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

Homeland Security

December 14, 2011

Alejandro Mayorkas
Director, U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
Washington, DC 20529

Dear Director Mayorkas:

As you are aware, the DHS Privacy Office conducted an investigation into the Fraud Detection and National Security Directorate's (FDNS), a component within U.S. Citizenship and Immigration Services (USCIS), use of social networking sites to inform benefit determinations. This investigation resulted in the 15 recommendations attached to this letter. The recommendations are divided into three distinct categories: 1) access control and privacy training, 2) auditing, and 3) compliance.

The DHS Privacy Office will follow up with the appropriate officials within USCIS and FDNS as to the status of these recommendations 90 days after the date of this letter. Following the 90 day review period, and likely at a future date, the DHS Privacy Office will perform a more detailed review and assessment of USCIS and FDNS to determine compliance with these recommendations and applicable laws and DHS and USCIS policies.

We want to thank you for the cooperation we received from USCIS and FDNS during the course of this investigation. If you have any questions about these recommendations, please do not hesitate to contact me.

Sincerely yours,

Mary Ellen Callahan
Chief Privacy Officer

cc: Steve Bucher, FDNS, Acting Associate Director

DHS-001-0427-001465

Attachment: Recommendations Resulting from DHS Privacy Office Investigation
A. Mayorkas, Director
U.S. Citizenship and Immigration Services
December 14, 2011

Within 90 days of the issuance of this letter, we recommend:

With regard to access control and privacy training:

1. USCIS cease the use of social networking sites for investigative or adjudication purposes until proper policies, procedures, and training are implemented.
2. USCIS issue specific policies and procedures approved by the DHS Privacy Office, the DHS Office of Policy, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel for the use of social networking sites by all USCIS personnel for investigative or adjudication purposes consistent with the December 2010 DHS decision memo and 1999 DOJ Principles.
3. USCIS establish specific guidelines for determining which personnel are allowed to utilize social networking sites in the performance of their duties.
4. USCIS maintain a log of all personnel granted access to social networking sites for case review. Access requests must be renewed on an annual basis consistent with the training requirements below.
5. USCIS personnel accessing social networking sites be required to sign "Rules of Behavior," that have been approved by the DHS Privacy Office, specifically related to the use of social networking sites.
6. USCIS provide training regarding the use of social networking sites to all personnel before being granted access. The USCIS Privacy Office, with assistance from the DHS Privacy Office, must review the training materials before implementation. Refresher training must be completed annually.
7. USCIS personnel document each case that is researched using social networking sites including what information was gathered and how it was used (e.g., whether it affected the granting of benefits).
8. USCIS personnel follow the requirement in DHS Sensitive Systems Policy Directive 4300A to use government-issued equipment and government accounts when accessing social networking sites.

With regard to auditing:

9. USCIS personnel place any information that is found and used to inform benefit determinations, derogatory or not, into FDNS-DS or other similar systems, obtained from social networking sites.
10. USCIS maintain audit logs of all access to social networking sites, to be reviewed, along with information placed into FDNS-DS, on a regular basis by USCIS Privacy Office staff.
11. USCIS Privacy Office, FDNS HQ, and DHS Privacy Office staff audit the use of social networking sites through privacy compliance reviews of FDNS-DS or other similar systems and required audit logs.

With regard to compliance:

12. FDNS HQ issue a policy memorandum to all FDNS personnel requiring notice and approval for all new uses of personally identifiable information and technology, including pilot projects, by completing and submitting Privacy Threshold Analyses (PTAs) to the DHS Privacy Office through the USCIS Privacy Office.
13. USCIS complete and submit to the DHS Privacy Office through the USCIS Privacy Office a Privacy Impact Assessment or appropriate Privacy Impact Assessment update for the use of social networking sites for operational use.
14. FDNS and/or the USCIS Office of Information Technology complete and submit to the DHS Privacy Office through the USCIS Privacy Office a Privacy Impact Assessment and System of Records Notice for the use of the Remote Retrievable Disposable Desktop.
15. USCIS complete and submit to the DHS Privacy Office through the USCIS Privacy Office Privacy Impact Assessments and System of Records Notices as applicable before using new technologies, or engaging in new collections of personally identifiable information, for investigative or adjudication purposes.