Health website's security prompts worries

RICARDO ALONSO-ZALDIVAR, Associated Press

WASHINGTON (AP) — Obama administration officials are facing mounting questions about whether they cut corners on security testing while rushing to meet a self-imposed deadline to launch online health insurance markets.

Documents show that the part of HealthCare.gov that consumers interact with directly received only a temporary six-month security certification because it had not been fully tested before Oct. 1, when the website went live. It's also the part of the system that stores personal information.

The administration insists the trouble-prone website is secure, but technicians had to scramble to make a software fix earlier this week after learning that a North Carolina man tried to log on and got a South Carolina man's personal information. A serious security breach would be an unwelcome game-changer for an administration striving to turn the corner on technical problems that have inconvenienced millions of consumers and embarrassed the White House.

Two computer security experts interviewed by The Associated Press said that clearly the better option would have been to complete testing.

"The best scenario is to have done end-to-end testing," said Lisa Gallagher, vice president of technology solutions for the Healthcare Information and Management Systems Society, a medical technology nonprofit. That it wasn't done "would cause me some mild concern," she continued, adding she would advise a relative or close

friend to wait until the website is stabilized before plunging in.

Asked former White House chief information officer Theresa Payton, "If you haven't done end-to-end testing, how can we say with certainty how hard or easy it is for cybercriminals to attack at different points in the process?"

"It makes me shudder a little," said Payton, a former bank security executive who now has her own company.

Payton served in the George W. Bush administration and has been consulted by congressional Republicans but says she has no partisan agenda on the health care law. "We need to help because we have to make this right," she said.

The website was supposed to provide easy access to a menu of government-subsidized coverage options under President Barack Obama's health care law. Administration officials say they remain confident it is secure.

"When consumers fill out the online application, they can trust that the information they've provided is protected by stringent security standards and that the technology underlying the application process has been tested and is secure," Medicare administrator Marilyn Tavenner assured the Senate's Health Committee on Tuesday.

But a short while later, Tavenner acknowledged the Carolinas security breach. "We actually were made aware of that" Monday, she said in response to a question from Sen. Johnny Isakson, R-Ga. "We implemented a software fix."

It was not immediately clear how the North Carolina man was able to view the personal information of the man in South Carolina. However, a vulnerability that has afflicted websites for years is known as "horizontal privilege escalation," in which a legitimate user of a website slightly alters the string of random-looking characters in the website's address or inside downloaded data files known as "cookies," causing the system to display information about the accounts of other users. It can be protected against by a well-designed website.

Tavenner, a respected former hospital executive, has emerged as a key cybersecurity decision-maker for the health care law. Her agency, the Centers for Medicare and Medicaid Services, is charged with carrying out the Affordable Care Act.

According to federal law and policy, all government computer systems must have a security certification before going live.

Tavenner approved the Sept. 27 security certification for the health website, which read: "Aspects of the system that were not tested due to the ongoing development exposed a level of uncertainty that can be deemed as a high risk."

It called for a four-step mitigation plan, including ongoing monitoring and testing, leading to a full security control assessment.

The agency's top three information security professionals signed on an accompanying page that said that "the mitigation plan does not reduce the risk to the ... system itself going into operation on Oct. 1" but that its added protections would reduce risk later and ensure full testing within six months.

HealthCare.gov has two major components: an electronic "back room" that did get full security certification and the consumer-facing "front room" that's temporarily certified.

The back room, known as the federal data hub, pings government agencies to verify applicants' personal information. It does not store data.

But the front room does. That's where consumers in the 36 states served by the federal website create and save their accounts. While the individual components of the front room did undergo security testing, the system as a whole could not be tested because it was being worked on until late in the game.

Tavenner testified that was the reason she had to issue a temporary certification. The decision was brought to her level because of the overall magnitude of the project, she said. She said she didn't voice the security concerns to her boss, Health and Human Services Secretary Kathleen Sebelius, or to the White House office that oversees federal agencies.

Rep. Darrell Issa, R-Calif., chairman of the House Oversight and Government Reform Committee, is investigating whether that decision compromised security. "Did the administration officials who signed off ... know the full risks associated with the website, and if so, why did they decide to go ahead with the launch anyway?" said spokeswoman Caitlin Carroll.

Some of the strongest supporters of the health care law have expressed unease over security. "This is a paramount concern," said Iowa Democratic Sen. Tom Harkin, chairman of the Senate Health, Education, Labor and Pensions Committee. "Consumers have to be absolutely certain that when they go on and they fill out that application ... no one can hack into that and steal their Social Security numbers or identity," Harkin added, as Tavenner testified before his panel.

Thomas Dougall, a lawyer from Columbia, S.C., says he doesn't trust the system anymore.

Dougall told the AP he buys his own insurance and went on HealthCare.gov last month out of curiosity to see if he could save money. Ultimately, he realized his current plan is cheaper.

He thought nothing more of it until he got home last Friday and played a message from North Carolina resident Justin Hadley, who said he received Dougall's personal information after trying to log on with his own username. Dougall first thought Hadley was a scammer, but then Hadley emailed him screen shots.

Hadley said that once he got past the login screen last Thursday he received links to documents meant for Dougall, with his information. "I was shocked," said Hadley, of Burlington, N.C. "After the initial shock wore off, I knew I needed to contact (Dougall) so he knew what was going on."

Administration spokeswoman Julie Bataille said that as of Tuesday it's the only report the government has gotten of that particular problem. "We put a fix in place to prevent it from happening in the future," she said.