ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

January 6, 2015

Eric Hess
Chief Executive Officer
KeyPoint Government Solutions, Inc.
1750 Foxtrail Drive
Loveland, CO 80538

Dear Mr. Hess:

I am writing to request information about a significant data breach that was recently reported at KeyPoint Government Solutions, Inc., one of the largest providers of background investigation services for the federal government. According to news reports, "[t]he computer files of more than 40,000 federal workers may have been compromised by a cyberattack at ... KeyPoint."[1] The personal information of approximately 48,439 federal workers appears to have been compromised in this attack.[2]

This data breach is particularly disconcerting given that it appears to be related to a similar data breach at another private company, USIS, that was also responsible for performing critical background check services for the federal government.[3] That breach reportedly compromised the personally identifiable information of at least 25,000 federal employees who were in the process of obtaining, or who had recently obtained, security clearances in order to conduct classified work for federal government agencies.[4]

---

[1] *See, e.g., Files of More Than 40,000 Federal Workers Breached*, ABC News (Dec. 18, 2014) (online at www.abcnews.go.com/Politics/wireStory/2nd-security-clearance-investigation-contractor-hacked-27698370).

[2] *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, Washington Post (Dec. 18, 2014) (online at www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.htmlwtw).

[3] *DHS Contractor Suffers Major Computer Breach, Officials Say,* Washington Post (Aug. 6, 2014) (online at www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html).

[4] *U.S. Undercover Investigators Among Those Exposed in Data Breach*, Reuters (Aug. 22, 2014) (online at www.reuters.com/article/2014/08/22/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822).

As a leading provider of background check services for the federal government, it is imperative that KeyPoint's systems have sufficient controls in place to properly safeguard the highly sensitive data it collects on federal employees through the course of its work. The increasing number and apparent sophistication of cyber attacks against companies tasked with conducting background checks for the U.S. government poses a clear and present danger to our nation's security.

For these reasons, I request that KeyPoint provide the following information:

(1) all data security requirements that apply to the company pursuant to federal contracts in effect at the time of the data breach at issue;

(2) a log of all successful cyber intrusions into the company's networks in the last four years, including: a description of all data breaches the company has experienced within that time frame; the date, manner, and method by which the company first discovered the breaches; the dates the breaches are believed to have begun and ended; and the types of data breached;

(3) the findings from forensic investigative analyses or reports concerning the data breach at issue, including findings about vulnerabilities to malware, the use of data segmentation to protect personally identifiable information (PII), and why the breach went undetected for the length of time it did;

(4) the individuals or entities suspected or believed to have caused the data breach at issue, and whether they have been reported to the appropriate law enforcement agencies;

(5) documents relating to any weaknesses or vulnerabilities in the company's data security identified by the United States Computer Emergency Readiness Team;

(6) a list of all federal customers that may have been compromised in the data breach at issue;

(7) the approximate number of federal employees that may have been affected by the data breach at issue, and the manner in which those employees were notified of the breach;

(8) an estimate of the total possible number of PII records that may have been compromised in the data breach at issue;

(9) the date range of records that may have been compromised in the data breach at issue, including when the records were created and last updated prior to the breach;

(10) an explanation of why the company retained PII of federal workers;

(11) an explanation of whether system log capabilities were sufficient to determine whether or not PII was removed or altered by the hackers;

(12) a description of data protection improvement measures the company has undertaken since discovering the breach at issue; and

(13) a description of the data security policies and procedures that govern the company's relationships with vendors, third-party service providers, and subcontractors, including the manner by which the company ensures that entities performing work on its behalf have reasonable data security controls in place to thwart cyber-attacks.

Please provide the requested information by January 30, 2015. I also request a briefing from your Chief Information Security Officer or similar IT security professional by January 26, 2015. If you have any questions about this request, please contact Lena Chang or Timothy D. Lynch at (202) 225-5051. Thank you for your cooperation in this matter.

Sincerely,

Elijah E. Cummings
Ranking Member

cc: The Honorable Jason Chaffetz, Chairman