Judicial Watch: Documents Expose Fatal Flaws From the Onset of Obamacare

Tuesday, the government watchdog group Judicial Watch released 944 pages of Department of Health & Human Services records it obtained through court order as part of a Freedom of Information Act lawsuit.

These records document security problems associated with the Affordable Care Act's sign-up website, and that the site was launched despite very serious concerns by its security testing contractor, Mitre Corporation. They also document internal executive-level apprehension about Internet security.

The organization's press release states:

> A July 2013 "Continuous Improvement Plan," prepared for updates and improvements to the website, defines the "Change Control Board" as a provider of final approval on new features and "politically sensitive issues."
>
> The documents reveal that Mitre recommended a "Denial Authorization to Operate" in the month prior to Obamacare's launch, noting that it could not adequately test the confidentiality and integrity of the system. It said that complete end-to-end testing of the system never occurred. Miter found that 11 "moderate" security findings and eight "low" findings remained open as September 19, 2013—12 days before the launch.
>
> And an unsigned "Authorization to Operate" prepared just five days before Obamacare's launch, indicates that the site's "validation contractor" was "unable to adequately test the confidentiality and integrity of the [Federally Facilitated Marketplace] system in full." That contractor,

Blue Canopy, noted that they were able to access data “that should not be publically [sic] accessible.”

On October 1, Americans started shopping for health insurance on , and the site crashed.

In an October 2013 email exchange requesting help with an upcoming test, IT security Chief Tom Schankweiler complained of a lack of a “grand strategy” in security testing the Obamacare website. Schankweiler complained about hackers hitting the site, and noted that confidential information was “growing legs and growing way beyond the normal borders.” Teresa Fryer, chief information security officer at CMS, agreed with Schankweiler, and also noted “conflict of interest issues” in the security testing.

In November senior CMS official Jon Booth discusses “a contingency system” for higher Obamacare enrollments that CMS Office of Administration wanted “kept under the radar” and “out of the spotlight, even from an internal perspective.” George Linares responds to Booth, noting that was still operating without an “Authorization to Operate,” and that the “contingency system” meant they needed a plan to “close the security gap as well.”

Among the released documents is a November draft press background briefer, in which CMS officials crossed out a line that read that consumers could “trust that the information that they are providing is protected by stringent security standards” and a line that the ACA website was “compliant with the Federal Information Security Management Act.”

> CMS Statement:
>
> The privacy and security of consumers’ personal information are a top priority for us. When consumers fill out their online Marketplace applications, they can trust that the information that they are providing is

protected by stringent security standards. Security testing happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. The website has been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institutes of Standards and Technology (NIST)."

In November, Schankweiler notes that they were faced with a choice of exposing users' personal identifiable information or having the website down for days, resulting in "a new round of political attacks," He also warns of a software problem causing a "high number of security and privacy incidents." Schankweiler's push to fix the problem was resisted by CMS official Rebecca Fender, who worried that the fix would take the Obamacare website down "for several days."

In early December, Schankweiler complains of a software problem that was causing "a high number of security and privacy incidents." Later in December Schankweiler complains about a security flaw that "allows anyone to access and edit records in the health care system."

In December 2013, Colin McVeigh from the CMS Center for Consumer Information and Insurance Oversight emailed to his colleagues his concerns that: "More than a month ago, we received reports that consumers were seeing other consumer's [sic] notices through a link on the application."

A December 2013 email exchange, two months after the site's launch, shows CMS official Lisa Feuerberg questioning Schankweiler as to why security testing wasn't done of the site, and another security official responded that his "one tester" couldn't get all the ACA sites scanned in time.

In a statement that accompanied the press release, Judicial

Watch President Tom Fitton reminded the public that this latest release merely compounds the troubles its FOIA activities have uncovered relative to Obamacare:

- In September 2014, Judicial Watch released 94 pages of documents obtained from the U.S. Department of Health and Human Services (HHS) including Security Controls Assessment Test Plans sent by CMS to Mitre Corporation. CMS advised Mitre that the highest "risk rating" should be given to flaws that could cause "political" damage to CMS. Moderate and low "risk ratings" were to include those resulting in potential "public embarrassment" to the agency.
- In March 2015, Judicial Watch released documents from the U.S. Department of Health and Human Services (HHS) revealing that Department of Homeland Security (DHS) worked with HHS on security for .
- In January 2016, Judicial Watch released documents showing federal health care officials' concerns with the Obamacare website in two productions of records: a 143-page production and an 886-page production. The emails showed that CMS Security Officer Teresa Fryer's refused to approve the "ATO" (Authorization to Operate).

"Obamacare is corrupt, as we see further proof in these FOIA documents that sensitive health information on millions of Americans was put at risk," Fitton said. "From its start, Obamacare was a project that its promoters were determined to inflict on us whether it was ready or not. And clearly it was not. Anyone who uses the Obamacare web site does so at great risk to their private information. Let this be a lesson for those in Washington who are now trying to clean up this mess." {eoa}