

Business

KeyPoint network breach could affect thousands of federal workers

By **Christian Davenport**
December 18, 2014

KeyPoint Government Solutions, which took over the bulk of federal background checks after one of its competitors was hacked, also recently suffered a computer network breach, officials said Thursday.

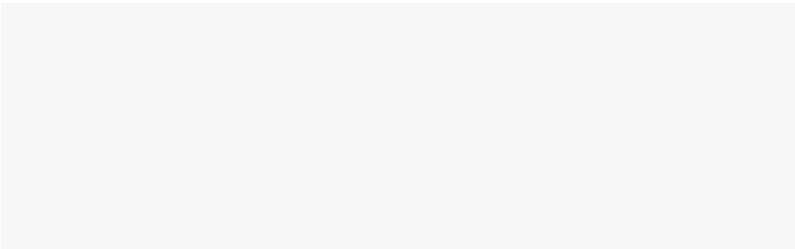
While there was “no conclusive evidence to confirm sensitive information was removed from the system,” Office of Personnel Management spokeswoman Nathaly Arriola said the agency would notify 48,439 federal workers that their personal information may have been exposed.

The breach comes just a few months after [OPM decided not to renew](#) a background investigations contract with USIS, which suffered a breach earlier this year.

USIS had been the largest provider of background checks used in security clearances for the federal government for years. After OPM decided not to renew USIS’s contract, Colorado-based KeyPoint quickly picked up the bulk of the work for the federal government.

KeyPoint and USIS declined to comment.

Earlier this month, USIS [pushed back against criticism](#) that it didn’t do enough to prevent a massive cyberattack and accused the OPM of neglecting to share information that might have helped it detect the intrusion earlier.

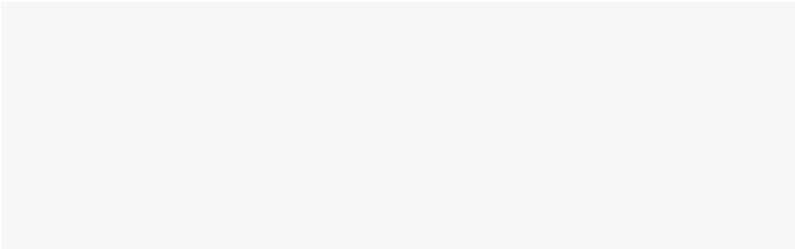


USIS, based in Falls Church, Va., said it sought to work closely with OPM after the breach. But the company wrote that “no meaningful partnership will ever exist if the U.S. government response to cooperation is to punish and shut down organizations that, like so many government agencies, happen to fall victim to a cyber attack.”

KeyPoint’s breach was yet another in a series of problems that have plagued the background-check process. Before it was hacked, USIS was accused in a whistleblower lawsuit, joined by the Justice Department, of “flushing” hundreds of thousands of checks — meaning they were submitted as complete even though they were not.

And members of Congress repeatedly urged OPM to end its contract with USIS.

The termination of the contracts on Sept. 30 had a devastating effect on USIS, which at one point employed about 3,000 workers in its investigations division.



KeyPoint moved quickly to fill the void, looking to double the size of its investigative workforce.

But USIS’s [caseload was significant](#) — 21,000 background checks a month, and once its contract was not renewed, some wondered who would be able to handle the task on short notice.

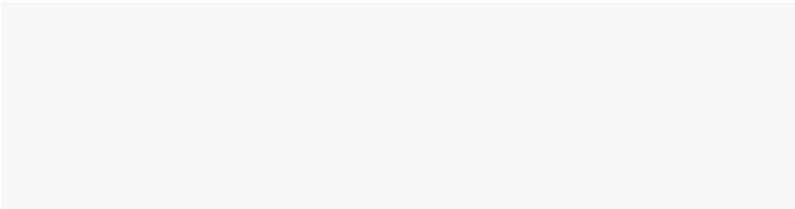
That amount of work requires significant managerial oversight, which is usually developed over time, said Nicole Smith, a former USIS senior investigator who now is an attorney at Tully Rinckey working on security clearance issues.

Once KeyPoint took over, she said one of the questions that concerned her was: “Can they even handle the influx of these new employees and all the work that gets dumped on them from OPM?”

In an e-mail to OPM colleagues, Donna Seymour, the agency’s chief information officer, said that “following the discovery of the problem, KeyPoint implemented numerous controls to strengthen the security of its network. The immediacy with which KeyPoint was able to remediate vulnerabilities has allowed us to continue to conduct business with the company without interruption.”

In the e-mail, a copy of which was obtained by The Washington Post, she said that the “security of our network and the data entrusted to us remains our top priority. This incident serves as yet another reminder that we all must be ever-vigilant in our efforts to understand, anticipate and guard against the threat of cyber-attacks.”

Arriola, the OPM spokeswoman, declined to comment on the sophistication of the attack or who might have been behind it, saying the investigation was ongoing. OPM will offer the employees free credit monitoring.



8 Comments



Economy & business email alerts

Important breaking news emails on the issues around the economy and business.

E-mail address

Sign up

By signing up you agree to our [Terms of Use](#) and [Privacy Policy](#)



Christian Davenport Christian Davenport covers the defense and space industries for The Washington Post's Financial desk. He joined The Post in 2000 and has served as an editor on the Metro desk and as a reporter covering military affairs. He is the author of "The Space Barons: Elon Musk, Jeff Bezos and the Quest to Colonize the Cosmos" (PublicAffairs, 2018). [Follow](#)

The Washington Post

Get a year of access for \$29. Cancel at any time.

Get this offer now

Send me this offer

Already a subscriber? [Sign in](#)

Most Read Business

- 1

Senate Republicans release massive economic stimulus bill for coronavirus response
- 2

Americans are very likely to get \$1,000 (or more) checks. Here's what you need to know.
- 3

Negotiations intensify on Capitol Hill over massive stimulus legislation as coronavirus fallout worsens
- 4

Paid sick leave: Who gets it during the coronavirus outbreak
- 5

Change in U.S. law will make millions more masks available to doctors and nurses, White House says

PostREPORTS

Latest episode

Republicans’ radical about-face on bailouts

► Listen 24:34

Unparalleled reporting. Expert insight. Clear analysis. Everything you’ve come to expect from the newsroom of The Post – for your ears.

The Washington Post

Get a year of access for \$29. Cancel at any time.

Get this offer now

Send me this offer

Already a subscriber? [Sign in](#)

Economy & business email alerts

Important breaking news emails on the issues around the economy and business.

E-mail address

Add

Market Watch

Dow 20,087.19	Today ↗ 0.95%
S&P 2,409.39	Today ↗ 0.47%
NASDAQ 7,150.58	Today ↗ 2.3%

Last Updated:03/19/2020

washingtonpost.com

© 1996-2020 The Washington Post

Help

Policies and Standards

Terms of Service

Privacy Policy

Print Products Terms of Sale

Digital Products Terms of Sale

Submissions and Discussion Policy

RSS Terms of Service

Ad Choices

Contact Us