

---

**THE WALL STREET JOURNAL**  
WSJ.com

---

JULY 6, 2009

## Troubles Plague Cyberspy Defense

By [SIOBHAN GORMAN](#)

WASHINGTON -- The flagship system designed to protect the U.S. government's computer networks from cyberspies is being stymied by technical limitations and privacy concerns, according to current and former national-security officials.

The latest complete version of the system, known as Einstein, won't be fully installed for 18 months, according to current and former officials, seven years after it was first rolled out. This system doesn't protect networks from attack. It only raises the alarm after one has happened.

A more capable version has sparked privacy alarms, which could delay its rollout. Since the National Security Agency acknowledged eavesdropping on phone and Internet traffic without warrants in 2005, security programs have been dogged by privacy concerns. In the case of Einstein, [AT&T Corp.](#), which would test the system, has sought written approval from the Justice Department before it would agree to participate, people familiar with the matter say.

An AT&T spokesman declined to comment.

The total cost of the system, designed to protect all nonmilitary government computers, is classified, but officials familiar with the program said the price tag was expected to exceed \$2 billion.

The Obama administration has made combating threats to the nation's computer networks a top priority. President Barack Obama recently called such attacks "one of the most serious economic and national security challenges" facing the country. Attacks on the government have been intensifying, and thousands of federal networks have been breached, including that of the Homeland Security Department, security officials say.

Homeland Security officials say they are pressing ahead with deliberate speed. Because the program is the first of its kind, "we're trying to get things as right as possible," a senior Homeland Security official said. It takes time to get all the other government agencies on board, the official added, but their buy-in will lead to a more effective system in the long run.

The Obama administration is now re-examining plans for a third iteration of Einstein to review its privacy protections and effectiveness, said Paul Kurtz, a cybersecurity specialist who led a review of the topic for President Obama's transition team.

"The good news is, I think [the administration] appears to be taking a close look at how best to do this," Mr. Kurtz said. "The bad news is, while they work to figure it out, the security of our networks is not necessarily getting any better."

Homeland Security spokeswoman Amy Kudwa described the various rollouts as "incremental improvements" designed also to protect privacy and civil liberties. "We don't want to let the perfect be the enemy of the good," she said.

Many of these problems predate the Obama administration. The administration supports the objectives of the "comprehensive national cybersecurity initiative," said a White House official. Government officials say military computer systems are equipped with much stronger technology to deflect cyber intruders.

The Homeland Security Department first developed Einstein in 2003, adapting technology from a Pentagon program that monitored military networks, according to former national-security officials. A voluntary program, it tracked Internet traffic flowing in and out of participating federal departments, such as the Transportation Department, and looked for abnormalities that might be cyberattacks.

By 2007, portions of just 16 agencies had subscribed, according to the Government Accountability Office, the nonpartisan investigative arm of Congress. Despite the small takeup, the system failed to produce warnings that were "consistently actionable and timely," the GAO said.

Armed with fresh funding from the Bush administration, officials started work on a new version, dubbed Einstein 2. It is supposed to detect known types of cyberattacks and immediately alert the cybersecurity center. The problem: Like its predecessor, it still can't detect or block sophisticated attacks that weren't previously known, said Stewart Baker, a former senior Homeland Security Department official. Homeland Security is the only department using it so far.

Other departments and agencies plan to use Einstein 2 technology run by Homeland Security but based inside the networks of the nation's telecommunications companies.

The government was concerned about how the public would react to its working with the phone company to monitor networks, and the move had to be cleared by a larger number of officials, Mr. Baker said. "It was purely a perception issue," he said. The NSA's warrantless wiretapping was done in coordination with phone companies.

It will take 18 months to launch Einstein 2 across most of the government, a senior Homeland Security official said, and then 96 smaller agencies will follow. Plans are already under way for Einstein 3. As envisioned by the Bush administration, Einstein 3 would draw from an NSA program that automatically identifies and deflects security breaches, according to former officials familiar with the program.

This version has raised bigger privacy issues because the technology has the ability to read the content of emails and other messages sent over government systems as it scans for attacks. Mr. Obama's transition team flagged Einstein 3 as a potential privacy concern, according to a person familiar with the discussions.

When officials told members of the Senate Intelligence Committee about plans to use "active sensors," lawmakers balked because that sounded too much like spying, a senior intelligence official said, adding that the perception was incorrect.

Homeland Security asked AT&T to test some of the technology that might be used for Einstein 3, a person familiar with the discussion said. The company demanded clearance from the Bush administration's Justice Department, this person said. But the pilot was delayed for a variety of technical and practical reasons and spilled over into the Obama administration, said a senior Homeland Security official. The Obama administration has approved the test, the official said.

James Lewis, who directed a cybersecurity study at the Center for Strategic and International Studies, said cyber threats could be handled if the U.S. was able to monitor major Internet gateways into the country, scanning private traffic for security purposes only. Such a move would require changes to spying laws to permit scanning of routine traffic without an individual warrant. Some committees on Capitol Hill are considering that approach, but Congress may not have the appetite to reopen the topic after wrangling over spying rules for much of 2008.

One alternative approach for Einstein 3 under consideration is to have telecommunications companies scan and block potential cyberattacks, said one former official familiar with the discussion. That might be combined with some of the scanning technology developed in the private sector and at the NSA.

Carriers like AT&T already provide such services for many major companies. The Bush administration didn't pursue that route because of the potential political problems related to working closely with phone companies, government officials said.

**Write to Siobhan Gorman at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com)**

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](http://www.djreprints.com)