Cyber shield for private sector sparks Big Brother fears

Is an NSA program to defend corporate critical infrastructure a step toward a surveillance state?

By **Amber Corrin** - **Jul 08, 2010**

The National Security Agency's new program to shield the networks of privately owned utilities and other critical infrastructure companies has caused some people to fear it's a step toward a surveillance state or a government power grab.

Named "Perfect Citizen," the plan is designed to detect cyber assaults that could potentially threaten critical infrastructure, which includes the electric grid, power companies, nuclear power plants, transportation, health care facilities and other necessities of modern life, according to a report in the **Wall Street Journal.** It would also deal with the networks of defense contractors and companies such as Google, which asked NSA for help after a major cyberattack last year.

The government would deploy sensors on the privately owned networks to identify unusual activity that could signal a potential intrusion or threat, but would not necessarily continuously monitor the networks.

According to the report, Raytheon has received a $100 million classified contract to start work on the program. No comment was available from either the NSA or Raytheon.

The program's revelation has triggered a wave of concerns and outcry over the surveillance aspect and the potential for invasion of privacy. Even in Raytheon there is disagreement over the program – an internal e-mail message leaked to the WSJ said, "The overall purpose of the [program] is our Government...feel[s] that they need to insure the Public Sector is doing all they can to secure Infrastructure critical to our National Security. Perfect Citizen is Big Brother."

"Big Brother" is the name for the dictator who oversees the oppressive -- and hyper surveillant -- government in George Orwell's dystopian novel "1984."

Jim Harper, writing for the **libertarian Cato Institute**, criticized the program's secrecy and potential expansion. "Benign intentions do not control future results, and government surveillance of the Internet for 'cybersecurity' may warp over time to surveillance for ideological and political purposes," he wrote.

However, government officials say such a program is critical for protecting national security. At a cybersecurity symposium held by AFCEA in Washington today, officials warned of the dire consequences of failing to protect the networks behind the country's most important utilities and communications systems.

"It's important for the public to understand there's a lot at risk. We need to think about [security] differently than in the past," said Army Brig. Gen. John Davis, director of current operations at the U.S. Cyber Command. CyberCom is tied to the NSA, including by the leadership of Gen. Keith Alexander, who heads both organizations.

"We need a regime where we can respond to incidents," Davis said.

Writing in **PC World**, Tony Bradley acknowledged the concerns while defending the program. "The name -- Perfect Citizen -- seems overtly Orwellian. The first thing that pops into my mind when reading about this program is the movie Eagle Eye, or HAL from Arthur C. Clarke's Space Odyssey saga. But, oppressive 'Newspeak' naming aside, the premise of the program seems both valuable and long overdue," he wrote.

However, Bradley added, "The concern is that Perfect Citizen could be just the beginning, or that the NSA will overstep its bounds and essentially monitor all domestic network activity. Access to critical infrastructure networks might also provide the NSA with access to details regarding the power usage, or travel plans of companies and individual citizens.

"It is a difficult balance to strike. ... Given the recent history of the NSA, it is easy to jump to insidious conspiracy theory conclusions. However, this is a long overdue step in safeguarding the critical infrastructure of the nation, and will hopefully be a first step in fostering more cooperation between public and private sector -- as well as between various private sector companies -- to collaborate on intelligence gathering and effective defense against cyberattacks."

Bruce Held, director of intelligence and counter-intelligence at the Energy Department, said being aggressive is vital for national cybersecurity. “With static cyber defense you can never win against an agile defense,” Held said.

In May, Deputy Defense Secretary William Lynn said the Defense Department is considering measures to protect the private networks with vulnerabilities that could threaten national security. He said a task force had been formed to determine an “enduring security framework” to examine the issues surrounding critical infrastructure network security.