

Files of more than 40,000 federal workers breached (Update)

December 18 2014, by Stephen Braun

The computer files of more than 40,000 federal workers may have been compromised by a cyberattack at federal contractor KeyPoint Government Solutions, the second breach this year at a major firm handling national security background investigations of workers at federal agencies, the government confirmed Thursday.

Concerned that some data might have been exposed, the Office of Personnel Management has begun notifying workers that their files were in jeopardy. Nathalie Arriola, speaking for the personnel office, said it will offer credit monitoring at no cost to those affected by the breach.

KeyPoint became the largest private clearance firm working for federal agencies several months ago after rival contractor USIS lost its investigations business with the government following a devastating cyberattack reported earlier this year. The USIS breach, similar to previous hacking episodes traced to China, tainted the files of at least 25,000 Department of Homeland Security workers and prompted the personnel office's decision to halt all of USIS' government field work. That move led to the cancelation of more than \$300 million in contracts with USIS.

Cyberattacks have targeted several other federal agencies this year. A wide-ranging strike reported in November compromised the data of more than 800,000 Postal Service workers. The personnel office itself was targeted earlier by cyberhackers traced to China.

Arriola said Thursday that officials recently concluded an investigation into the KeyPoint breach and found "no conclusive evidence to confirm sensitive information was removed from the system." She said her agency is continuing to work with KeyPoint despite the severity of the strike. "KeyPoint has worked closely with OPM to implement additional security controls," she said.

In an earlier email within the agency, Donna Seymour, the chief information officer, said KeyPoint had added "numerous controls to continue to conduct business with the company without interruption." She also said that 50 OPM workers had been affected by the breach but neither she nor Arriola would identify the other federal agencies with workers whose files were possibly affected.

In the USIS breach, that firm and the OPM differed over how extensively USIS needed to upgrade its computer network and security safeguards. Federal officials said last month that assessments of the USIS computer network by government computer experts raised concerns that the system and its managers were not primed to detect the breach quickly once hackers got inside. The disagreement was still unresolved when OPM suspended the work of all USIS field investigations in August.

Neither Arriola nor Seymour said when the latest strike occurred or was reported to federal authorities, or whether a foreign state was suspected.

Colorado-based KeyPoint declined comment through its representatives, Fleishman Hilliard, Inc., a public relations firm.

© 2014 The Associated Press. All rights reserved.

Citation: Files of more than 40,000 federal workers breached (Update) (2014, December 18) retrieved 28 January 2023 from <https://phys.org/news/2014-12-clearance-contractor-hacked.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.