

Congress of the United States

Washington, DC 20515

June 26, 2015

The President
The White House
Washington, DC 20500

Dear Mr. President:

According to published reports and testimony at Committee hearings on June 16, 2015 and June 24, 2015, at least 4.2 million Americans' personal and sensitive information is now in the hands of our adversaries because the Office of Personnel Management (OPM) failed to secure its networks.

The breach of OPM's networks is especially alarming because the information that the hackers accessed could include data related to security clearances, and could date as far back as 1985. In her testimony before the Committee, OPM Director Katherine Archuleta stated that "there is high degree of confidence that OPM systems related to background investigations of current, former, and prospective Federal government employees, and those for whom a federal background investigation was conducted, may have been compromised," and "any federal employee across all branches of government, whose organizations submitted service records to OPM, may have been compromised."¹ One former senior intelligence community official referred to the stolen data as the "crown jewels" and "a gold mine for a foreign intelligence service."²

Director Archuleta and her leadership team failed to correct serious vulnerabilities to OPM's network and cybersecurity posture despite repeated and urgent warnings from OPM's Inspector General that date back to 2007, at least. For eight years, the agency's leadership has been on notice as to the "material weakness" of OPM's data security.³ As recently as 2014, the Inspector General warned that many of OPM's major information systems were at high risk.⁴ According to the Inspector General's FY 2014 FISMA Final Audit Report, 11 out of 47 major information systems at OPM lacked proper security authorization.⁵

Five of those systems were in the Office of Chief Information Officer (CIO) Donna Seymour - the primary office responsible for OPM's cybersecurity policies and practices - and they remain a material weakness, according to the Inspector General. Ms. Seymour acknowledged in the hearing the risks inherent in operating systems without valid authorizations, yet continued to defend her decision to ignore the Inspector General and operate important systems without authorizations in place. That decision alone is, in our opinion, disqualifying.

¹ Testimony of Hon. Katherine Archuleta, Director, Office of Personnel Management, before the H. Comm. on Oversight and Gov't Reform, *OPM: Data Breach*, 114th Cong. (June 16, 2015).

² David Perera and Joseph Marks, *Newly disclosed hack got 'crown jewels,'* POLITICO, June 12, 2015.

³ U.S. Office of Personnel Management, Office of the Inspector General, *Final Audit Report: Federal Information Security Management Act Audit FY 2014*, 4A-CI-00-14-016 (Nov. 12, 2014) at 7, available at <http://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf> (last accessed June 16, 2015).

⁴ *Id.*

⁵ *Id.* at 10.

There is no excuse for failing to encrypt sensitive data at rest, require multi-factor authentication for remote access to critical systems, and properly segment data within the network, among other things that OPM failed to do. These are basic cybersecurity best practices that should have been addressed years ago. These catastrophic failures to implement relatively routine countermeasures allowed our adversaries to land a “significant blow” to America’s human intelligence programs.⁶

Simply put, the recent breach was entirely foreseeable, and Director Archuleta and CIO Donna Seymour failed to take steps to prevent it from happening despite repeated warnings.

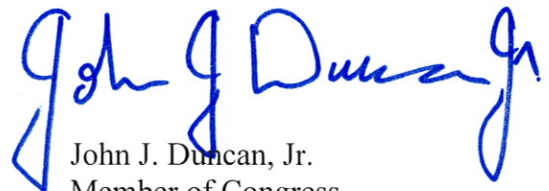
We listened closely to both Director Archuleta’s and Ms. Seymour’s testimony before the Committee. We have lost confidence in Director Archuleta’s ability to secure OPM’s networks and protect the data of millions of Americans. We have also lost confidence in OPM CIO Donna Seymour’s ability to do the same. This country’s hard working federal employees deserve better, and these systems are too important to leave unsecured.

Therefore, we respectfully request that you address this serious issue by removing Director Archuleta and Ms. Seymour from their positions. Thank you for your attention to this important matter.

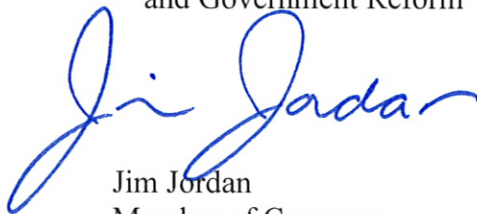
Sincerely,



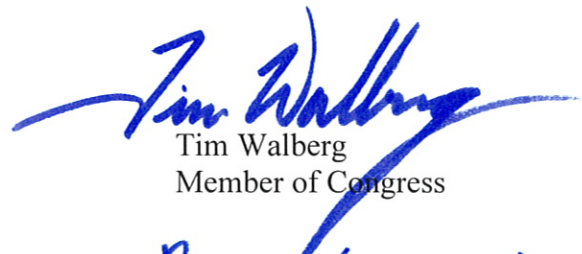
Jason Chaffetz
Chairman
Committee on Oversight
and Government Reform



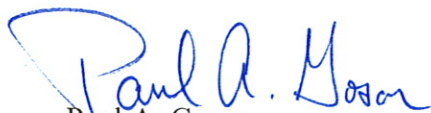
John J. Duncan, Jr.
Member of Congress




Jim Jordan
Member of Congress



Tim Walberg
Member of Congress

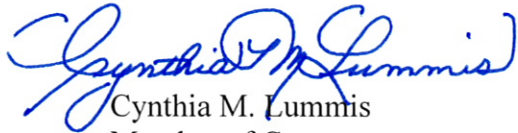


Paul A. Gosar
Member of Congress



Blake Farenthold
Member of Congress

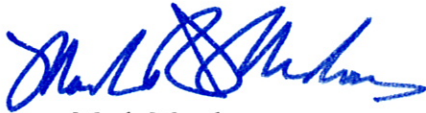
⁶ David Perera and Joseph Marks, *Newly disclosed hack got ‘crown jewels,’* POLITICO, June 12, 2015.



Cynthia M. Lummis
Member of Congress



Thomas Massie
Member of Congress



Mark Meadows
Member of Congress



Ron DeSantis
Member of Congress



Mick Mulvaney
Member of Congress



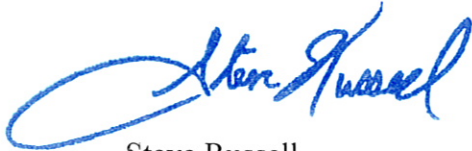
Mark Walker
Member of Congress



Rod Blum
Member of Congress



Jody B. Hice
Member of Congress



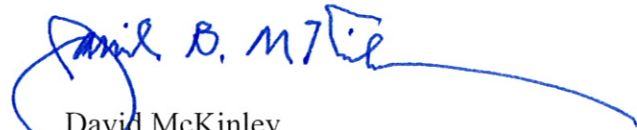
Steve Russell
Member of Congress



Glenn Grothman
Member of Congress



Will Hurd
Member of Congress



David McKinley
Member of Congress