Internal DHS Efforts to Implement the NICE Framework

September 18, 2013

Background

- In June 2012, the Secretary established a Homeland Security Advisory Council (HSAC) Task Force on CyberSkills with a two-part mandate:
  - To identify the best way DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges; and
  - To outline how DHS can improve its capability to recruit and retain the cybersecurity talent it needs.

- The HSAC CyberSkills Task Force Report released in the Fall of 2012 included specific findings and recommendations for improvement.

- DHS launched the CyberSkills Management Support Initiative (CMSI) to provide continued support to the cybersecurity workforce by focusing on:
  1. Hiring, testing, and training to standards;
  2. Growing and expanding the pipeline for talent;
  3. Strategically managing the workforce;
  4. Aligning procurement and contracting for cybersecurity services; and
  5. Creating a cyber surge capacity force.

Background

- The Task Force identified an initial set of DHS mission critical cybersecurity skills (or tasks):
  1. System and Network Penetration Tester
  2. Application Penetration Tester
  3. Security Monitoring and Event Analysis
  4. Incident Responder In-Depth
  5. Threat Analyst / Counterintelligence Analyst
  6. Risk Assessment Engineers
  7. Advanced Forensics Analysts for Law Enforcement
  8. Secure Coders and Code Reviewers
  9. Security Engineers - Operations
  10. Security Engineers / Architects for Building Security-In

DHS Existing Workforce Tracking

- As part of efforts to strategically manage the DHS cybersecurity workforce, CMSI has created a Cybersecurity Workforce Inventory database, which is populated with data on positions/employees known to be performing mission critical cybersecurity tasks, as defined by the current list of 10 DHS tasks.

Implementing the Cyber Data Element

- To address the requirement of the July 8, 2013 “Special Cybersecurity Workforce Project” from OPM, DHS is expanding its existing workforce tracking to capture additional data.

- Initially, DHS will focus on identifying the appropriate Cybersecurity Category/Specialty Area codes for the subset of positions/employees that have been identified as performing DHS mission critical tasks and are already captured via our existing reporting process.

- DHS has already created a crosswalk of our mission critical tasks and the categories and specialty areas of the NICE Framework, and we are finalizing the guidance that program managers and human capital support will use to select the appropriate code for each position/employee.

Initial Coding Pilot

- In coming weeks, DHS Components will report on their mission critical cybersecurity workforce with new information about the NICE code of each position/employee.

- CMSI will review the information at the Departmental level and will centrally code each position in the National Finance Center (NFC) system.

- After testing coding processes with this pilot population, DHS will determine a strategy for coding any additional employees outside of our current mission critical Workforce Inventory.

Addressing Position Descriptions

- Once the Department has determined the appropriate code for each position/employee and integrated that data into NFC, we will be releasing guidance to Components to ensure that related position descriptions (PDs) are updated.

- CMSI is also currently engaged in supporting several DHS Components as the work to fill highly-technical cybersecurity positions through the creation of revised PDs and human capital documents that contain enhanced cybersecurity language.

- As these positions are classified and new PDs are created, we are prospectively including the appropriate code and integrating the positions into our existing workforce tracking.

QUESTIONS ?