United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

October 2, 2014

The Honorable Katherine Archuleta
Director
Office of Personnel Management
1900 E St. NW
Washington, DC 20415-1000

Dear Director Archuleta:

We are writing to ask about steps you will take to ensure the quality and timeliness of background investigations by the Office of Personnel Management (OPM) in light of OPM's decision not to extend the options on its contracts with U.S. Investigations Services, Inc. (USIS).

Background investigations are critical to national security. Federal officials rely on these investigations to determine who are trustworthy to have access to classified information, who have the character and credentials to work in federal service or as a federal contractor, and who should have access to sensitive federal facilities or information systems.

As you know, we and many of our colleagues in Congress have had growing concerns about the role of USIS in background investigations due to fraud allegations that have been brought against the company by the Department of Justice, as well as recent revelations about a cyber breach of the company's systems.

Recently, OPM has relied on only three contractors to perform background investigation fieldwork, with roughly half of the work being contracted to USIS. Because OPM performs over 90 percent of background investigations for the entire federal government, the removal of any one of OPM's contractors could have a significant governmentwide impact on processing of background investigations.

The redistribution of work previously done by USIS undoubtedly will be a major management challenge. Therefore, we would appreciate an update in writing, as well as a briefing for Committee staff, on the following, by October 16, 2014:

1. What are the short- and long-term plans for assigning background investigations that otherwise would have been performed by USIS?

2. What precautions will you take to ensure that quality standards are fully met as workloads surge for OPM's own investigators and those of OPM's other contractors?

3. What actions has OPM taken over the past year, and what further actions do you plan, to develop and apply metrics to assess the completeness and quality of background investigations, whether performed by federal employees or contractors?

4. What will be the impact on timeliness of reviews as work is transitioned from USIS elsewhere? How will OPM work with other agencies to prioritize reviews whose completion is most urgent?

5. Have you assessed what the appropriate balance between contractor and federal employees should be for background investigation work, and if so, what is the appropriate ratio?

6. Is OPM subject to any personnel ceilings that hinder augmentation of the OPM investigative staff?

7. Even if OPM reduces its overall reliance on contractors in terms of the number of investigations conducted by contractor employees, should OPM increase the competitive pool of contractors who are eligible to conduct investigations in order to avoid the risks of being overly reliant on any one contractor?

8. What suspension or debarment actions, or other actions, has OPM taken against individual employees of USIS who have engaged in fraud, or who have otherwise demonstrated that they lack the responsibility required to be a federal contractor, so that these individuals are not hired by other contractors?

9. How does OPM evaluate its contractors for compliance with cybersecurity best practices and requirements, including the Federal Information Security Management Act (FISMA) and the Cybersecurity Framework developed pursuant to Executive Order 13636?

10. What steps is OPM taking to ensure its other contracts, as applicable, contain an appropriate level of cybersecurity requirements to help prevent another breach among its contractors?

11. What data was accessed on the USIS cybersecurity breach? What agencies had data on the USIS database and were affected? What actions have been taken to address potential security or counterintelligence concerns associated with this breach?

12. Is OPM aware of any other incidents of USIS's or other federal agencies' networks being breached by a cyber attack? If so, please list and describe all such incidents for the two most recent fiscal years.

We appreciate your attention to these important questions, and we are committed to working with you to address these challenges. [redacted] Should these questions require classified information to be included in the response, please send that portion of the response separately to the Office of Senate Security.

With warmest personal regards, we are

Sincerely yours,

Thomas R. Carper
Chairman

Tom A. Coburn, M.D.
Ranking Member