NSA Adds Five Schools to Centers of Academic Excellence Roster

Posted At : July 23, 2014 9:33 AM | Posted By : Kyra Fussell

Related Categories: Intelligence Community, Information Security, IT Workforce, Cybersecurity

The National Security Agency (NSA) Central Security Service (CSS) Center of Academic Excellence (CAE) programs support the President's **National Initiative for Cybersecurity Education (NICE)** in growing the base of skilled workers capable of supporting a cyber-secure nation. Mid July 2014, NSA recognized five schools as additions to the Cyber Operations Program.

The Cyber Operations program includes technologies and techniques pertinent to cyber operations as well as legal and ethical considerations. According to the NSA, "these technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform [cyber] specialized operations." The **July 14, 2014 announcement** added five schools to the ranks of qualified academic institutions:

- New York University (New York);
- Towson University (Maryland);
- The United States Military Academy (New York);
- The University of Cincinnati (Ohio); and
- The University of New Orleans (Louisiana).

The additions bring the total of schools in the Cyber Operations program up to thirteen. NSA's Centers for Academic Excellence include programs addressing Cyber Operations, Information Assurance Education, and Research. The Information Assurance Research and Information Assurance Education, jointly overseen by NSA and the Department of Homeland Security, boast over 100 existing centers of academic excellence.

While the Cyber Operations program is "designed to cultivate more U.S. cyber professionals," it's not clear whether these individuals are expected to bolster the nation's information security from within government ranks. While students may consider the CAE designation in evaluating schools, they might have their sights set on the private sector.Students participating in the Cyber Operations program will have opportunities to pursue summer internships at NSA, which suggests that there is hope to bring in new talent. Considering the workforce challenges agencies have faced in recent years, it's questionable whether that's where students will head. When it comes to information security personnel, federal agencies have struggled with recruitment, retention, training, and hiring system complications.

Although the most recent FISMA report did not include data on security personnel, the FY2012 FISMA Report indicated a continue reliance on skilled personnel. Workforce amounted to approximately 90% of FY2012 IT security costs. Within civilian agencies, around 42% of the FTEs with major responsibilities in information security were contracted roles. Defense agencies managed to fill 68% of those information security roles with government employees, but they still relied on contractors for nearly a third of the workforce with information security responsibilities. It's clear that agencies will need contractor support for the foreseeable future. At the same time, the current fiscal environment casts this cost structure in an unsustainable light. Perhaps, the more realistic expectation for these academic programs is simply to serve as incubators for cyber talent. In the long run, both industry and government (often through contracted support) stand to benefit, and continued government-industry collaboration will help improve our overall cybersecurity posture adapt to future threats.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@FIAGovWin**.*