United States Senate

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

October 2, 2014

The Honorable Jeh C. Johnson
Secretary
U.S. Department of Homeland Security
Washington, DC 20528-0150

Dear Secretary Johnson:

We are writing to obtain more information about the steps the Department of Homeland Security (DHS) is taking to respond to the data breach at U.S. Investigations Services, Inc.(USIS) and to ensure the quality and timeliness of background investigations for the DHS workforce.

As you know, we, along with 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. The recent revelation about a breach of the company's information systems only adds to our concerns and raises many questions about the background investigation process at DHS.

The breach at USIS also raises many questions about the safeguards contractors are taking to protect against cyber intrusions, as well as the oversight provided by the contracting agency. As the department charged with helping to secure federal civilian networks, DHS must lead by example in this area and work with other agencies across the government to help them better protect their sensitive information. If you determine that additional tools and authorities are needed to further improve federal network security, we urge you to inform the Committee as soon as possible.

It is our understanding that the Department has already taken many steps to address the USIS breach and notify impacted individuals. To further understand these efforts and to provide more clarity on the impact of the breach at DHS, we request answers to the following questions, as well as a briefing for Committee staff, by October 16, 2014. Any classified information provided in response to this letter should be provided under separate cover through the Office of Senate Security.

1. Why does the Department continue to conduct its own background investigations when the Office of Personnel and Management conducts more than ninety percent of all background investigations for the government? Are there cost savings or efficiencies that are available to the Department that it would not otherwise receive if it worked through OPM? If so, please provide the Department's analysis demonstrating these cost savings or efficiencies.

2. It is our understanding that the USIS data breach exposed the personal information of significantly more individuals at DHS than other agencies. Please explain why. In doing so, please discuss how USIS stored background investigation information for DHS and whether this process differed from how USIS worked with and stored background information for other agencies. If different, please discuss why and whether DHS is reconsidering how it processes background information for security clearances.

3. Does DHS assess there to be any counterintelligence or other security risk posed to DHS employees whose information may have been exposed by this breach?

4. What actions has DHS 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?

5. What will be the impact on timeliness of reviews as the stop order for work performed by USIS continues? What is your plan for mitigating any impact on timeliness, and how will you prioritize reviews whose completion is most urgent?

6. What cyber security requirements does DHS typically include in its contracts and what cybersecurity requirements did DHS have in its contract with USIS?

7. How does DHS 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? To what extent, and how frequent, were evaluations conducted on USIS?

8. Since the USIS breach, what steps has DHS taken to ensure other contracts, as applicable, contain an appropriate level of cybersecurity requirements to help prevent another breach among its contractors?

9. What steps has DHS taken to help other federal agencies review the sufficiency of cybersecurity requirements in their contracts with vendors?

We appreciate your attention to these important questions, and we are committed to working with you to address these challenges. [redacted]

With warmest personal regards, we are

Sincerely yours,

Thomas R. Carper
Chairman

Tom A. Coburn, M.D.
Ranking Member