



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.



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
1900 E STREET NW, WASHINGTON, DC 20415

BIOGRAPHY

Donna K. Seymour

Donna K. Seymour is the Chief Information Officer (CIO) for the Office of Personnel Management (OPM). She is responsible for the information technology and innovative solutions that support the OPM's mission to recruit, retain, and honor a world class workforce.

Before coming to OPM, Mrs. Seymour served as the acting Deputy Assistant Secretary of Defense for the Office of Warrior Care Policy. She is a member of the Senior Executive Service for the Department of Defense, responsible for policy and oversight related to wounded, ill, and injured transitioning Service members.

In addition, Mrs. Seymour served as the Principal Director for Civilian Personnel Policy. Her responsibilities included human resources management policies affecting more than 900,000 civilian employees world-wide. She joined the Senior Executive Service in September 2007 and has more than 34 years of federal service. She also served as the Executive Director, Enterprise Human Resource Information Systems where she was responsible for providing Department-wide information technology solutions to meet the needs of 35,000 HR specialists, DoD civilian employees, and military and civilian managers and leaders.

Her previous experience includes: Director, Logistics Planning and Innovation Division for the Deputy Chief of Naval Operations (Fleet Readiness and Logistics); Acting Assistant for Administration and the Deputy Assistant for Administration to the Secretary of the Navy; and the Associate Chief Information Officer for Information Technology Policy Oversight at the Department of Transportation after serving as the Chief Information Officer at the Maritime Administration.



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
1900 E STREET NW, WASHINGTON, DC 20415

She began her federal career in 1978 and has concentrated primarily in the area of information technology, especially its ability to transform the workforce and business of the federal government, acquisition, financial management, and human resources management.

Mrs. Seymour holds a bachelor's of science degree in computer science from George Mason University where she graduated with Honors and Distinction, and has completed graduate level courses in operations research and management sciences. In 2010, she was awarded the Distinguished Civilian Service Award by the Secretary of the Navy, and in 2007 was named as a Top 100 Chief Information Officer by Computerworld.

As the Director of OPM, Archuleta is committed to building an innovative and inclusive workforce that reflects the diversity of America. As a long-time public servant, she is a champion of Federal employees.