

See a sample reprint in PDF format.

Order a reprint of this article now

THE WALL STREET JOURNAL.

WSJ.com

U.S. NEWS | JULY 8, 2010

U.S. Plans Cyber Shield for Utilities, Companies

262612: 12;g n n k i g



[View Full Image](#)

Bloomberg News

The control room at a nuclear-power plant in Limerick, Pa. The National Security Agency's 'Perfect Citizen' program will detect cyber assaults on critical infrastructure, but could also help companies in other fields, such as Google, which sustained a major attack late last year.

The federal government is launching an expansive program dubbed "Perfect Citizen" to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants, according to people familiar with the program.

Related Videos

[AM Report: U.S. Hit by Cyber Attacks](#)
02/18/10

[News Hub: A Citigroup Hack Attack](#)
12/22/09

[New Military Command to Combat Cyber Spies](#)
04/22/09

[U.S. Intelligence Detects Cyber Spies](#)
04/08/09

The surveillance by the National Security Agency, the government's chief eavesdropping agency, would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack, though it wouldn't persistently monitor the whole system, these people said.

Defense contractor [Raytheon Corp.](#) recently won a classified contract for the initial phase of the surveillance effort valued at up to \$100 million, said a person familiar with the project.

An NSA spokeswoman said the agency had no information to provide on the program. A Raytheon spokesman declined to comment.

Some industry and government officials familiar with the program see Perfect Citizen as an

intrusion by the NSA into domestic affairs, while others say it is an important program to combat an emerging security threat that only the NSA is equipped to provide.

"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," said one internal Raytheon email, the text of which was seen by The Wall Street Journal. "Perfect Citizen is Big Brother."

Journal Community

What do you think of the NSA's 'Perfect Citizen' plan to monitor cyber security?

- Great idea
- I have concerns
- Terrible idea

[SUBMIT VOTE](#) [View Results »](#)

Raytheon declined to comment on this email.

A U.S. military official called the program long overdue and said any intrusion into privacy is no greater than what the public already endures from traffic cameras. It's a logical extension of the work federal agencies have done in the past to protect physical attacks on critical infrastructure that could sabotage the government or key parts of the country, the official said.

U.S. intelligence officials have grown increasingly alarmed about what they believe to be Chinese and Russian surveillance of computer systems that control the electric grid and other U.S. infrastructure. Officials are unable to describe the full scope of the problem, however, because they have had limited ability to pull together all the private data.

More

[Espionage Is Back on Front Burner](#)

[U.S. Hampered in Fighting Cyber Attacks, Report Says](#)

[U.S. Backs Talks on Cyber Warfare](#)

[FBI Targets Cyber Mules](#)

[Read More on the National Security Agency](#)

Perfect Citizen will look at large, typically older computer control systems that were often designed without Internet connectivity or security in mind. Many of those systems—which run everything from subway systems to air-traffic control networks—have since been linked to the Internet, making them more efficient but also exposing them to cyber attack.

The goal is to close the "big, glaring holes" in the U.S.'s understanding of the nature of the cyber threat against its infrastructure, said one industry specialist familiar with the program. "We don't have a dedicated way to understand the problem."

The information gathered by Perfect Citizen could also have applications beyond the critical infrastructure sector, officials said, serving as a data bank that would also help companies and agencies who call upon NSA for help with investigations of cyber attacks, as Google did when it sustained a major attack late last year.

The U.S. government has for more than a decade claimed a national-security interest in privately owned critical infrastructure that, if attacked, could cause significant damage to the government or the economy. Initially, it established relationships with utility companies so it could, for instance, request that a power company seal a manhole that provides access to a key power line for a government agency.

With the growth in concern about cyber attacks, these relationships began to extend into the electronic arena, and the only U.S. agency equipped to manage electronic assessments of critical-infrastructure vulnerabilities is the NSA, government and industry officials said.

The NSA years ago began a small-scale effort to address this problem code-named April Strawberry, the military official said. The program researched vulnerabilities in computer networks running critical infrastructure and sought ways to close security holes.

That led to initial work on Perfect Citizen, which was a piecemeal effort to forge relationships with some companies, particularly energy companies, whose infrastructure is widely used across the country.

The classified program is now being expanded with funding from the multibillion-dollar Comprehensive National Cybersecurity Initiative, which started at the end of the Bush administration and has been continued by the Obama administration, officials said. With that infusion of money, the NSA is now seeking to map out intrusions into critical infrastructure across the country.

Because the program is still in the early stages, much remains to be worked out, such as which computer control systems will be monitored and how the data will be collected. NSA would likely start with the systems that have the most important security implications if attacked, such as electric, nuclear, and air-traffic-control systems, they said.

Journal Community

DISCUSS

Wow, the name "Perfect Citizen" just screams of Orwellian repression.

—Mike Lorrey

about what data they will then share with the government, industry and government officials said.

While the government can't force companies to work with it, it can provide incentives to urge them to cooperate, particularly if the government already buys services from that company, officials said.

Raytheon, which has built up a large cyber-security practice through acquisitions in recent years, is expected to subcontract out some of the work to smaller specialty companies, according to a person familiar with the project.

Write to Siobhan Gorman at siobhan.gorman@wsj.com

Intelligence officials have met with utilities' CEOs and those discussions convinced them of the gravity of the threat against U.S. infrastructure, an industry specialist said, but the CEOs concluded they needed better threat information and guidance on what to do in the event of a major cyber attack.

Some companies may agree to have the NSA put its own sensors on and others may ask for direction on what sensors to buy and come to an agreement

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com