570.01-M certification requirements.

For more information, see:

- <u>CSWF/IAWF description</u>
- <u>Cyberspace Workforce/IAWF Credential Summary</u>
- MeasureUp CompTIA Certification Pre-Tests

Sailors in the CTN Rating should review the information for CS - Computer Network Defense (CND).

Updated: June 28, 2013

- <u>Contact Us</u>
- <u>COOL Overview</u>

- About Credentials
- <u>Costs & Resources</u>
- <u>Media</u>
- <u>COOL Quotes</u>
- Related External Sites
- Accessibility
- Disclaimer



Click link to go to CompTIA Network+ COOL Snapshot page.

Network+ is an intermediate skill level certification for IT technicians who can describe the features and functions of networking components and manage, maintain, troubleshoot, install, operate and configure basic network infrastructure. Network+ is appropriate for computer network technicians, engineers, analysts and administrators. Although not a prerequisite, it is recommended that CompTIA Network+ candidates have at least nine months of experience in network support or administration or academic training, along with a CompTIA A+ certification.

Click link to go to Cisco Certified Network Associate Routing and Switching (CCNA) COOL Snapshot page.

Cisco Certified Network Associate Routing and Switching (CCNA) validates the ability to install, configure, operate, and troubleshoot medium-size route and switched networks, including implementation and verification of connections to remote sites in a WAN. This includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. The Routing and Switching CCNA is an Associate level certification which is considered the foundation level of networking certification. The Routing and Switching CCNA certification is appropriate for Information Technology occupations such as network and computer systems operators, engineers and technicians. There are no experience or education requirements that must be met prior to taking the exam(s).

The Routing and Switching CCNA exams have been recently updated and the newest version (exam 200-120) is currently available. The older exams (exam 640-802) will be available until September 30, 2013.

Click link to go to Certified Information Systems Security Professional (CISSP) COOL Snapshot page.

The Certified Information Systems Security Professional (CISSP) is an advanced skill level certification for experienced professionals in the computer security field who are responsible for developing the information security policies, standards, and procedures and managing their implementation across an organization. To be eligible for CISSP, candidates must have five years of information security experience in at least two of the following areas: Access Control; Application Security; Business Continuity and Disaster Recovery Planning; Cryptography; Information Security and Risk Management; Legal, Regulations, Compliance and Investigations; Operations Security; Physical (Environmental) Security; Security Architecture and Design; and Telecommunications and Network Security.

Click link to go to GIAC Certified Incident Handler (GCIH) COOL Snapshot page.

The GIAC Certified Incident Handler (GCIH) is an intermediate skill level certification for individuals who are responsible for incident handling/incident response and individuals who require an understanding of the current threats to systems and networks, along with effective countermeasures. GCIHs have the knowledge, skills, and abilities to manage incidents, understand common attack techniques and tools, and defend against and/or respond to such attacks when they occur. This certification is appropriate for computer security specialists responsible for incident handling and response. There are no prerequisites for this certification.

Click link to go to GIAC Certified Intrusion Analyst (GCIA) COOL Snapshot page.

The GIAC Intrusion Detection In-Depth (GCIA) is an intermediate skill level certification that was created to provide assurance that a certified individual holds the appropriate level of knowledge and skill necessary for anyone relied upon by an organization to perform intrusion detection using network and host-based techniques. GCIAs are individuals who configure and monitor intrusion detection systems, and read, interpret, and analyze network traffic and related log files. This certification is appropriate for information security occupations. There are no prerequisites for the GCIA certification.

Click link to go to GIAC Security Essentials Certification (GSEC) COOL Snapshot page.

The GIAC Security Essentials Certification (GSEC) is an entry level security certification created to provide assurance that a certified individual holds the appropriate level of knowledge and skill necessary for anyone with hands on technical responsibilities in the key or essential areas of information security. The certification is targeted toward IT security professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are

required to demonstrate an understanding of information security beyond simple terminology and concepts. There are no prerequisites for the GSEC certification.

Click link to go to GIAC Systems and Network Auditor (GSNA) COOL Snapshot page.

The GIAC Systems and Network Auditor (GSNA) is an intermediate skill level certification targeted towards auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing. GSNAs have the knowledge, skills and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems. This certification is targeted toward experienced information security auditors and those who have information security management responsibilities. There are no prerequisites for the GSNA certification.

Click link to go to Systems Security Certified Practitioner (SSCP) COOL training gap analysis page.

The Systems Security Certified Practitioner (SSCP) is an intermediate skill level certification for individuals involved in network and systems security administration who are responsible for developing the information security policies, standards, and procedures and managing their implementation across various hardware and software programs in their organization. The SSCP is targeted toward those working towards positions such as Network Security Engineers, Security Systems Analysts, or Security Administrators. It is also appropriate for personnel in other non-security disciplines that require an understanding of security but do not have information security as a primary part of their job description, including information systems auditors; application programmers; system, network and database administrators; business unit representatives, and systems analysts. Candidates must have at least one year of systems security-related work experience.

Click link to go to CompTIA Security+ COOL Snapshot page.

The CompTIA Security+ certification designates knowledgeable professionals in the field of IT security. Security+ is an introductory level certification that proves competency in system security, network infrastructure, access control, assessments and audits, cryptography and organizational security. Occupations relevant to this certification include computer security specialists, computer and information systems managers, and network and computer systems administrators. Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of technical networking experience, with an emphasis on security. The CompTIA Network+ certification is also recommended.

Click link to go to GIAC Certified Forensics Analyst (GCFA) COOL Snapshot page.

The GIAC Certified Forensic Analyst (GCFA) is an intermediate skill level certification for individuals who are responsible for forensic investigation/analysis, advanced incident handling, or formal incident investigation in information security. GCFAs have the knowledge, skills, and abilities to handle advanced incident handling scenarios, conduct formal incident investigations, and carry out forensic investigation of networks and hosts. This certification is appropriate for computer security specialists responsible for incident handling and investigation. There are no prerequisites for this certification.

Click link to go to GIAC Security Leadership Certification (GSLC) COOL Snapshot page.

The GIAC Security Leadership Certification (GSLC) is an intermediate skill level certification for individuals with managerial or supervisory responsibility for information security staff. The GSLC certification covers topic areas including security management, cryptography, incident handling, risk assessment, web security and vulnerability management. There are no prerequisites for the GSLC certification.

Click link to go to Certified Information Security Manager (CISM) COOL Snapshot page.

The Certified Information Security Manager (CISM) is an advanced certification for the individual who designs, builds, and manages an enterprises information security. CISM focuses on information risk management as the basis of information security. It also includes material on broader issues such as how to govern information security as well as on practical issues such as developing and managing an information security program and managing incidents. This certification is targeted toward experienced information security managers and those who have information security management responsibilities. Five or more years of information security work experience, with a minimum of three years of information security management work experience is required.

Click link to go to Check Point Certified Security Principles Associate COOL Snapshot page.

The Certified Security Principles Associate is an entry level certification designed for individuals who have basic knowledge of security issues, risk management, business recovery strategies, the nature of intrusions and attacks and the fundamentals of cryptography. CCSPAs are responsible for implementing and enforcing an organization's security policies, recognizing network security threats, and recommending security solutions to meet business needs. Occupations relevant to this certification include computer security specialists, computer and information systems managers, and network and computer systems administrators. There are no experience or education requirements that must be met prior to taking the exam.

Click link to go to Certified in Homeland Security Level IV (CHS-IV) COOL Snapshot page.

Certified in Homeland Security level IV, CHS-IV is designed for Senior-level individuals who have at least two years or more of professional experience, along with continued education, knowledge, skills and general instruction in their perspective fields. Level III is generally aimed at preparing for, protecting against or managing the consequences of harm on American soil. Element of this certification are actions to safeguard the public, property, critical infrastructure, military installations and the government. Certification is limited to those who have proven experience; Military members desiring to become certified in their rating must have occupations directly corresponding within Homeland Security and its security fields. Some additional requirements such as work or education may have to be completed to become qualified.

Click link to go to Certified in Homeland Security Level V (CHS-V) COOL Snapshot page.

Certified in Homeland Security level-V, CHS-V is the final and Premier level within the CHS process. Prerequisites for applying for the CHS-V, applicants must have successfully completed CHS-IV. Applicants who want to pursue Level-V certifications are strongly recommended to download suggested preparation material from the www.Abchs.com website. Level-V challenges the courses taught and education and experienced gained throughout the Homeland Security domain. Participants are encouraged to review the National Response Framework, along with Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE). A live Homeland Security overview course is available, and participants are tested following the course. Contact ABCHS for details.

Click link to go to Certified in Homeland Security Level I, II, & III (CHS-I, II, & III) COOL Snapshot page.

Certified in Homeland Security Level I, II, & III is a three part program designed to establish a better understanding of natural (accidental) or man-made (can be intentional) disasters, as well as an expanded knowledge of the vocabulary and terminology that is used by professionals working in homeland security and disaster preparedness. See the individual level descriptions for more information.

Click link to go to CyberSecurity Forensic Analyst (CSFA) COOL Snapshot page.

The CyberSecurity Forensic Analyst (CSFA) is an advanced level certification for individuals who have the ability to conduct a thorough forensic analysis using sound examination and handling procedures, and are able to communicate the results of their analysis effectively. The CSFA certification is designed for professionals who already possess practical experience in the field of digital forensics. A minimum of at least two years of experience with both the technical and administrative aspects of conducting forensic analysis is required. To become CSFA certified, applicants must pass a written and practical exam, and complete an FBI criminal background check.

Click link to go to Certified Ethical Hacker (CEH) COOL Snapshot page.

The Certified Ethical Hacker (CEH) program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in networks and/or computer systems and uses the same knowledge and tools as a malicious hacker upon request from an organization. The certification is for individuals who are responsible for securing (or testing the security of) computer networks. The CEH is appropriate for security officers, auditors, security professionals, site administrators, and others who may be concerned about the integrity of their organizations network infrastructure. Applicants must have a minimum of two years of security related work experience.

Click link to go to GIAC Assessing and Auditing Wireless Networks (GAWN) COOL Snapshot page.

The GIAC Assessing and Auditing Wireless Networks (GAWN) certification is an intermediate level certification for auditors, network administrators and penetrationtesters who are responsible for assessing the security of wireless networks. The GAWN certification focuses on the different security mechanisms for wireless networks, the tools and techniques used to evaluate and exploit weaknesses, and techniques used to analyze wireless networks. There are no formal education or experience requirements associated with this certification. Training is available but not required.

Click link to go to Certified Security Analyst (CSA) COOL Snapshot page.

The EC Council Certified Security Analyst (CSA) is an advanced ethical hacking certification for individuals who wish to demonstrate expertise in computer security by exploring the analytical phase of ethical hacking. This certification complements the Certified Ethical Hacker (CEH) certification and is a prerequisite for the Licensed Penetration Tester (LPT) designation. The CSA certification explores how to analyze the outcome of the tools and techniques used in ethical hacking to identify and mitigate risks to the information security of the infrastructure. The CSA is appropriate for security officers, auditors, security professionals, site administrators, and others who may be concerned about the integrity of their organizations network infrastructure. Candidates are not required to attend training courses, but those who do not must submit an Eligibility Application Form and obtain authorization from EC-Council before attempting the exam.

Click link to go to Licensed Penetration Tester (LPT) COOL Snapshot page.

The Licensed Penetration Tester (LPT) is an advanced certification which trains IT security professionals to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. Certification holders will have the skills to use penetration testing methodologies, tools and techniques to design, secure, and test networks to protect an organization from threats. The LPT is appropriate for security officers, auditors, and security professionals. Candidates must be current holders of the Certified Ethical Hacker (CEH) and Certified Security Analyst (CSA) certifications. There is no additional exam required to obtain the LPT certification, however, candidates must complete an application detailing professional experience, previous certifications and references, as well as submit documentation for a criminal background check. US residents are required to obtain FBI clearance.

Click link to go to Sensitive Security Information, Certified (SSI) COOL Snapshot page.

Sensitive Security Information, SSI is an entry level new program designed for professionals who are currently, or will be, in a position that deals with handling sensitive security information. With obtaining this credential, you will gain comprehensive knowledge of every aspect of Sensitive Security Information (SSI) as it relates to government, business, and your own personal use. The program teaches how to protect sensitive documents, history of espionage and levels of Sensitive security. Personnel enrolled in this program should have at least two years in the field of knowledge of Sensitive Security Information in the private sector, government/military areas of protecting data.

Click link to go to Certified in Disaster Preparedness (CDP-I) COOL Snapshot page.

Certified in Disaster Preparedness CDP-1, CDP-1 is an entry to mid-level program for Military personnel, First Responders; Emergency Management officials who need better information with which to train their communities. Faith-Based Organizations who want to cement their position as an integral part of community safety. Civic Groups that are looking for ways to help their members and Schools that would like to teach preparedness as a class. It is also for those individuals that will train and prepared those to report for duty and leave their families behind. This course prepares you to understand the threat, survive the causality and protect you and your family in harsh conditions and environments. Persons taking this course should have from 1-5 years or more experience and knowledge of emergency preparedness/knowledge.

Click link to go to GIAC Certified Penetration Tester (GPEN) COOL Snapshot page.

The GIAC Certified Penetration Tester (GPEN) is an intermediate level certification for individuals responsible for assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test. There are no formal education or experience requirements. Training is available but not required.

Click link to go to Associate Information Technology Coordinator - Associate Level COOL Snapshot page.

Associate Information Technology Coordinator - Associate Level. The Information Technology Consulting field is a broad area that is for the "generalist" in Information Technology. Information Technology Consultants work in systems development, web development, database development, desktop and network support, information security, and several other areas in the Information Technology industry. The PSI Certified Associate Information Technology Coordinator (PCAITC) certification is an entry level certification for individuals starting out in the Information Technology field. It is recommended that you have at least 2 years of experience in the field prior to taking the certification test. Candidates must pass a 40-question examination. This credential is good for three years; then it must be recertified through a fee, and 40 Professional Development Credits.

Click link to go to CompTIA Advanced Security Practitioner (CASP) COOL Snapshot page.

The CompTIA Advanced Security Practitioner (CASP) certification is targeted to individuals with advanced-level security skills and knowledge. The CASP exam is designed to verify an applicants knowledge and skill in the areas of enterprise security, risk management, research and analysis, and the integration of computing, communications, and business disciplines. Although there are no required pre-requisites, the CASP certification is intended to follow the CompTIA Security+ certification as the next step in security certifications. A minimum of 10 years experience in IT administration with at least 5 years in hands-on technical security experience is recommended.

Click link to go to Associate of ISC2 COOL Snapshot page.

The Associate of ISC² is a certification status earned by candidates who successfully pass an ISC² certification exam but do not have the required number of years of

experience yet to fully qualify for the certification. The Associate of ISC² is granted after passing one of the following exams: Certified Information Systems Security Professional (CISSP), Certified Secure Software Lifecycle Professional (CSSLP), Certified Authorization Professional (CAP), and Systems Security Certified

Practitioner (SSCP). Associate's of ISC² are required to meet continuing education guidelines while gaining professional experience. Once an Associate meets the professional years of experience required by the certification, they may complete the application requirements for the certification they are pursuing (CISSP, CSSLP, SSCP or CAP).