National Initiative for Cybersecurity Careers and Studies

Concept:

NICCS changes the way we train for and think about Information Security. Past strategies have always been to chase certification bodies and follow what they want to teach and test us on as security professionals.

The problem was a potential conflict of interest, and the cyber security professional was left to “play along.” We needed an impartial view. We needed an organizational map for all of us: government, military, and the world.

The NICCS framework defines professional requirements in Cybersecurity, much as other professions, such as medicine and law, have done. Cybersecurity is organized into seven categories, each with specialty areas wherein the required knowledge, skills, abilities, and tasks are mapped out.

When NICCS clearly defined 40 Cybersecurity specialty areas, they did us all a great service. Outlining these specialty areas allows the Security Professional to take control of our own learning, by putting the power of career and training decisions into our own hands.

With the NICCS framework, Cybersecurity Careers are successfully shifting from fragmented certifications to streamlined professionalization.

At Expanding Security, we reorganized our training content to match the NICCS framework of Cybersecurity education. We did not force our courses to fit NICCS; we rebuilt from the ground up.

Our NICCS courses directly mirror the requirements of each NICCS specialty area.

Each specialty area can be thought of as the totality of knowledge, skills, ability and tasks that need to be performed. Our courses arm the Security Professional for successful execution.

NICCS has also defined the basic levels of knowledge that are required for a security professional, consistent with the college level course themes being 100 to 400.

You may have a high degree of advanced understanding in a few tasks and knowledge areas but missing others in a Specialty Area. A useful feature in our courses is that you can opt to test out of the General Knowledge area and show competency.

NICCS ES website courses:

All courses incorporate streamlined training based directly on the KSA’s and Tasks designated in the NICCS learning objectives. Each item will be covered in a single meeting. The tasks typically equate to labs. The knowledge, skills, and abilities tend toward lecture and discussion. There are readings before each session and a quiz at the end to validate the learning.

Minimum prerequisites for all NICCS Courses: 3 years administration of computing environment.

(All) General Knowledge Areas:

Course Length: 5 hours. The 5 KSA's and Tasks that are covered in all specialty areas of NICCS v2. If you are attending any NICCS 101 course, this course is free. If you choose to skip this course you must pass a 50 question pre-test with at least a 90%. This course introduces you to the main concepts of NICCS.

NICCS Course Customer Service and Technical Support 101

Course length: 28 hours. Objectives: To build the Functional Development of Customer Service and Technical Support personnel and understand how to accomplish the goals, skills, and tasks required including knowing network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth), and acquiring skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.

Data Administration 101

Course length: 43 hours. Objectives: To build Functional Development for Data Administration personnel and understand how to accomplish the goals, skills, and tasks required including learning skills in optimizing database performance, designing databases, and allocating storage capacity in the design of data management systems.

Digital Forensics 101

Course Length: 40 hours. Objectives: To understand the management development of digital forensics personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including knowing network security architecture concepts such as topology, protocols, components, and principles (e.g., application of defense-in-depth); preserving evidence integrity according to standard operating procedures or national standards, knowing types of digital forensics data and how to recognize them. This course is an excellent primer for technologists who want to understand what they would be doing as a Digital Forensics Examiner.

Enterprise Network Defense Analysis 101

Course Length: 40 hours. Objectives: To build the Functional Development of Computer Network Defense Analysis personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including learning intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies, detecting host and network based intrusions via intrusion detection technologies (e.g., Snort), learning cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities. Learn defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Enterprise Network Defense Infrastructure Support 101

Course Length: 34 hours. Objectives: To build the Functional Development of Computer Network Defense Infrastructure Support personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including using incident handling methodologies, knowing data backup, types of backups and recovery concepts and tools, knowing processes for reporting network security related incidents, securing network communications.

Incident Response 101

Course Length: 40 hours. Objectives: To learn how to respond to crises or urgent situations within this domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches to maximize survival of life, preservation of property, and information security. To know general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks). To learn cyber defense policies, procedures, and regulations, investigation and analysis of all relevant response activities and handling methodologies.

Information Systems Security Operations 101

Course Length: 51 hours. Objectives: To learn how to oversee the information assurance program of an information system in or outside the network environment, which may include procurement duties. To build the Functional Development of Information Systems Security Operations personnel and understand how to accomplish the goals, skills, and tasks of this specialty area. The following positions would benefit from this course: Contracting officer, Information Assurance Manager, Program Manager, Security Officer, Information Systems Security Manager, Operator, and Officers.

Network Services 101

Course Length: 56 hours. Objectives: To build the Functional Development / Management Development of Network Services personnel and understand how to accomplish the goals, skills, and tasks of this specialty area, including analyzing network traffic capacity and performance, and protecting networks against malware.

Secure Software Engineering 101

Course Length: 40 hours. Objectives: To build the Functional Development of Secure Software Engineering personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including knowledge of interpreted and compiled computer languages, knowledge of secure coding techniques.

Strategic Planning and Policy Development 101

Course Length: 40 hours. Objectives: To apply knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy

that will support new initiatives or required changes. The following people would benefit from this course: CIO, Command Information Officer, Information Security Policy Analyst and Manager, Policy Writers and Strategists.

System Administration 101

Course Length: 54 hours. Objectives: to build the Functional Development / Management Development of System Administration personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including learning to maintaining directory services, configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware), learning server diagnostic tools and fault identification techniques.

Systems Development 101

Course Length: 40 hours. Objectives: To build the Functional Development of Systems Development personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including how to develop and apply security system access controls, create policies that reflect system security objectives, conduct audits or reviews of technical systems.

Systems Security Architecture 101

Course Length: 40 hours. Objectives: to build the Management Development of Systems Security Architecture personnel and understand how to accomplish the goals, skills, and tasks of this specialty area including knowledge of cryptography and cryptographic key management concepts, knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework –TOGAF), Department of Defense Architecture Frame.

Vulnerability Assessment and Management 101

Course Length: 43 hours. Objectives: to build the Functional Development of Vulnerability Assessment and Management personnel and understand how to accomplish the goals, skills, and tasks of this course.

Risk Management 101

Course Length: 39 hours. Objectives: To learn the skills to oversee, evaluate, and support the documentation, validation, and accreditation processes necessary to ensure new and existing information technology (IT) systems meet the organization's information assurance and security requirements. Develop methods to monitor and measure risk, compliance, and assurance efforts.

NICCS catalogue courses:

All of the following Expanding Security NICCS courses are listed in the NICCS Catalogue:

We have done your homework: with the vast list of NICCS courses, we know some will grow in importance and we carefully selected key courses from the 7 Categories as "must haves."