JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

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
MINORITY (202) 225–5051
http://oversight.house.gov

August 6, 2015

The Honorable Beth F. Cobert
Acting Director
U.S. Office of Personnel Management
1900 E Street, NW
Washington, D.C. 20415-1000

Dear Ms. Cobert:

I write to augment concerns that Ms. Donna Seymour, Chief Information Officer (CIO) for the Office of Personnel Management (OPM), is unfit to perform the significant duties for which she is responsible.

On June 26, I communicated to President Obama that I have lost confidence in Ms. Seymour's ability to execute her role as CIO. Despite repeated warnings from the OPM Inspector General, Ms. Seymour failed to prevent breaches of personally-identifiable information, harming over 22 million federal employees and other individuals, and weakening our national security. As a result, I asked the President to address this serious issue by removing Ms. Seymour from her position.

I am deeply troubled Ms. Seymour remains at her post over a month after this request was made. My concerns about Ms. Seymour's ability to serve are amplified by a communication the Committee received from the Inspector General. In a letter dated August 3, 2015, OPM's IG notified me that on July 22, 2015 a memorandum was sent to you, and the letter advised me that "there have been situations where actions by the OCIO have interfered with, and thus hindered, the OIG's work. Further, the OCIO has repeatedly provided the OIG with inaccurate or misleading information."[1]

The Inspector General Act of 1978, as amended, makes clear the role of the Inspector General is to ensure the effective administration of the Agency and its programs. The IG relies

[1] Aug. 3, 2015, ltr. to Chairman Jason Chaffetz and Ranking Member Elijah E. Cummings from OPM Inspector General Patrick E. McFarland attaching, SERIOUS CONCERNS REGARDING THE OFFICE OF THE CHIEF INFORMATION OFFICER, Jul. 22, 2015.

on the leaders of each agency to take appropriate action when there are serious impediments to the efficacy of the agency's mission. It has been two weeks since the IG informed you of these serious transgressions and Ms. Seymour is still in a position of trust at the agency. Ms. Seymour has already failed the American people with her inability to secure OPM's networks, and to learn that her office may be actively interfering with the work of the Inspector General only adds insult to injury.

As Chairman of the House Committee on Oversight and Government Reform, the committee of jurisdiction for OPM, I urge the immediate removal of Ms. Seymour from her position.

Sincerely,

Jason Chaffetz
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Member

Enclosure

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

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

August 3, 2015

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

Enclosed is a July 22, 2015, memorandum that I sent to the U.S. Office of Personnel Management (OPM) Acting Director Beth F. Cobert discussing serious concerns held by the OPM Office of the Inspector General (OIG) regarding the OPM Office of the Chief Information Officer (OCIO).

Specifically, there have been situations where actions by the OCIO have interfered with, and thus hindered, the OIG's work. Further, the OCIO has repeatedly provided the OIG with inaccurate or misleading information, some of which was repeated under oath by former OPM Director Katherine Archuleta and OPM's Chief Information Officer at the hearings held by your Committee on June 16th and June 24th.

As you are aware, the OIG generally adheres to a policy whereby we provide the agency with two full business days to review a report or other document of special interest before we send it to Congress. However, because she has been at OPM for less than one month, Acting Director Cobert requested, and I granted, a one week extension before I transmitted the memorandum to you.

We have been informed that the agency is preparing a response to this memorandum. From what we understand, OPM will be providing it to you directly.

In a few weeks, we expect to issue an update to the Flash Audit Alert that we issued on June 17, 2015. This document will include (1) comprehensive analysis of OPM's

June 22, 2015, response to the Flash Audit Alert, and (2) updates on OIG audit work related to the infrastructure improvement project.

If you have any questions, please do not hesitate to contact me at (202) 606-1200, or your staff may contact J. David Cope, Assistant Inspector General for Legal and Legislative Affairs, at (202) 606-2851 or dave.cope@opm.gov, or Susan L. Ruge, Associate Counsel, at (202) 606-2236 or susan.ruge@opm.gov.

Sincerely,

Patrick E. McFarland
Inspector General

cc: The Honorable Mark Meadows, Chairman, Subcommittee on Government Operations, Committee on Oversight and Government Reform, U.S. House of Representatives

The Honorable Gerald E. Connolly, Ranking Member, Subcommittee on Government Operations, Committee on Oversight and Government Reform, U.S. House of Representatives

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

July 22, 2015

MEMORANDUM FOR BETH F. COBERT
Acting Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Serious Concerns Regarding the Office of the Chief Information Officer

I would like to bring to your attention concerns held by the U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) regarding OPM's Office of the Chief Information Officer (OCIO). It is imperative that these concerns be addressed if OPM is to overcome the unprecedented challenges facing it today. I am sharing this with you not to accuse any OPM employees of intentional misconduct, but rather to clear the air and rebuild a productive relationship between the OIG and the OCIO.

In certain situations, the OCIO's actions have hindered the OIG's ability to fulfill our responsibilities under the Inspector General Act of 1978, as amended (IG Act). Further, we have found that the OCIO has provided my office with inaccurate or misleading information, some of which was subsequently repeated by former OPM Director Katherine Archuleta at Congressional hearings.

Under the IG Act, we are charged with conducting independent and objective oversight of agency operations so that we may keep you and Congress informed about major problems or deficiencies that we may discover. My office provides you with a unique perspective that hopefully allows you to better evaluate the status of OPM's programs and activities. It is with this in mind that I write to you today.

In the past, the OIG has had a positive relationship with the OCIO. Although the OIG may have identified problems within the OCIO's areas of responsibility, we all recognized that we were on the same team, and the OCIO would leverage our findings in an effort to bring much needed attention and resources to OPM's information technology (IT) program. Unfortunately, this is no longer the case, and indeed, recent events make the OIG question whether the OCIO is acting in good faith.

There appears to be a shift in the attitude of OCIO leadership. It may be best exemplified by a statement made by [redacted]

[redacted]"[1] This is disappointing because I would hope that the OCIO would want to work with my office regardless of whether they are "required" to, but rather because it is in the best interest of the agency to do so.

One result of this new culture is that the OCIO has interfered with, and thus hindered, the OIG's oversight activity. Examples of this are included in Attachment A to this memorandum. One of the most troubling examples is how the agency embarked upon a complex and costly IT infrastructure improvement project without any notification to our office. It is disturbing that the OCIO would exclude the OIG from such a major initiative, especially given the fact that it was undertaken in response to the March 2014 data breach.

In addition, the OCIO has created an environment of mistrust by providing my office with incorrect and/or misleading information. Examples of this are included in Attachment B to this memorandum. (We assume the former Director based the misstatements listed upon information from the OCIO.) It is surprising, given the high level of interest expressed by both Congress and the public, that the Office of Management and Budget (OMB) has not offered any clarification on these serious matters. Our audit team will be reaching out to OMB to discuss this.

I appreciate the interest you have demonstrated in working with us. I look forward to hearing your thoughts on how we can move forward together.

[1] [redacted]

Attachment A:
OCIO's Interference with and Hindrance of OIG Activities

1. **Situation:** In October 2014, due to concerns raised after a security breach at United States Investigative Services (USIS) was identified in June 2014, the U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) informed [redacted] of our intent to audit KeyPoint Government Solutions (KeyPoint). At an October 16, 2014 meeting, [redacted] requested that we delay this audit, stating that the U.S. Department of Homeland Security (DHS) had just completed a comprehensive assessment of KeyPoint, which was also in response to the USIS breach. Therefore, [redacted] was concerned that our audit would interfere with KeyPoint's remediation activity. The OIG tries to coordinate our oversight work with the OPM program offices to the maximum extent possible, and so we agreed to delay our audit. We later discovered, however, that OPM became aware in early September 2014 that KeyPoint had been breached. Despite knowing this, [redacted] did not inform OIG staff of the breach in the October 16th meeting when [redacted] requested that we delay our audit work.

   Result: Our audit, which was a comprehensive evaluation of the information technology (IT) security posture of KeyPoint, was delayed for over three months. The DHS review was focused on incident response objectives, and did not have as wide of a scope as [redacted]. In fact, our audit identified a variety of areas that were not part of DHS's review where KeyPoint could improve its IT security controls. [redacted] The delay also prevented us from communicating important information that may have been relevant to the recent Congressional hearings regarding the OPM data breaches.

2. **Situation**: The Office of the Chief Information Officer (OCIO) failed to timely notify the OIG of the first data breach at OPM involving personnel records. OPM did not inform the OIG of the breach until *one week* after it was discovered. In fact, the OIG learned about it only because the OIG Special Agent in Charge (SAC) ran into the OCIO [redacted] in the hallway, and the [redacted] asked the SAC to meet with him later (at which time the SAC was informed of the first breach).

   Result: Failure to include OIG investigators and auditors from the beginning of the incident impeded our ability to coordinate with other law enforcement organizations and conduct audit oversight activity.

3. **Situation**: During the investigation of the second breach involving background investigation files, the OIG requested to attend meetings between OCIO staff, the Federal Bureau of Investigations (FBI), and the DHS U.S. Computer Emergency Readiness Team (US-CERT). [redacted] stated that the OIG could not attend these meetings because our presence would "interfere" with the FBI and US-CERT's work.

   Result: This action is a violation of the Inspector General Act of 1978, as amended (IG Act). The OIG contacted the FBI and US-CERT directly and did indeed meet with them

without adversely affecting the progress of the investigation. These meetings provided the OIG with critical information necessary for our own investigatory and audit work. What [redacted] considered "interference" was simply the OIG fulfilling our responsibilities.

4. **Situation**: The OCIO failed to inform the OIG of a major new initiative to overhaul the agency's IT environment. [2] We did not learn the full scope of the project until March 2015, nearly a year after the agency began planning and implementing the project. This exclusion from a *major* agency initiative stands in stark contrast to OPM's history of cooperation with our office.

   Result: The role of the OIG is to promote economy, efficiency, and effectiveness in the administration of the agency's programs, as well as to keep the Director, Congress, and the public informed of major problems and deficiencies.[3] Because the OIG was not involved, agency officials were denied the benefit of an independent and objective evaluation of the project's progress from the beginning. The audit work that we have performed since learning of this project has identified serious deficiencies and flaws that would have been much easier to address had we been able to issue recommendations earlier in the project's lifecycle.

[2] In fact, during the fall of 2014 the OIG had to repeatedly request that OIG IT support staff (not OIG auditors) be allowed to attend meetings about IT security upgrades that OPM was implementing. In an email exchange discussing the OIG's request to attend, [redacted] At that time, we did not know that these upgrades were actually part of the overarching infrastructure improvement project because OPM never informed us that such a vast project was underway.

[3] IG Act § 2(2)-(3).

Attachment B:
Incorrect/Misleading Information Provided by OCIO

1. [redacted]

2. [redacted]

3. [redacted]

[redacted]

[redacted]

4. [redacted]

[redacted]

[redacted]

5. [redacted]

[redacted]