Competition for Cyber Talent Drives New Army and DHS Efforts

Posted At : May 6, 2015 1:41 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Department of Defense, Department of Homeland Security, Information Security, IT Workforce, Army, Training, Internet of Things, Cybersecurity

There is rarely a day that goes by when you won't see a top story on cybersecurity and the scarcity of people with the right IT security skills to address the growing challenges. It is this very demand for skilled cybersecurity staff that is driving some new, creative, and some might say bold efforts by the Army and the Department of Homeland Security (DHS) to raise up, recruit, and retain talent.

The Department of Defense (DoD) may be the one federal entity where building a cyber workforce is the most prominent, as they continue to grow a cadre of uniformed cyberwarriors to staff various cyber commands and other network defense organizations, like the **Joint Task Force-DoD Information Networks** (JTF-DoDIN). However, building the force is only part of the challenge. Once their tour of service commitment is fulfilled these skilled cyberwarriors often have the attractive option to land high-paying jobs in the private sector, so the sustainability of a cyber-force is a major DoD priority.

Recognizing these realities is a driving force behind the establishment of the **Army Reserve's Cyber Private Public Partnership**, or Cyber P3, among the DoD, universities and private employers. In recent comments in a **story by *Nextgov***, Cyber P3 program manager Lt. Col. Scott Nelson said that the program is trying to answer key questions of "how do we retain the investment the Army made in that soldier" and also "allow them to get a really good job with our industry partners?"

Maximizing the return on investment in cybersecurity personnel is not the only item on the Cyber P3 agenda. They also want to enhance the pipeline of skilled cyber personnel through building parallel cybersecurity education and training programs among military and universities. In that pursuit, several universities, companies and federal agencies are collaborating on the effort with the goal of establishing 3,500 to 5,000 Army reserve cyberwarriors that can be at the ready when the need arises. Among the 21 private companies that have already stepped up to help transition service members into civilian careers include Citibank, Microsoft, Fox Entertainment and Chevron, according to the *Nextgov* report. (Read more about Cyber-P3 **here** and **here**.)

The Pentagon is not the only federal agency looking to industry to bolster its long-term cybersecurity posture. The **Department of Homeland Security** Secretary **Jeh Johnson announced** at the RSA Conference in San Francisco that DHS is opening a cybersecurity branch office in Silicon Valley to "strengthen critical relationships… and ensure that the government and the private sector benefit from each other's research and development." Collaboration and synergy is not the only thing on Johnson's mind, however. He's recruiting. He intends to "convince some of the talented workforce in Silicon Valley to come to Washington," highlighting the new United States Digital Service program that provides mechanisms for tech talent in private industry to complete a "tour of service" within government agencies. But on a more formal level, Johnson is "on the hunt" for a cybersecurity "all-star" to head up DHS' National Cybersecurity and Communications Integration Center (NCCIC), promising a direct reporting and communications line to the department Secretary, i.e. Himself.

These efforts, and others, underscored the ongoing urgency and scope expansion of cybersecurity into nearly every area of modern life. As the "Internet of Things" (IoT) continues to march on – bringing digitization, sensor-ization and connectivity to everything from communications to home appliances and motor vehicles – securing this infrastructure from exploitation and destruction becomes even more critical. Further, the farther down the cybersecurity road we go, the more it becomes apparent that there is only so much we may be able to automate with tools – at least for now. This is especially true when it comes to decision-making and rapid response. Skilled people are critical, in high demand, and in short supply.

These efforts by the DoD, DHS, and others will take time to build the pipeline necessary to meet the demand. It will likely take years, not a cheerful prospect when one considers the growing threats we face. Meanwhile, the competition for these skills will remain fierce.