CSIS Roundtable Discussion
The Manpower Crisis in Cyber Security: Promising Solutions

During the deliberations of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, one of the great challenges identified by the commission members was the shortage of security professionals with the deep technical skills needed to eliminate or mitigate the damage from more sophisticated cyber attacks that increasingly plague U.S. government and industry sites. The manpower problem was deemed so acute that the Commission formed a special panel that documented its dimensions and scale in a report entitled "A Human Capital Crisis in Cyber Security." (http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity) However, in the months since the report was released, the cyber threat to the nation has come into sharper focus, and the critical shortage of technical skills has become even more evident. As a result the U.S. Cyber Challenge (USCC) is convening a roundtable discussion with cyber security leaders to deal with specific aspects of the problem that need immediate action:

- Estimates of 30,000 additional technical security professionals have been widely circulated. What are the jobs that need to be done? Where are they (employers)? What skills are needed?
  It appears many students graduating from cyber security programs in colleges and graduate schools are capable of "talking" about security but cannot actually perform the tasks required to protect systems or to find attackers who have breached the perimeter. Is it time to establish a minimum set of qualifications of technical skills to be taught and tested in cyber security programs?
- Nearly all security vulnerabilities in software are created by programmers who write code and design systems that have security flaws. Colleges that graduate people who become programmers do not appear to be ensuring those people know how to write safe code or find security flaws in the code they are writing. Should colleges be incentivized to transform their programming courses so security is an integral part of the teaching and grading? Should federal funding be contingent on the schools implementing secure code training as a core part of their curricula?

Where? The USCC Western Regional Cybersecurity Camp located at San Jose State University in the Student Union as a lunch discussion with the camp participants. The address is:

San Jose State University
One Washington Square
San Jose, CA 95192
Contact: Virginia Lehmkuhl-Dakhwe virginia.lehmkuhldakhwe@sjsu.edu

When? Tuesday, August 12, 2014

Who will participate in the Roundtable? The Roundtable will be co-hosted by Dr. Ernest McDuffie, Lead for the National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology and Darren Ash, Co-Chair for the Workforce Committee of the Federal Chief Information Officers (CIOs) Council and the Deputy Executive Director for Corporate Management and CIO for the Nuclear Regulatory Commission and other participants include Karen S. Evans, National Director for the US Cyber Challenge, Stuart Solomon, VP Technical Services and Client Operations, iSight Partners, Chris Bjornson, Chief Information Officer, Accenture Federal Services, and other leaders from industry and government.

What is the desired outcome? The camp participants will understand the dimensions of the problem they will help solve and see how critical their technical skills are to the solution. They will also learn about opportunities. All of those will help keep them involved in USCC and with STEM activities. We hope this panel will make the workforce issues and opportunities "real" for them.