

Feds Strengthen Cybersecurity Workforce Plans

As the pressure mounts on government to keep its systems secure, efforts to improve the federal cybersecurity, particular hiring practices for cybersecurity pros, are pushing forward.

By J. Nicholas Hoover, [InformationWeek](#)

Aug. 13, 2010

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=226700237>

Federal agencies are making some progress on developing and executing strategies for building a stronger cybersecurity workforce, but much remains to be done, government officials and industry representatives said at a conference this week.

Coordinated efforts to spark improvements in the federal cybersecurity workforce, formerly part of the Comprehensive National Cybersecurity Initiative (CNCI), have been folded into a larger effort, the National Initiative for Cybersecurity Education (NICE), a broader national agenda, announced in April, which includes K-12 education and awareness campaigns as well as federal workforce efforts.

"We want to become a resource to not only get the federal government up to the best level it can be, but to be a leader for the rest of the country," NIST's NICE program lead, Dr. Ernest McDuffie, said in an interview.

In terms of government, NICE includes two tracks of work focused explicitly on improving the federal cybersecurity workforce -- one on workforce structure, and the other on training and professional development. Some of the work under these buckets had already begun when NICE began, but it's beginning to accelerate.

For example, the Office of Personnel Management embarked on a path to sharpen and redefine cybersecurity job policies last November, and that effort is picking up steam. Earlier this year, working groups began re-defining competency models -- key roles and responsibilities -- for cybersecurity pros in government. Soon, OPM will survey agencies to get feedback on draft competency models, and plans to release the final competency models in December.

However, the competency models are only the first step. OPM and auditors have long found cybersecurity pros working in a number of federal job series -- groups of formally defined jobs -- and there's still some consideration of whether the cybersecurity workforce needs its own series to help better define what cybersecurity pros do. OPM is also considering whether hiring authorities and practices need to change, Maureen

Higgins, OPM's assistant director for agency support and technology assistance, said in an interview.

Work on workforce structure seems to be moving along, but training and professional development suffer from numerous challenges, such as a muddle of certifications, required skills and training that can sometimes make it difficult for hiring managers to determine who's qualified or just what additional training their employees need.

Some things under consideration in terms of workforce development include the use of a practical, hands-on exam to determine qualifications. "There's some divisiveness here, so we're trying to get to what makes sense here," John Mills, special assistant to the CNCI from the office of the assistant secretary of defense for networks and information integration, said in a presentation.