NICE issues cybersecurity workforce framework for public comment

November 9 2011

The National Initiative on Cybersecurity Education (NICE) has published for public comment a draft document that classifies the typical duties and skill requirements of cybersecurity workers. The document is meant to define professional requirements in cybersecurity, much as other professions, such as medicine and law, have done.

NICE is an interagency effort coordinated by the National Institute of Standards and Technology (NIST) and focused on cybersecurity awareness, education, training and professional development. NICE activities include increasing cybersecurity awareness for children and adults of all ages, promoting community college and university-level programs in cybersecurity, and expanding professional training opportunities.

The new document, the NICE Cybersecurity Workforce Framework, was created by the NICE group responsible for creating and maintaining a highly skilled workforce to meet the nation's computer security needs. Over 20 participating agencies contributed to the group's efforts.

"One thing NICE has found is that there has not been a consistent way to define or describe cybersecurity work across the federal workforce," says NICE Lead Ernest McDuffie. Cybersecurity professionals previously have not fit into the standard occupations, job titles, position descriptions and the federal job classification and job grading system managed by the Office of Personnel Management (OPM).

Not having a common language to discuss and understand the work and skill requirements hinders federal employers in setting basic requirements, identifying skill gaps and providing training and professional development opportunities for their workforce. "Other professions have organized their specialties, and now it is time for a common set of definitions for the cybersecurity workforce," said McDuffie.

The NICE Cybersecurity Workforce Framework provides a working taxonomy, or vocabulary, that is designed to fit into any organization's existing occupational structure. The framework is based on information gathered from federal agencies through two years of surveys and workshops by OPM, a major Department of Defense study of the cybersecurity workforce and a study by the Federal CIO Council.

In opening the draft document up for public comment, NICE hopes to refine the framework so that it can be useful in both the public and private sectors to better protect the nation from escalating cybersecurity threats. Authors also want the framework to address emerging work requirements to help ensure the nation has the skills to meet them. The authors are requesting input from all of the nation's cybersecurity stakeholders including academia, professionals, not-for-profit organizations and private industry.

The framework organizes cybersecurity work into high-level categories ranging from the design, operation and maintenance of cybersecurity systems to incident response, information gathering and analysis. The structure is based on job analyses and groups together work and workers that share common major functions, regardless of job title.

More information: To read the document and provide comments, go to csrc.nist.gov/nice/framework/. The webpage also provides a template for comments, which are due Dec. 16, 2011.