

Credentialing the
Cybersecurity Workforce:
CompTIA Insights into the
Certification Process



CONTENTS

FOREWORD	3
THE CYBERSECURITY TRAINING IMPERATIVE	4
INDUSTRY-DRIVEN, VENDOR-NEUTRAL CERTIFICATIONS: THE CompTIA STORY	4
IT CERTIFICATION IN THE CYBERSECURITY ENVIRONMENT	5
WHAT IS A CERTIFICATION?	5
PRODUCING TRUSTED CYBERSECURITY CERTIFICATIONS	6
THE CERTIFICATION DEVELOPMENT PROCESS	6
HOW IS A CERTIFICATION MADE?	6
HOW IS A CERTIFICATION DELIVERED?	8
WHAT TO MEASURE IN A CREDENTIAL EXAMINATION:	9
KNOWLEDGE OR PERFORMANCE?	
THE CompTIA PUBLIC-PRIVATE-ACADEMIC PARTNERSHIP:	10
OPTIMUM RESPONSIVENESS TO RAPID DEVELOPMENTS	
IN THE CYBERSECURITY THREAT ENVIRONMENT	
CompTIA AND THE CYBERSECURITY CREDENTIALS INDUSTRY:	11
GOOD AND GETTING BETTER	
GLOSSARY	12
APPENDICES	16

FOREWORD

CompTIA, the leading global provider of vendor-neutral IT certifications, develops security certifications that are foundational and promote the workforce skills needed to combat cyber threats and weaknesses. Though we believe that the CompTIA role is well defined, the broader IT credentialing world can at times seem opaque and, as such, susceptible to charges that today's IT credentialing system is not keeping pace with emerging technologies and threats. This white paper will dispel that notion by providing a transparent explanation of CompTIA's expertise in developing, disseminating, and updating IT security certifications. While other peer organizations may offer procedural variations, it is our hope that this description of the CompTIA methodology will provide a broader understanding of the importance and effectiveness of the private sector credentialing community. In this paper we set forth:

- The importance of developing varied career paths to meet today's challenges.
- CompTIA's network of learning and testing partners and the origin and importance of vendor-neutral certifications.
- The meaning of a certification: A credential achieved through examination that validates the knowledge and skills of an individual or organization.
- How effective certification is constructed and kept up to date by assembling subject matter experts to develop a Job Task Analysis (JTA), an examination blueprint, and extensive examination questions that map to the blueprint.
- A discussion of our testing partners and the steps undertaken to ensure the integrity of examinations and their results.
- The value of both knowledge- and performance-based testing.
- The breadth of CompTIA relationships with government and academic communities, all of which enhance the effectiveness of the credential and the rapidity by which real-world developments can drive updates, improvements, and training.
- A framework that demonstrates order and coherence to the cybersecurity credentialing ecosystem.

With a rapidly developing cybersecurity threat matrix, both government and private-sector professionals must be nimble and collaborative. We are all a part of the solution.

Todd Thibodeaux, President and CEO

CompTIA

“Every day we see waves of cyber thieves trolling for sensitive information—the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services... It’s been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to one trillion dollars. In short, America’s economic prosperity in the 21st century will depend on cybersecurity.”

– President Barack Obama, “On Securing Our Nation’s Cyber Infrastructure,” May 29, 2009.

“The United States is fighting a cyber-war today, and we are losing. It’s that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking...for all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts.”

– Admiral Mike McConnell, Former Director of National Intelligence, The Washington Post, February 28, 2010.

THE CYBERSECURITY TRAINING IMPERATIVE

Technology innovation has given us an interconnected global marketplace. We now have hundreds of millions of online users with constantly evolving mobile computing platforms offering ubiquitous access to information, communication, and commerce wherever we live. We now have more raw computing power contained in smart phones than the cumulative mission-control IT capability that propelled mankind on the first lunar missions in the 1970s. The correspondingly complex and mobile nature of digital threats to the world’s computer networks is growing at the same exponential pace.

Training the cybersecurity workforce for tomorrow’s threat environment requires forward-looking approaches; merely informing end users and IT security professionals about existing cyber threats is not enough. Those responsible for hiring the best human cybersecurity talent must have confidence—before a breach or breakdown occurs—that employees are trained and equipped in a manner that can be confidently identified, measured, and validated. The challenge we face is to produce the best-trained professionals in the world, equipped with proper tools. Further, it is essential to develop and provide ongoing training so that the professional workforce is prepared to address new and emerging threats to our increasingly digital way of life.

Cybersecurity professionals have relied on a variety of ways to prepare for cyber threats. In most cases, training and corresponding credentials come through degree programs (from higher education or technical training institutions) and technical certifications (in either vendor-specific software or hardware products). Other sources include vendor-neutral credentials that address a broader subject or practice area, on-the-job training programs, internships or other practical, experience-based programs.

In the cybersecurity world, career paths vary from technical information assurance and auditing to IT management—with levels within each scaling from apprentice to master. Each pathway serves a distinct and important role in addressing today’s cyber threats and requires unique training and skill sets.¹ (See Appendix 1 for details.)

CompTIA works in collaboration with thousands of academic and vendor-specific IT training programs around the world. CompTIA also covers a wide array of IT fields including storage, healthcare, green IT, and more. However, the focus of this paper is the suite of IT certifications that are the basis for cybersecurity training and the specific role of certifications in addressing the critical need to train, credential, and deploy thousands of professionals to protect our national IT infrastructure.

INDUSTRY-DRIVEN, VENDOR-NEUTRAL CERTIFICATIONS: THE CompTIA STORY

The success of the personal computer led the computer service and repair industries to commission CompTIA to create its globally recognized, vendor-neutral CompTIA A+ certification examination program in 1992. The continuing success of CompTIA A+ certification demonstrates an ongoing need to provide a means of validating skills across a wide spectrum of computer hardware and software. Following on the success

¹ A useful resource for viewing the structure for how IT certifications advance along different career paths is the Department of Defense Directive 8570 (<http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>). Civilian career paths can and do map to DOD equivalents. Another resource is the Essential Body of Knowledge matrix developed by the Department of Homeland Security (<http://www.us-cert.gov/ITSecurityEBK/EBK%20Matrix-Sept08.pdf>).

of the A+ certification, CompTIA developed and introduced CompTIA Network+, and CompTIA Security+. Each CompTIA certification is industry-driven, validating technical skills for both individuals working in IT and for the people who hire and train them.

By securing and validating core skills and knowledge, both jobseekers and established professionals can progress to more complex and specialized cybersecurity credentials, such as vendor-specific hardware and software training. As a career in cybersecurity matures, it may well necessitate higher-level, specialty training and skills in subjects such as security auditing, forensics, and cybersecurity management. Workers might also feel compelled to acquire additional credentials to validate those skills to current or prospective management. A diverse array of career paths needs to be available, and is indeed necessary, in order to maintain a skilled cybersecurity workforce.

Along with a global network of third-party academic and training providers, CompTIA plays an important role in the skills-development efforts for today's cybersecurity workforce. As a result of our focus on creating independent certification credentials developed in isolation from the training community, CompTIA is recognized worldwide as a trusted provider of vendor-neutral certification exams.

IT CERTIFICATION IN THE CYBERSECURITY ENVIRONMENT

In addition to validating core competencies, certifications can be developed and deployed quickly to address ever-evolving threats to our IT infrastructure. Certifications can demonstrate that a workforce remains current and informed on technology advancements that defend against ever-present cyber threats. The responsiveness of CompTIA's credentialed certifications in addressing technological advancements has led to government and private-sector mandates for continuing education requirements for cybersecurity professionals—a development that CompTIA fully supports.

What is a certification?

Determining what constitutes a certification as compared to a certificate, a credential, and accreditation can be challenging. Put simply, a certification is achieved through an examination that validates the knowledge and/or skills of an individual or an organization. A certification differs from a certificate program, which is usually an educational offering that confers a document at the program's conclusion. The American National Standards Institute (ANSI) provides a useful definition:

Certification and certificate are distinct terms, yet they are often used synonymously. Certification is more comprehensive and includes an assessment of an individual's knowledge, skills, and abilities based on a body of knowledge pertaining to a profession or occupation. In comparison, certificate programs emphasize learning events and coursework completion. Certification is valid for a specific time period and involves recertification at the expiry of the stated period. Certificates are generally issued for life.²

Beyond this important distinction, the industry often refers to credentials and accreditations. Credentials attest to someone's knowledge or authority such as a FBI agent badge, a Ph.D. in physics, or an IT security certification. Accreditation is granted when

² <https://www.ansica.org/wwwversion2/outside/PERfaq.asp?menuID=2>

stated quality criteria are met. Thus, for example, CompTIA has sought accreditation of its certifications by submitting to a voluntary, self-regulatory process through ANSI.

The wide variety of methods used to train and validate knowledge for cybersecurity professionals demonstrates there is no “one-size-fits-all” solution. While most academic and professional programs promote broad, introductory knowledge for cybersecurity professionals, the generalized scope of such programs is impractical for many full-time IT professionals. Specialty certifications can be more effective in providing “just-in-time” training and validation for a specific technology tool or skill. But in some situations, more in-depth training and certification, which generally requires more experience in a profession and more core knowledge, is appropriate. Ideally, IT professionals, along with their career guidance personnel, can construct learning and career paths using a variety of credentialing options as tools to develop the skill sets required to ensure national cybersecurity.

PRODUCING TRUSTED CYBERSECURITY CERTIFICATIONS

IT certification has evolved into a validation instrument that is a trusted resource in both the IT and the human resources (HR) communities. How is an internationally validated and trusted certification instrument constructed?

The Certification Development Process

To be an effective and defensible IT certification, a credential must meet the following criteria:

- **Technical Precision and Accuracy** with respect to the current and particular body of knowledge.
- **Comprehensive in Scope** to validate the breadth of skills required by the IT and cybersecurity professional.
- **Educationally Valid Verification** to fairly and accurately gauge skills and knowledge.
- **Integrity in the Exam Creation Process** so students trust that an exam fairly validates the requisite skills for a particular job or skills area and is worth requisite study and experience; and that IT management and HR professionals trust both the credential and the holder as a person who possesses genuine and comprehensive knowledge.
- **Rigorous and Effective Security** in Delivery to ensure that cheating does not take place.

To meet these important benchmarks, CompTIA employs an exacting process to develop and disseminate credentials.

How is an IT Certification Made?

Development of an IT certification begins by identifying and bringing together Subject Matter Experts (SMEs) to draft a blueprint for the examination known as a Job Task Analysis (JTA). Using the JTA, SMEs proceed to draft a series of questions that form the basis of the certification exam. (See Appendix 3.)

Bringing Subject Matter Experts to the Table

To be accurate and to validate current knowledge, CompTIA first selects SMEs to construct a certification instrument. Each SME is required to sign a legally binding non-disclosure agreement³ precluding any profit motive in the credentials-training industry. This is done to address any potential conflicts of interest. To assure both a balanced and comprehensive product, SMEs are selected from a wide variety of disciplines and vertical markets, including government, private sector, and, where individuals are not in any way involved in course preparation or delivery for IT certifications, academic professions. Recent SMEs for CompTIA IT security certifications have included government professionals from the U.S. Department of Homeland Security, the U.S. Air Force, and the U.S. Navy. Private-sector experts from companies including Booz Allen Hamilton and Lockheed Martin have also participated. CompTIA allows no more than two individuals from the same organization or agency to participate in the process, ensuring that the exam is not skewed or biased toward any one agency or vendor technology.

After a group of qualified SMEs is selected, it is sequestered at CompTIA's headquarters (much like a deliberating jury in a legal setting) with precautions taken against tampering or outside influences upon the group's deliberations.

Creating a Job Task Analysis and Examination Blueprint

The foundation of a strong certification program is a Job Task Analysis (JTA) that defines the subject matter content that is valid for assessment. The JTA is then used to develop a blueprint to test against. The JTA, along with other test development procedures, helps ensure the defensibility of the resulting content. The collaborative nature of the process is underscored in the requirement that both the draft JTA and the draft examination blueprint cannot be received in final form until a significant volume of feedback is received from qualified professionals worldwide.⁴ The partnership between public, private, and academic sectors of the cybersecurity learning, research, and practice domains is clearly evident in the final product.

The Separation of Teaching and Learning Materials from Test Creation

Once the JTA and examination blueprint are published, a number of activities take place. Curriculum developers, book publishers, authors and designers, and other professionals begin developing teaching and learning materials for training and the eventual certification exam. CompTIA has maintained a policy of precluding all instructors, professors, authors, training executives, and even unauthorized members from its own organization (e.g., marketing and sales personnel) from the vital activities required in the creation of an examination. While there may be other avenues to a similar outcome, this process protects against proprietary knowledge obtained in the creation of a test from being used to “teach to the test.” CompTIA's practice is to maintain a clear wall of separation to protect the integrity and validity of the examination process.

³ For details about the agreement that SMEs must sign before participating in CompTIA's certification development process, see <http://www.comptia.org/certifications/examdevelopment.aspx>.

⁴ CompTIA generally seeks approximately 200 responses within the target audience in order to validate a JTA blueprint.

“The President has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter...The Executive Branch was also directed to work closely with all key players in US cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure US security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century.”

– The Comprehensive National Cybersecurity Initiative (CNCI), The White House, DECLASSIFIED 2010

Writing the Questions

Once the JTA and examination blueprint are completed, another group of SMEs is convened for the question-writing phase of the process. This is a difficult and precise process, because hundreds of questions are needed for the initial drafts of the exam. Questions are accepted based on their relevance to the material and the clarity of the question, with care to omit any ambiguities in terminology or verbiage.

Once the required number of questions mapped to every area on the examination blueprint is created, the examination—still in beta format—is published to the world. At authorized CompTIA testing centers, professionals are encouraged to take the beta examination and submit feedback. After the beta exam is completed, a standard-setting workshop is conducted to determine that valid inferences are made from the test. This is one of the most crucial steps in exam development. At the workshop, another group of SMEs estimates the number of minimally qualified candidates who would answer each question correctly. As such, the workshop determines the cut score, which is the demarcation between pass and fail.

Keeping the Credential Current, Valid, and Relevant

Given the type of threats and the corresponding levels of complexity of hardware and software to meet the exigencies of IT security, a valid certification examination must stay up to date. CompTIA relies upon a Certification Advisory Committee, yet another group of impartial industry experts, academics, and analysts who review the certification blueprint. This group reports significant developments in a subject area to CompTIA credential managers. If the committee recommends that additional technologies be addressed before a scheduled exam update, the development cycle is altered in order to cover all knowledge, skills, and abilities necessary to perform the job functions associated with cybersecurity—and yet another question-writing development cycle is added to the certification for that year.

As an example, since CompTIA's Security+ was first published in 2002, CompTIA has provided regular updates and major revisions to this ANSI/ISO 17024-accredited certification.⁵ Subject Matter Experts from the government, academic, and private sectors meet regularly to ensure that the content of the examination remains relevant and accurate. As the technology has evolved and the threats and exploits have grown (see Appendix 2), so too has the response in providing timely and accurate training materials and best practices.

How is a Certification Delivered?

In conjunction with its authorized examination centers worldwide, CompTIA takes several precautions to mitigate cheating. Individuals who cheat risk losing their credential and being reported to authorities and governing professional bodies. They also face legal prosecution if they divulge answers or other prohibited intellectual property relating to an examination.⁶

To deter cheating, a variety of proprietary technologies are employed. These include delivery and transmission of exams in encrypted formats, random scrambling of

⁵ Exams are updated with new questions every six to eight weeks. CompTIA is soon to launch its third major revision of the exam.

⁶ Pearson VUE, Prometric, and the Government Services Agency (GSA) through TestSmart are leading CompTIA testing partners. Incidentally, they are also the preferred testing providers for the DOD 8570 information assurance program.

examination questions and answers, pools of thousands of potential questions to stem the brute-force memorization of answers, and digital forensics such as biometrics and time-per-question analysis. The objective is to ensure that a CompTIA security certification is ethically created and honestly earned. Further, CompTIA participates in forums with other credential providers to maintain the integrity and security of IT certification credentials.

WHAT TO MEASURE IN A CREDENTIAL EXAMINATION: KNOWLEDGE OR PERFORMANCE?

There is an internal debate among cybersecurity practitioners as to what is more important to validate: 1) an individual's conceptual knowledge, or 2) performance associated with a particular job or responsibility. Advocates for each of these two aspects of validation may hold one of the approaches as superior over the other. However, CompTIA regards this growing rift as a false dilemma. Both domain knowledge expertise and practical skills are absolutely vital and should be a part of any serious competency training and validation process.

When a certification is developed or updated, CompTIA works closely with its learning partners to ensure training materials are available in the industry and are available in multiple mediums. Both knowledge- and performance-based aspects are necessary for training, and nothing can substitute for hands-on learning. Moreover, a significant portion of testing for CompTIA certifications includes scenario-based questioning that asks the test taker to react to real-life situations.

A meaningful benefit in certifications that are predominately knowledge-based, however, is that they help establish criteria or measure an individual's readiness and ability to move to higher-level and more complex certifications. This core base of knowledge provides confidence in situations not previously encountered and leads to the development of best practices, resulting from lessons learned in other settings. Psychometric validation that can accurately measure conceptual knowledge has existed for decades and is evident in the trustworthiness of high-stakes assessments such as the SAT, GRE, MDCAT, and LSAT. We need to know how to drive the car, to be sure, but we also need to know things about speed limits, right of way, and other conceptual knowledge before we can secure a driver's license. It's really not one or the other; it's a matter of authentically integrating both the practical and the foundational knowledge and then making sure that testing processes validate both types of knowledge.

Innovations that allow for test simulations will increasingly promote performance-based testing as appropriate for specific career paths and levels of expertise. In 2011, CompTIA will introduce its first mastery-level certification exam in the cybersecurity domain, the CompTIA Advanced Security Practitioner (CASP) certification exam. This exam will validate a higher level of skills required for both systems and network security. It is highly recommended that individuals taking this exam have a minimum of five years of technical security experience at the enterprise level. The CASP certification exam will have a special software design that allows for simulation-based items.

As cybersecurity specializations develop, expertise will lean toward performance-based criteria but will also continue to be supported by a foundation of core conceptual knowledge—much like a surgical internship practically validates a medical student who has already passed his or her graduation requirements. The key is to make sure that such a process does not unnecessarily bottle neck the cybersecurity education and training ecosystem. We need cybersecurity professionals who are trained and credentialed in a timely manner.

THE CompTIA PUBLIC-PRIVATE-ACADEMIC PARTNERSHIP: OPTIMUM RESPONSIVENESS TO RAPID DEVELOPMENTS IN THE CYBERSECURITY THREAT ENVIRONMENT

Through interaction with cybersecurity peers, we quickly learned that protecting networks is not a one-time exercise, but rather a constantly evolving process. Reliance on one particular channel, organization, or sector of the ecosystem would be shortsighted. CompTIA believes the cybersecurity challenges of today and tomorrow can be solved by dedicated professionals working in a collaborative setting, utilizing the best available technical tools.

CompTIA certifications along with training provided by partners are an indispensable piece of an entire ecosystem that stands at the ready to protect our vital digital infrastructure. Ultimate success can only be found in a plurality of approaches—and IT certification plays a critical role in a collective process.

Occasionally, recommendations arise that suggest all cybersecurity certification programs be consolidated under a single entity, such as a government agency or academic program. There have also been suggestions that the government author its own internal cybersecurity credentials. Such recommendations overlook basic facts:

- 1) America's critical infrastructure comprises far more than just government and defense networks. Industrial, transportation, economic, commercial, and energy networks increasingly are digitally driven and are equally vital to the national interest. The complex cyberspace infrastructure relationships, as identified by the U.S. Department of Homeland Security, are illustrated in Appendix 4. The same expertise that secures our government networks must closely collaborate with those who secure other vital national networks.
- 2) Most government-controlled digital networks are managed by a combination of military and civilian personnel. Attempts to certify only one segment of the professionals securing these networks would be shortsighted and incomplete.
- 3) Networks are most secure when they are protected by professionals who 1) have distinct career responsibilities and focus, and 2) leverage the best of the government, commercial, and academic sectors. This workforce must be composed of individuals whose training and expertise is as diverse and resilient as the threats they face.

The wide variety of training, educational, and credential options testifies to the varied career paths that are required for IT security. It also confirms the need to validate skills in a rapidly

changing digital world. Similar to our efforts to bring clarity to the credentialing world, the government is also working to define Federal information assurance job functions and roles, which will allow for a more effective public-private partnership effort to map credentials. Working through its liaison relationships, academia⁷, the Defense Department⁸, and the National Institute of Standards and Technology⁹, CompTIA and the private sector credentialing community continue to support and collaborate on efforts to train and validate the skills and know-how needed to secure digital networks for years to come.

CompTIA AND THE CYBERSECURITY CREDENTIALS INDUSTRY: GOOD AND GETTING BETTER

As domain areas in cybersecurity continue to evolve, there is a corresponding increase in credentials that validate new skill sets. While proliferation of credentials can lead to confusion, in most cases the distinctions among them can be understood when one considers the particular domain addressed, as well as the complexity of the skill and any reference to vendor-specific or vendor-neutral expertise. Appendix 1 is a visual representation of the Cybersecurity Credentials Ecosystem. This illustration lists only some of the leading sponsoring organizations, their relationship to a particular function, and their relation to technical, auditing, or management practice levels.

A simple but important way to distinguish valid credentials from “fly-by-night” entrants is to consult the American National Standards Institute (ANSI).¹⁰ ANSI maintains a personnel certification accreditation program, and governmental agencies in key sectors such as national security, public safety, and healthcare rely on ANSI accreditation for third-party verification of the competence of certification bodies. ANSI is the only personnel certification accreditation body in the U.S. to fulfill the globally recognized requirements of ISO/IEC 17011:2004, which represents the highest internationally accepted practices for accreditation bodies. So, for example, all CompTIA certifications that are used by the U.S. Department of Defense 8570.1 Directive are both ANSI and ISO certified.

CompTIA also works closely and collaboratively through meetings and engagements with peer certification organizations and stakeholders in government, academia, and the private sector. The shared objective is to align credentials to identified career pathways, inform senior IT leadership and the educational community about the role of cybersecurity credentials, and provide continuous improvement and management of the credentialing ecosystem. It is incumbent upon those of us in the IT security credentials world to align our various organizations and vendor companies in order to publicize more coherent and interrelated career paths—from entry-level to mastery levels of IT expertise. In this manner we will continue to inspire trust and support from IT and HR personnel in the cybersecurity world.

7 CyberWatch (<http://www.cyberwatchcenter.org>)

8 DOD Information Assurance Workforce Improvement Program (www.dtic.mil/whs/directives/corres/pdf/857001m.pdf)

9 National Initiative for Cybersecurity Education (NICE) (<http://csrc.nist.gov/nice/education.htm>)

10 Refer to the ANSI Accreditation Directory (<https://www.ansica.org/wwwversion2/outside/PERdirectory.asp?menuID=2>)

GLOSSARY

ANSI. American National Standards Institute, a 501(c)(3) non-profit association and the voice of the U.S. standards and conformity assessment system. While helping to assure the safety and health of consumers and the protection of the environment, ANSI oversees the creation, promulgation, and use of thousands of norms and guidelines that directly impact businesses in nearly every sector—from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accrediting programs that assess conformance to standards, including globally recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

Bloom's Taxonomy. A classification scheme of intellectual behavior developed by Benjamin Bloom who identified six levels of cognitive learning—from the simple recall of facts (Knowledge), as the lowest level, through the increasingly complex levels of Understanding, Application, Analysis, Synthesis, and Evaluation.

CompTIA A+ Certification. The CompTIA A+ certification is the industry standard for computer support technicians. The international, vendor-neutral certification proves competence in areas such as installation, preventative maintenance, networking, security, and troubleshooting. CompTIA A+ certified technicians also have excellent customer service and communication skills to work with clients.

CompTIA Network+ Certification. The CompTIA Network+ certification is the sign of a competent networking professional. It is an international, vendor-neutral certification that proves a technician's competency in managing, maintaining, troubleshooting, installing and configuring basic network infrastructure. Since its introduction in 1999, more than 235,000 people have become CompTIA Network+ certified.

CompTIA Security+ Certification. CompTIA Security+ is an international, vendor-neutral certification that proves competency in system security, network infrastructure, access control, and organizational security.

Critical IT Infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for: electricity generation, transmission and distribution; gas production, transport, and distribution; oil and oil products production, transport, and distribution; telecommunication; water supply (drinking water, waste water/sewage, and dikes and sluices); agriculture, food production, and distribution; heating (e.g., natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railway network, airports, harbors, inland shipping); financial services (banking, clearing); and security services (police, military). (Wikipedia)

Cyberspace. Cyberspace is a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP1-02)

Cybersecurity. A synonym of Information Security as cited in ISO 27001.

Examination Blueprint is a document related to a particular area of domain knowledge, composed of one or many learning objectives. A learning objective answers the question: What is it that an individual should be able to do or know? A learning objective makes clear the intended learning outcome rather than what form the instruction will take. Learning objectives focus on student performance. Action verbs that are specific, such as list, describe, report, compare, demonstrate, and analyze should state the behaviors students are expected to perform. Clearly defined objectives form the foundation for selecting appropriate content, learning activities, and assessment measures. (From Patricia Archer, 1979, *Writing Higher-Level Learning Objectives: The Cognitive Domain*, New York: Media Systems Corporation)

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. The global information grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called GIG. (JP 6-0)

Global Information Infrastructure. The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (JP 3-13)

Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DOD 8500.01E, October 24, 2002, recertified April 23, 2007)

Information Security is defined as the preservation of the confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved (ISO/IEC 17799:2005). Also see NIST 800-30, "Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically. The five security goals are integrity, availability, confidentiality, accountability, and assurance."

ISO. The International Organization for Standardization, a standard-setting body composed of representatives from various national standards organizations. Founded on February 23, 1947, the organization promulgates worldwide proprietary industrial and commercial standards. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments. (Wikipedia)

Job Task Analysis (JTA). The formal process of defining the requirements of a position and identifying the knowledge, skills, and abilities necessary to effectively perform the duties of the position. (www.hss.energy.gov/DepPersonnelSec/hrp/html/glossary.htm)

Malware. Software such as viruses or “Trojan Horse” programs designed to cause damage or disruption to a computer system. (AFDD 3-12)

Psychometrics. Psychometrics is the field of study concerned with the theory and technique of educational and psychological measurement, which includes the measurement of knowledge, abilities, attitudes, and personality traits. The field is primarily concerned with the construction and validation of measurement instruments, such as questionnaires, tests, and personality assessments. It involves two major research tasks, namely: (i) the construction of instruments and procedures for measurement; and (ii) the development and refinement of theoretical approaches to measurement. Those who practice psychometrics are known as psychometricians and although they may also be clinical psychologists, they are not obliged to be so and could instead be, for example, human resources or learning and development professionals. Either way specific, separate qualifications in psychometrics are required. (Wikipedia)

Subject Matter Expert (SME). An SME or domain expert is a person who is an expert in a particular area or topic. When spoken, sometimes the acronym «SME» is spelled out («S-M-E») and other times voiced as the word “smee.”

APPENDIX 1

Credentials, Certificates, Certifications: Clearing the Confusion Cyber security

Cyber Warrior				
Master	EC Council, GIAC			
Journeyman	EC Council, GIAC			
Apprentice	EC Council, GIAC			

Information Assurance				
	Audit	Technical	Management	Vendor Specific
Master	ISACA	ISC2 EC Council ISACA GIAC	ISC2 EC Council ISACA GIAC	Cisco Microsoft Etc ... Cisco
Journeyman	ISACA	ISC2 EC Council ISACA GIAC CompTIA	ISC2 GIAC ISACA CompTIA	Microsoft Etc ...
Apprentice	ISACA	CompTIA ISACA GIAC EC Council	CompTIA ISACA GIAC	Cisco Microsoft Etc ...
	Process People	Technology People	Process People	Technology People

College	CompTIA, GIAC, EC Council, Cisco, Microsoft
High School	CompTIA, Cisco, Microsoft

APPENDIX 2

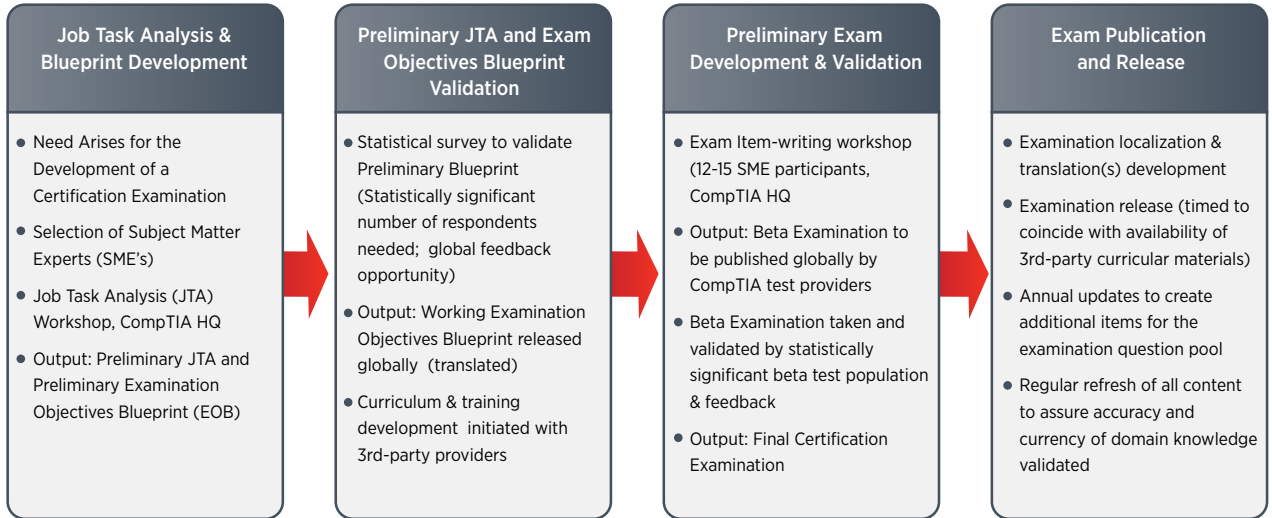
Threats in Cyberspace¹¹

Type of Threat	Nature of Threat Parameters
Nation State	This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Other nations may employ cyberspace to attack and conduct espionage against the U.S. Nation-state threats involve traditional adversaries and sometimes, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource third parties to achieve their goals.
Transnational Actor	Transnational actors are formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist action.
Criminal Organization	Criminal organizations may be national or transnational in nature depending on how they are organized. Criminal organizations steal information for their own use or, in turn, sell it to raise capital.
Individual or Small Group Network	Individuals or small groups of people can illegally disrupt or gain access to a network or computer system—these people are better known as hackers. The intentions of hackers vary. Some are peaceful and hack into systems to discover vulnerabilities, sometimes sharing the information with the owners and some have malicious intent. Other hackers have political motivations and use cyberspace to spread their message to target audiences. Another type of hacker desires fame or status, and obtains it by breaking into secure systems or creating malware that creates havoc on commercial or government systems. Malware is the short name for malicious software. Hackers can also be exploited by the other cyberspace threats, such as criminal organizations, in order to execute concealed operations against specific targets while preserving their identity or create plausible deniability.
Traditional	Traditional threats typically arise from states employing recognized military capabilities and forces in well-understood forms of military conflict. Within cyberspace, these threats may be less understood due to the continuing evolution of technologies and methods. Traditional threats are generally focused against the cyberspace capabilities that enable our air, land, maritime, special operations, and space forces and are focused to deny the U.S. military freedom of action and use of cyberspace.
Catastrophic	Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. While WMD attacks are physical (kinetic) events, they may have profound effects within the cyber domain by degrading or destroying key cyber-based systems vital to infrastructure like SCADA systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly even globally. For example, an electromagnetic pulse could cause widespread damage to segments of the cyberspace domain in which operations must occur.
Natural	Natural threats that can damage and disrupt cyberspace include events such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring the DOD to maintain or restore key cyberspace systems. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.
Accidental	Accidental threats are unpredictable and can take many forms. From a backhoe cutting a fiber optic cable of a key cyberspace node to inadvertent introduction of viruses, accidental threats unintentionally disrupt the operation of cyberspace. Although post-accident investigations show that the large majority of accidents can be prevented and measures put in place to reduce accidents, accidents should be anticipated.

¹¹ Adapted from "National Military Strategy for Cyberspace Operations", 2006.

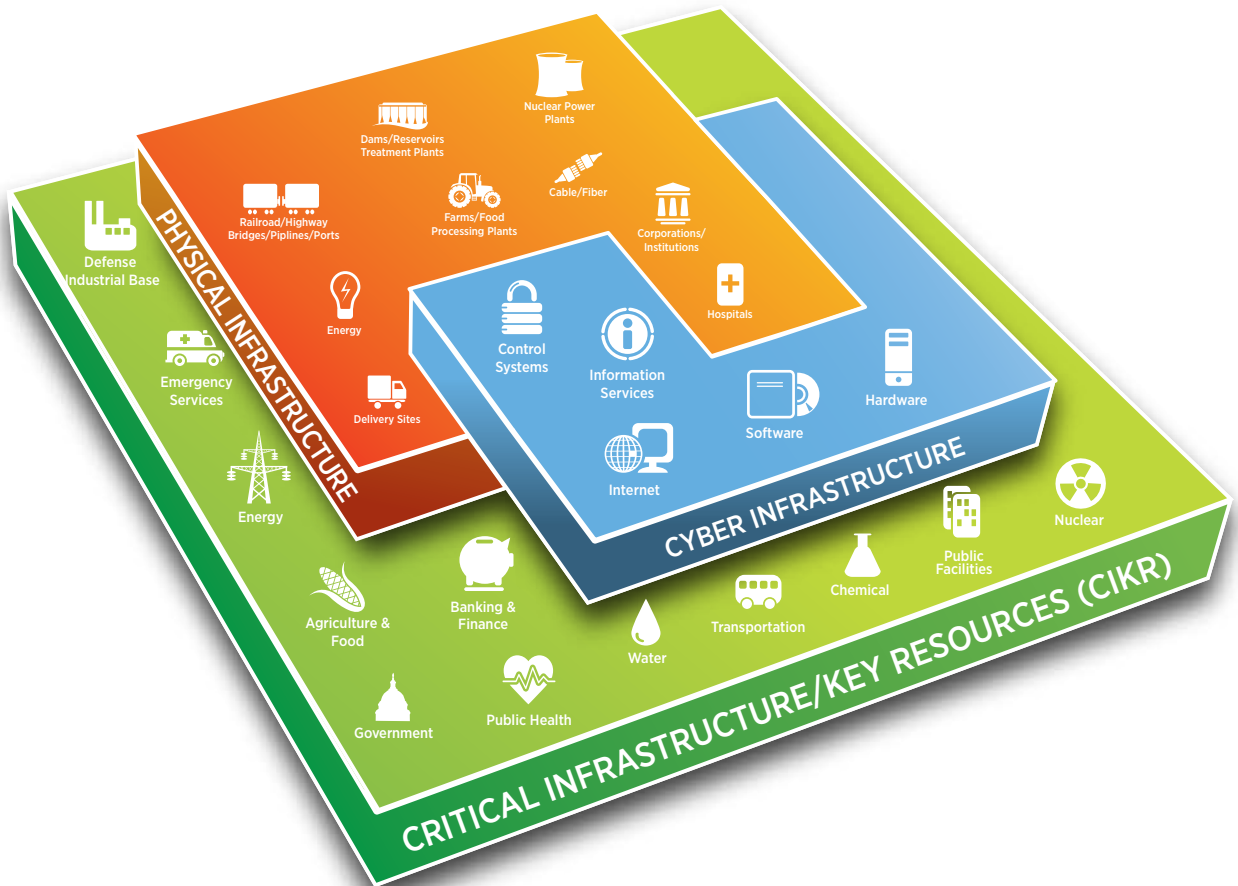
APPENDIX 3

Certification Exam Development Process



APPENDIX 4

Cyberspace Infrastructure Relationships¹²



¹² Adapted from "Securing the Nation's Critical Cyber Infrastructure," US Department of Homeland Security

ABOUT CompTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association representing the information technology (IT) industry and the leading global provider of vendor-neutral IT certifications. CompTIA represents over 2,500 IT companies. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. CompTIA members include major computer hardware manufacturers, software developers, technology distributors, and IT specialists that help organizations integrate and use technology products and services. CompTIA is dedicated to serving its membership by advancing industry innovation and growth through its educational programs, market research, networking events, professional certifications, and public policy advocacy.



www.comptia.org

CompTIA Worldwide Headquarters

CompTIA Member Services, LLC

3500 Lacey Road, Suite 100,

Downers Grove, Illinois 60515

630.678.8300

www.comptia.org