From: Tony Sager <tsager@sans.org>
Date: Saturday, April 6, 2013 10:01 AM
To: cyberframework <cyberframework@nist.gov>
Cc: Tony Sager <tsager@sans.org>
Subject: The Cyber Workforce and the Executive Order

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Topic: The Cyber Workforce and the Executive Order

At the first NIST/EO Workshop (April 3) there were questions about the development of the cyber workforce, and would this be addressed in the Framework? The answer given was generally positive, but did not sound definitive. Although cyber workforce issues are not specifically named in the EO, they could be seen as covered by the stated need for "best practices" and "business...approaches".

I believe that it is important to consider both technical/process standards as well as workforce skill issues together. Technical cybersecurity controls without appropriately skilled people to execute them will fail. And one of the key measures of a successful cybersecurity framework will be its ability to minimize the manual and error-prone "grunt work" of defense, and to empower people for more worthy activity.

I recommend consideration of the report of the DHS Cyberskills Task Force, found at....

https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

This report, created by a very senior group representing a very wide range of publlc-private views, in effect established a roadmap for organizational best practice in cyber workforce development. It includes proven ideas from both public and private organizations with extensive experience in this area. The key themes of the report include:

- focusing on mission critical jobs;
- identifying the specific hands-on skills required to execute those jobs;
- looking to early identification as well as non-traditional sources (e.g.., community colleges, separating Veterans) in order to increase the workforce pool;
- aligning the organizational system of identification, hiring, training, continuous assessment, contracts/acquisition etc around those skills.

The report is consistent with the large, all-encompassing **National Cybersecurity Workforce Framework** from NICE, but focuses instead on jobs with the highest mission/business impact, and refines the specific hands-on job skills needed to a much greater level of detail.

The report has the merit of being fully accepted by DHS, and is now being implemented as the Cybersecurity Management Support Initiative(CMSI) -- with organizational changes to institutionalize these recommendations across the entire Department.

In addition, some of the ideas from the Report are being developed and expanded nationally. Most notably, the CyberAces Foundation (http://www.cyberaces.org/) is building a consortium of State governments, Community Colleges, and employers to create a full ecosystem of early identification (through on-line gaming and simulation), core technical knowledge, special cyber training, and guided employment ("residencies"). This has the potential to dramatically increase the workforce pool, focus the training on the specific critical skills, and provide sponsored pathways into employment. The first pilot activities are underway.

The work required to build such an ecosystem highlight the lack of a national framework for licensing and certification processes such as those found in more mature fields, especially for pilots and doctors (which were some of the models examined by the Task Force).

thank you

Tony Sager
Director, The SANS Institute
Member, DHS Cyberskills Task Force