NICE framework provides resource for a strong cybersecurity workforce

November 3 2016

The NICE Cybersecurity Workforce Framework provides building blocks for a trained workforce. Credit: Natasha Hanacek/NIST

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) released a resource that will help U.S. employers more effectively identify, recruit, develop and maintain cybersecurity talent. The draft NICE Cybersecurity Workforce Framework (NCWF) provides a common language to categorize and describe cybersecurity work to help organizations build a strong staff to protect their systems and data. It was announced today at the 2016 NICE Conference and Expo.

Cybersecurity is still a nascent and rapidly developing field in which job titles and role descriptions vary from organization to organization and

sector to sector. The NCWF can be viewed as a cybersecurity workforce dictionary that will help organizations define and share information in a detailed, consistent and descriptive way.

The NICE workforce framework was developed by the NIST-led National Initiative for Cybersecurity Education (NICE) and is the culmination of many years of collaboration between industry, government and academia. The U.S. Departments of Defense and Homeland Security were significant contributors.

The NCWF was designed to serve several key groups, including employers, current cybersecurity staff, students and workers considering a career in the field, educators and workforce trainers and technology providers.

In addition to helping educate, recruit, train and retain a qualified cybersecurity workforce, the NCWF will serve as a building block for the development of training standards, as well as for individual career planning. It will also allow organizations to develop a more realistic image of their cybersecurity workforce.

"When identifying their cybersecurity staff, many organizations overlook cybersecurity tasks being performed by lawyers, auditors and procurement officers," said Bill Newhouse, NICE deputy director and lead author of the document. "The NCWF can help an organization identify cybersecurity tasks within a work role that are vital to its mission and then examine if its current staff can perform those tasks and, if not, hire staff who can."

The NCWF organizes the workforce into an overarching structure of seven high-level categories that group work and workers sharing common functions. Two examples are "Oversight and Govern" and "Protect and Defend." The seven categories are made up of more than

30 specialty areas such as "Incident Response" and "Legal Advice and Advocacy." Some specialty areas map to a single work role and others are contained in more than one work role.

The more than 50 work roles defined in the framework include "cyber legal advisor" and "vulnerability analyst." Each work role is defined by extensive sets of related knowledge, skills and abilities (KSAs) and tasks.

The federal government will soon be using the NCWF to identify its cybersecurity workforce, as directed by the Federal Cybersecurity Workforce Assessment Act of 2015 (Division N, Consolidated Appropriations Act, 2016).

Provided by National Institute of Standards and Technology