Eric Hess, CEO, KeyPoint Government Solutions
"OPM Data Breach: Part II"
House Committee on Oversight and Government Reform
June 24, 2015

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, my name is Eric Hess, and I am President and Chief Executive Officer of KeyPoint Government Solutions ("KeyPoint").

Since 2004, KeyPoint has provided fieldwork services for background investigations to a number of federal agencies, including the Office of Personnel Management ("OPM"). KeyPoint, which employs investigators in every state, is proud to be part of OPM's team, helping to ensure that the security clearance investigations it conducts are thorough, detailed, and consistent. KeyPoint takes issues of cybersecurity very seriously and, as a contractor providing critical services across the federal government, we stand in partnership with the federal government in trying to combat ever-present and ever-changing cyber-threats. KeyPoint is committed to ensuring the highest levels of protection for the sensitive information with which we are entrusted.

The recently-announced data breach at OPM is the focus of this hearing. With that in mind, I would like to make clear that we have seen no evidence suggesting KeyPoint was in any way responsible for the OPM breach. There have been some recent media reports suggesting that the incursion into KeyPoint's system last year is what facilitated the recently-announced OPM breach. There is absolutely no evidence that KeyPoint was responsible for that breach. The press also has reported that hackers stole OPM credentials assigned to a KeyPoint employee and leveraged them to access OPM's systems. As Director Archuleta noted at a Senate hearing yesterday, there is no evidence suggesting that KeyPoint was responsible for or directly involved in the incursion. To be clear, the employee was working on OPM's systems, not KeyPoint's.

Now, I know that during this hearing, the incursion into the KeyPoint system that was discovered last September will also be discussed. Before going into more detail, I would note that KeyPoint has continuously maintained its Authority to Operate (known as an ATO) from OPM and from DHS (under our TSA contract and more recently our CBP contract). This means we met the stringent information security requirements imposed under our federal contracts. KeyPoint only maintains personal information that is required under our contractual obligations. However, we, like the government, face aggressive, well-funded and ever-evolving threats that require us to exceed current FISMA requirements in order to protect the sensitive information in our charge.

So let me say a few words about the earlier incursion of the KeyPoint system. In December 2014, *The Washington Post* reported that OPM had announced it would notify over 48,000 federal workers that their personal information "*may* have been exposed" as the result of an incursion into KeyPoint's systems.[1] I emphasize the word "may" in the report because, after an

[1] Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, THE WASHINGTON POST, Dec. 18, 2014, http://www.washingtonpost.com/business/economy/keypoint-suffers-

(Cont'd on next page)

extensive analysis of this incursion, we found no evidence of the exfiltration of sensitive personal data.

Last August, following public reports of a data security breach at another federal contractor providing background checks, OPM Chief Information Officer Donna Seymour asked KeyPoint to invite the United States Computer Emergency Readiness Team, or US-CERT, to test KeyPoint's network, and KeyPoint agreed. A team from the Department of Homeland Security National Cybersecurity Assessment and Technical Services ("NCATS") conducted a Risk and Vulnerability Assessment ("RVA"). The NCATS team conducted a full network and application vulnerability test of KeyPoint's systems, including network mapping and internal and external penetration testing. The NCATS team provided a number of findings at the end of its engagement, which were resolved while the team was onsite, as well as recommendations for the future. Ultimately, while the NCATS team found issues, they have been resolved and the team found no malware on KeyPoint's network.

Then in September, the US-CERT Hunt team informed KeyPoint that it had found indications of sophisticated malware undetectable by commercial antivirus on two computers. The US-CERT team provided KeyPoint with a mitigation recommendation to remove the malware from the environment and other recommendations on hardening its network to prevent and detect future compromises. KeyPoint acted quickly and immediately began implementing the recommendations.

KeyPoint conducted an internal investigation of the data security issues identified by US-CERT and concluded that the malware in question was not functioning correctly, potentially caused by errors made when it was installed on KeyPoint's systems. Again, neither US-CERT's investigation, nor our investigation found evidence of the exfiltration of sensitive personal information.

I recently attended a classified briefing at OPM, where I learned more about the OPM breach. In this open setting, I cannot go into the details that were presented in that briefing, however, I can reiterate that we have seen no evidence of a connection between the incursion at KeyPoint and the OPM breach that is the subject of this hearing.

That said, we are always striving to ensure that KeyPoint's cyber-defenses are as strong as possible, and we welcomed US-CERT's recommendations for strengthening the security of our system. We have also been working closely with our customers OPM and CBP to improve our information security posture in light of new advanced persistent threats. OPM presented us with a 90-day network hardening plan. We completed it. We have been working diligently to make our systems more resilient and stronger by implementing the US-CERT recommendations. A number of the most significant improvements we put into place are as follows:

(Cont'd from previous page)

network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html (emphasis added).

- **Full Deployment of Multifactor Authentication** to login to our laptops, KeyPoint VPN connections, and PIV authentication for all VPN access to the OPM network.
- **Security Information and Event Management (SIEM),** which centralizes logging and alerting of all network and system events.
- **Enhanced Intrusion Detection System (IDS) –** improving our IDS capability that monitors the network for malicious activities and produces alerts and reports to a management station.
- **NetFlow and Packet Capture (PCAP) Network Information –** collection and retention of data to provide detailed analysis of IP network traffic for any future forensic investigations.
- **Improved Network Segmentation –** upgrading our existing segmentation to include customer level isolation.
- **And many more…**

Additionally, we have been working with all our customers to update our ATOs. This process includes an audit from a third party independent 3PAO assessor.

In closing, cybersecurity is vital to KeyPoint's mission, and we will continue to fortify the protection of our systems and information. Our adversaries are constantly working to create new methods of attack against our systems, and we must constantly work to meet and deter those attacks. While it may be impossible to ever truly eliminate the threat of a cyber-attack, we will continue to evaluate our protections to ensure they reflect the most current "best practices."

I want to thank the committee for drawing attention to this critical issue, and for allowing KeyPoint to share its perspective with the committee today. I look forward to addressing your questions.