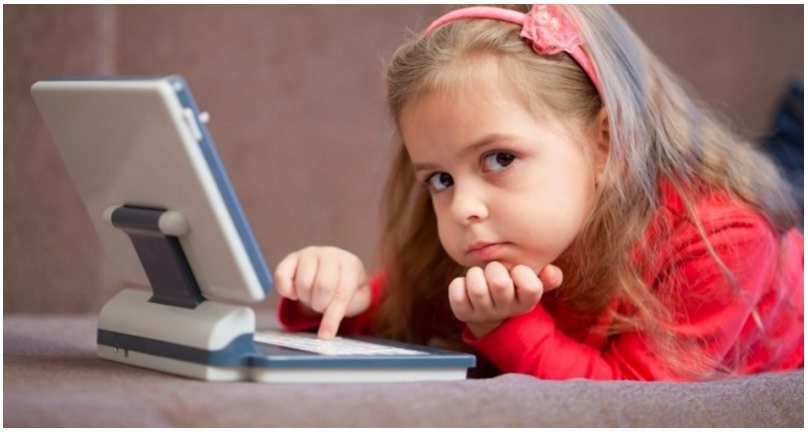
Written by **Brian Koenig** on October 30, 2012

DHS Proposes Cybersecurity Education to Begin in Kindergarten



In an effort to embolden the next generation of cyber professionals, the Department of Homeland Security (DHS) is devising an initiative to encourage and equip young Americans with knowledge and skills in the science of cybersecurity. Writing a blog entitled, "Inspiring the Next Generation of Cyber Professionals" DHS Secretary Janet Napolitano announced a plan to extend "the scope of cyber education" beyond the federal labor force through the National Initiative for Cybersecurity Education, targeting students from kindergarten all the way up to post-graduate school.

In detailing the plan, the DHS emphasizes the need to educate young Americans about technology — primarily for the use of cybersecurity — alongside the traditional subjects of science, engineering, mathematics, reading, and writing.

Napolitano spoke at the Women in International Security conference on Thursday, hosted by the Center for Strategic and International Studies, about what she branded as one of the "most urgent and important issues facing our nation — cybersecurity." She explained how her agency was formulating a cyber-workforce composed of skilled and highly-qualified workers to contrive innovative techniques to combat this plaguing issue. The DHS Secretary wrote of the agency's goals:

> At DHS, we're working to develop the next generation of leaders in cybersecurity while fostering an environment for talented staff to grow in this field. We are building strong cybersecurity career paths within the Department, and in partnership with other government agencies. We are also creating training and development opportunities to retain our most talented employees and ensure their professional development. In collaboration with the National Security Agency, we are strengthening the nation's educational infrastructure by supporting Centers of Academic Excellence across the country.

The DHS is also sponsoring the U.S. Cyber Challenge, Napolitano added, "a program that works with academia and the private sector to identify and develop the best and brightest cyber talent to meet our nation's growing and changing security needs." The National Initiative for Cybersecurity Education (NICE) notes that the National Science Foundation and the Department of Education are heading the Formal Cybersecurity Education Component.

"Their mission is to bolster formal cybersecurity education programs encompassing kindergarten through 12th grade, higher education and vocational programs, with a focus on the science, technology, engineering and math disciplines to provide a pipeline of skilled workers for the private sector and government," the NICE website explains. "A digitally literate workforce that uses technology in a secure manner is imperative to the Nation's economy and the security of our critical infrastructure."

Under a new recruitment initiative, the department is also calling on recent college graduates to embrace the federal government's cybersecurity vision, under "The Secretary's Honors Program." Napolitano's goal is to recruit entry-level workers to pursue the program, which would educate on cyber-related skills.

The Associate Press reports on how November's two presidential candidates stand on cybersecurity issues:

> President Barack Obama wants owners and operators of essential U.S. infrastructure to meet minimum cybersecurity standards that the private sector and federal agencies would develop together. He says federal agencies and businesses should exchange information about looming cyberthreats or malicious software that can damage computer networks.
>
> Republican presidential candidate Mitt Romney says within his first 100 days in office he would order all federal agencies to develop a national strategy to deter and defend the country from cyberattacks. Romney's Republican allies in Congress support the sharing of cyberthreat information but oppose giving Washington a say in how the private sector protects its networks.

While cyber-crimes could pose a devastating threat to American businesses, critics are questioning the freedom-related implications of government action, as regulations and government-private sector alliances could impede on civil liberties. One bill brought to the table late last year would establish a quasi-governmental entity, called the National Information Sharing Organization (NISO), which would be staged as a clearinghouse for exchanging relevant information regarding cyber threats and vulnerabilities.

The entity would consist of a DHS-appointed board of directors, comprised of members from five different federal agencies and 13 members of the private sector. In sum, NISO's goal would be to establish a point of connection between the government and U.S. businesses to pool information about potential cybersecurity threats and to collaborate on methods to hinder such threats from occurring.

Many civil liberties groups and freedom-minded lawmakers have expressed concern over such legislation, as these policies could lead to austere privacy rights violations. Gregory Nojeim, senior counsel at the Center for Democracy & Technology, a public interest organization working to maintain an open and free Internet, believes a completely privately-run organization would be an effective mode to combat cybersecurity threats, but that governmental involvement could lead to unfortunate civil consequences.

For example, under the purported legislation, if a business shares information on a user's web activities that it acquired to preclude the user's account from being hacked, the government would have the ability to use that information for its own purposes, including for criminal prosecutions independent of cybersecurity. While NISO would comprise mostly private-sector members, Nojeim added, companies could have limited say in promulgating rules, granting federal officials unprecedented influence over the entity's functions.

"Approaches to cybersecurity that would eliminate pseudonymous and anonymous speech online would put privacy at risk, chill free expression and erode the Internet's essential openness," Nojeim asserted in a May 2009 congressional testimony. "As the founders of our country recognized, anonymity and pseudonymity play essential roles in allowing political views to be aired."