Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528-0655

Homeland Security

September 9, 2015

Ms. Lisa Sotto
Chair, DHS Data Privacy and Integrity Advisory Committee (DPIAC)
c/o Hunton & Williams LLP
200 Park Avenue
New York, NY 10166

Dear Lisa:

The Department of Homeland Security (DHS) has a duty to safeguard personally identifiable information (PII) in its possession in order to prevent the compromise of the PII and to maintain the public's trust. In the event of an incident in which PII is compromised or potentially compromised, the Department is required to evaluate whether notice should be provided to affected individuals and to determine the timing and content of that notice. Notification to the individuals affected by the incident is a critical step toward mitigating the adverse effects of a loss or compromise of PII and it is imperative that the Department provide notice that is appropriate and adequate for a particular incident.

In order that the Department may benefit from the DPIAC's substantial experience, I request that the Committee provide written guidance on best practices for notifying individuals impacted by a large-scale data breach. Specifically, I ask that the Committee consider and address the following:

> In the context of large-scale data breaches, what criteria should the Privacy Office consider to inform DHS's decision of whether and when to notify the impacted individuals? Once DHS has decided to notify impacted individuals, what are best practices with respect to the source, content, and delivery mechanism (e.g., mail, e-mail) for the notification? Is it possible to 'over notify,' by saturating affected individuals with information or bulletins? In addition to delivering the actual notification, are there best practices supporting a notification process (e.g., establishing a call center) that should be considered?

If my office can provide any assistance to you as the Committee undertakes this tasking, please do not hesitate to let Sandra Taylor, Naomi Parnes, or me know.

Very truly yours,

Karen L. Neuman
Chief Privacy Officer