Cyber security workforce becomes even more critical

By: Jacob Goodwin

Although intelligence agencies, homeland security and private industry groups have long searched for and recruited workers who understand cyber security techniques and technology, their efforts have accelerated in recent months, as some high-ranking officials warn of an impending “Cyber Pearl Harbor.”

The need for cyber security professionals with science and technology backgrounds has never been greater for public and commercial interests, according to intelligence and DHS officials. Secretary of Defense Leon Panetta warned in early October that the U.S. faces a Cyber Pearl Harbor if more electronic defenses aren’t put in place. To underscore his point, Panetta had information declassified about one of the largest private industry cyber attacks ever seen to illustrate what he considers to be a looming threat.

In mid-October, Panetta, speaking at a business conference in New York, detailed a malware attack on Saudi Arabian oil giant Aramco that destroyed 50,000 of the company’s computers. The sponsors of that attack remain shadowy, but some have blamed the Iranian government.

Panetta said he revealed details of the attack to show just how urgently cyber defenses and skilled workers are needed.

In October, federal agencies ramped up their efforts to recruit and retain experienced cyber professionals, as well as develop new talent. On October 26, for example, Department of Homeland Security Secretary Janet Napolitano said her agency had extended its scope of cyber education beyond the federal labor force to include students from kindergarten to post-graduate school through the National Initiative for Cybersecurity Education (NICE).

The NICE strategic plan, issued last September, said one of its primary goals was to "Increase exposure to cybersecurity in preK-12 education by emphasizing connections to science, technology, engineering, and mathematics (STEM) education and the role of mathematics and computational thinking in cybersecurity,” said Napolitano.

Napolitano said her agency had also launched a new recruitment initiative for exceptional recent college graduates called “The Secretary’s Honors Program,” aimed at recruiting, retaining and developing exceptionally talented entry-level people to support the department’s missions, including cyber.

The agency has also begun implementing recommendations from its Homeland Security Advisory Council task force on cyber skills, in conjunction with public-private partners, to develop a more agile cyber workforce across the federal government. The recommendations, Napolitano said, are aimed at improving the department’s ability to build a world-class cyber security team and allow it to tap into pools of talent, such as armed forces veterans, who already have operational experience suited to cyber security work.

As Napolitano announced DHS’s deeper cyber education initiative, officials at the Office of the Director of National Intelligence (ODNI) -- the principal advisor to the President, the National Security Council and the Homeland Security Council about intelligence matters related to national security -- said the agency could forego some of its missions to hold onto its cyber workforce in the face of shrinking federal budgets.

In remarks to the SINET cyber security conference in Washington, DC, on Oct. 25, Stephanie O'Sullivan, principal deputy director of national intelligence at ODNI, said maintaining her agency's highly-skilled, cyber-savvy workforce could be achieved at the expense of some of the agency's other operations, in the face of steep budget reductions.

"We're now thinking more strategically and realistically," said O'Sullivan, as budgets shrink, but security demands increase. "We can't pretend we can do everything. We must think differently. We will cut whole programs and stop doing some things," she added. However, one of those things, she said, *won't* be cutting the highly-skilled workforce the agency has amassed to analyze electronic data and intel. She said the agency made a mistake in the 1990's when it cut its workforce during the government's budget woes. "It takes time to train" skilled cyber workers, she noted. "If our adversaries catch up with us" on cyber, she observed, "our advantage will be lost for some time."

Cyber professionals are not just important to government, said other DHS and private industry officials. They're also important to private industry. However, while some companies have the resources to bolster and maintain considerable electronic defenses, smaller companies could be an Achilles heel. Appearing at the same conference as O'Sullivan, Mark Weatherford, deputy under secretary at DHS for cyber security, National Protection and Programs Directorate (NPPD), said cyber security professionals were also needed at small- and medium-sized private companies, which have been described as "the soft underbelly" of cyber security in the U.S.

Rich Baich, chief information security officer, enterprise technology services, at Wells Fargo Bank, who appeared with Weatherford, agreed. "That's the challenge," said Baich. "The DHS outreach programs have to work with small business" and other grassroots organizations, like community chambers of commerce, to develop cyber skills and STEM education, he said.