8-Federal Times-Contractor breach

By Aaron Boyd

Jun 23, 2015

A breach of KeyPoint Government Solutions — a contractor used by federal agencies to conduct background checks — gave hackers the credentials needed to access sensitive employee data held by the Office of Personnel Management, the agency director confirmed Tuesday.

During a hearing in front of the Senate Appropriations Subcommittee on Financial Services and General Government, OPM Director Katherine Archuleta told legislators there was a direct line between the August breach of KeyPoint systems and the two intrusions of OPM servers detected in April.

More: Could OPM have prevented the breach?

[Disappointment]

“While the adversary leveraged a compromised KeyPoint user credential to gain access to OPM’s network, we don’t have any evidence that would suggest KeyPoint as a company was responsible or directly involved in the intrusion,” Archuleta said.

Having valid credentials allowed the intruders access to the system, as well as any encrypted files and other data that might have otherwise been restricted. The hackers successfully exfiltrated data on some 4.2 million current and former employees in an initial breach and highly sensitive background investigations on a still untold number of feds in a second intrusion.

More: OPM breach a failure on encryption, detection

[Disappointment]

The two contractor breaches were also significant in their own right. The Department of Homeland Security announced last August that unauthorized users gained access to records held by USIS, which DHS also contracted with, exposing data on some 27,000 DHS employees.

That month, hackers also breached KeyPoint's systems, the second largest contractor for DHS and OPM, affecting more than 48,000 employees. DHS and KeyPoint announced the breach publicly in December 2014.

More: Data on 48,000 feds exposed in contractor breach

Data from USASpending.gov show a sharp decline in contracting dollars going to USIS (and parent company Altegrity) in 2015, after OPM decided to not renew its contract. KeyPoint and CACI International picked up the majority of those contracts and are now the two largest background investigators for the federal government.

(Government data also shows a dip in contract awards to USIS in 2013, due to adjustments made from excess funds awarded in prior years.)

More: DHS, OPM suspend contracts with USIS after major cyberattack

"Since last year, we have been working with KeyPoint and they have taken strides in securing its network and have been proactive in meeting the additional security controls that we have asked them to use," Archuleta told the subcommittee.

[Rebuild]

Lawmakers brought up the possibility that compromised contractor credentials were used to access OPM's systems during the first congressional hearing on the OPM breach, held by the House Committee on Oversight and Governmental Reform on June 16.

More: OPM laxity to blame for data breach, lawmakers say

[Disappointment]

“Did these cyberattackers gain access to OPM’s data systems using information they stole from USIS or KeyPoint last year? Did they get the keys to OPM’s networks from one of its contractors?” Rep. Elijah Cummings, D-Md., asked.

Officials declined to answer the question directly *[Deny]* during that first hearing, offering to brief committee members later that day during a confidential session.

Cummings said he asked for representatives from KeyPoint and USIS to attend the House hearing, however both declined.

Third party background investigators have seen drastic shifts in the amount of contract spending coming from OPM.

Photo Credit: John Harman/Staff

About Aaron Boyd

Aaron Boyd is an awarding-winning journalist currently serving as editor of Federal Times — a Washington, D.C. institution covering federal workforce and contracting for more than 50 years — and Fifth Domain — a news and information hub focused on cybersecurity and cyberwar from a civilian, military and international perspective.

Share: