



**UNITED STATES OFFICE OF PERSONNEL MANAGEMENT**

**STATEMENT OF  
DONNA SEYMOUR  
CHIEF INFORMATION OFFICER  
U.S. OFFICE OF PERSONNEL MANAGEMENT**

**before the**

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM  
UNITED STATES HOUSE OF REPRESENTATIVES**

**on**

**“Enhancing Cyber Security of Third-Party Contractors and Vendors”**

**---**

**April 22, 2015**

---

Chairman Chaffetz, Ranking Member Cummings and Members of the committee:

Thank you for inviting me to participate in today’s hearing to examine the cyber security of third party contractors. I am happy to be here with you today to share OPM’s experiences in the important area of cybersecurity.

As Chief Information Officer (CIO) for the Office of Personnel Management (OPM), I am responsible for the information technology (IT) security that supports OPM's mission to recruit, retain, and honor a world class workforce. Director Katherine Archuleta tasked me with conducting a thorough assessment of the state of IT at OPM – including cybersecurity. Director Archuleta’s goal, as laid out in OPM’s Strategic IT Plan, is to innovate IT infrastructure at OPM in a way that protects the sensitive information entrusted to us by the Federal workforce and the American people.

OPM and its contractors are under constant attack by advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused. In an average month, OPM thwarts almost two and a half billion confirmed attempts to hack its network. These attacks will not stop – if anything, they will increase. While we need to focus on how to prevent attacks, we know from the National Institute of Standards and Technology (NIST) Cybersecurity Framework

**Statement of Donna Seymour**  
**U.S. Office of Personnel Management**

---  
**April 22, 2015**

it is equally important that we focus on how to detect, investigate, and mitigate attacks.

In the past year, OPM and some of its contractors became the victims of cyber-attacks. Throughout the process of analyzing the breaches, OPM worked closely with the US Computer Emergency Readiness Team (CERT) at the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and other agencies. We also worked with the Office of Management and Budget (OMB), the CIO Council, and the Privacy Council. OPM followed OMB protocols in forming the Agency Response Team, investigating the incidents, and making notifications. We learned there were significant differences in our ability to understand and respond to these attacks because of the way sensitive information is exchanged, because of technical architecture, and because of the contractual relationship with the company.

The way in which the government shares sensitive information with the company is important to understand. In one case, company-owned laptops connected directly to the OPM network. In another case, company-owned laptops connected to the company's network and then to the OPM network. If laptops connect directly to the government network, it is easier to assess their security posture and limits exposure of the sensitive information.

The architecture of the network is important because it provides a framework for how sensitive information is accessed and exchanged, and it defines the boundaries for protecting the network. If the network is well defined and data is segregated, it is easier to protect. A well architected network also makes it easier to investigate incidents. And, of course, network logs help us understand what might have happened during an incident. When the government has a well-defined relationship with the contractor that specifically addresses information security and incident management, it is easier to work with the company to obtain information and plan remediation efforts. As a result of lessons learned this past year the agencies have collaborated, with the help of OMB Office of Federal Procurement Policy and the CIO Council, to share lessons learned. This includes contracting clauses that strengthen our relationship with contractors.

For example, at the onset of the contract a security assessment serves as a method to review the security features in place to protect sensitive information. This assessment should be validated by an independent assessment organization. But this only provides a perspective of the security posture at a point in time. A

**Statement of Donna Seymour  
U.S. Office of Personnel Management**

---  
**April 22, 2015**

continuous monitoring program is essential to enabling insight into the security posture of a system on a recurring basis.

Director Archuleta recognizes cyber-security as an agency priority. OPM's 2016 budget request included \$21 million to complete the modernization of our IT infrastructure. This funding is critical to continue the progress we have made so far in protecting data from relentless adversaries. For example, OPM is implementing continuous monitoring, in a lawful manner, both for its own network and systems as well as its contractor systems. We look at security controls on a rotating, more frequent basis, identifying vulnerabilities in real time given the changing nature of threats. Plans of action and milestones are created and tracked to remediate any concerns. OPM has also grown its cybersecurity capability which will allow us to do onsite technical inspections of contractor networks.

Thank you for this opportunity to testify today and I am happy to address any questions you may have.



Chief Information  
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

April 24, 2015

The Honorable Elijah E. Cummings  
Ranking Member  
Committee on Oversight  
and Government Reform  
United States House of Representatives  
2471 Rayburn House Office Building  
Washington, DC 20515


Dear Ranking Member Cummings:

Thank you for providing the U.S. Office of Personnel Management (OPM) the opportunity to testify at Wednesday's hearing "Enhancing Cybersecurity of Third-Party Contactors and Vendors." I am writing to clarify a response that I provided to your question as to whether I had seen any signs that Alteryx or USIS might bring a lawsuit against OPM.

After the hearing, I had an opportunity to review a timeline of events pertaining to the question. On September 9, 2014, OPM's contracting officer notified USIS that OPM would not exercise the options on the two then-existing contracts with USIS. On September 12, 2014, outside counsel for USIS requested a meeting with OPM's General Counsel. On September 16, 2014, outside counsel for USIS and Alteryx's General Counsel met with OPM's General Counsel, indicated that litigation with OPM was imminent, and requested preservation of documents relevant to USIS. Consequently, on September 17, 2014, OPM's General Counsel issued a litigation hold letter to several senior officials at OPM pertaining to documents that might be relevant to potential litigation with USIS. Although I was one of the recipients of the letter, I do not have a legal background and therefore did not fully understand the nature of your question. On September 18, 2014, OPM's General Counsel received a letter from outside counsel for USIS which noted that litigation appeared likely and memorialized USIS' September 16, 2014 verbal request for preservation of documents relevant to USIS. OPM's Office of General Counsel has informed me that, to date, no complaint has been filed by USIS or Alteryx against OPM.

I apologize for the lack of clarity and precision in the answer I provided at the hearing and look forward to working with you and the members of the Committee on the important issue of cybersecurity for third-party contractors and vendors.

Sincerely,



Donna Seymour

Chief Information Officer

cc: Representative Jason Chaffetz, Chairman, Committee on Oversight  
and Government Reform, United States House of Representatives