

National Initiative For Cybersecurity Education (NICE)

[Click Here to view SecureNinja's course alignment with the NIST's NICE Framework"](#)

SecureNinja Course Alignment with NICE CyberSecurity Workforce Framework's Careerpaths™

SecureNinja Course Alignment with NICE CyberSecurity Workforce Framework's Careerpaths™ are copyrighted by SecureNinja DBA SecureNinja. ©2012 SecureNinja DBA SecureNinja. All Rights Reserved.

Secure Ninja, a leader in Information Security training and services, has aligned our course offerings with the recent NIST initiative; The National Initiative For Cybersecurity Education (NICE)™. This mapping of Secure Ninja training courses to the NICE Frameworks' specialty areas/job titles simplifies the development of your personal or organization's training and education roadmap.

What is the NICE Cybersecurity Workforce Framework?

Today, there is little consistency in how cybersecurity work is defined and described throughout the nation. The lack of a common language to discuss and understand the work requirements of cybersecurity professionals hinders our nation's ability to:

- Baseline capabilities,
- Identify skill gaps,
- Develop cybersecurity talent in the workforce, and
- Prepare the pipeline of future talent.

Establishing and using a unified framework for cybersecurity work and workers is not

merely practical but vital to the nation's cybersecurity. Much as other professions have defined their specialties (e.g., law, medicine), it is now time to forge a common set of definitions for the cybersecurity workforce. The NICE Cybersecurity Workforce Framework offers a working taxonomy and common lexicon that can be overlaid onto any organization's existing occupational structure.

About National Initiative For Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) has evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security.

Purpose

The NICE Strategic Plan identifies goals and objectives that will contribute to the realization of a cyber-secure public and a globally competitive cybersecurity workforce.

NICE Mission

NICE will enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population.

NICE Vision

A secure digital nation capable of advancing America's economic prosperity and national security in the 21st century through innovative cybersecurity education, training, and awareness on a grand scale.

1. Raise awareness among the American public about the risks of online activities.
2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce.

The National Institute of Standards and Technology (NIST) is leading the NICE initiative, comprised of over 20 federal departments and agencies, to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability. Many NICE activities are already underway and NIST will highlight these activities, engage various stakeholder groups and create forums for sharing information and leveraging best practices. NIST will also be looking for "gaps" in the initiative -- areas of the overarching mission that are not addressed by ongoing activities.

To speak with a Secure Ninja NICE training solution specialist on planning your education roadmap call 703-535-8600.

[Click Here to view SecureNinja's course alignment with the NIST's NICE Framework](#)