Policy Number: 10083.1
FEA Number: 360-112-002b

Office of the Director

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

U.S. Immigration and Customs Enforcement

MAY 17 2013

MEMORANDUM FOR: ICE Personnel

FROM: John Morton
Director

SUBJECT: Use of Public Online Information for Non-Law Enforcement Work-Related Activities

Purpose:

This memorandum provides U.S. Immigration and Customs Enforcement (ICE) personnel guidance on acceptable uses of online information, including the operational use of social media, within the scope of their non-law enforcement work-related activities.

Background:

On June 8, 2012, the Chief Privacy Officer of the Department of Homeland Security (DHS) issued a Directive and Instruction, "the DHS Privacy Policy" that established DHS privacy policy for the operational use of social media.[1] The definition of social media in the DHS Policy is drafted broadly so as to likely include general uses of online information.[2]

Pursuant to the DHS Privacy Policy, all components are required to complete a template detailing any categories of the operational use of social media in which ICE is currently or will be engaged and submit it to the DHS Chief Privacy Officer for approval. Components must also draft Rules of Behavior governing each category of operational use of social media in which they are currently or will be engaged. On June 28, 2012, the Memorandum for law enforcement personnel titled the "Use of Public and Non-Public Online Information" was issued providing ICE's rules of behavior for personnel engaged in law enforcement activities. The present memorandum provides ICE personnel with guidance on acceptable uses of online information, including the operational use of social media, within the scope of their non-law enforcement work-related activities.

---

[1] See DHS Management Directive 110-01 and Instruction 110-01-001, *Privacy Policy for the Operational Use of Social Media.*

[2] See DHS Instruction 110-01-001, *Privacy Policy for the Operational Use of Social Media* at 4.

Discussion:

Personnel at ICE should follow the below principles for the non-law enforcement use of public and non-public online information.

To implement these core principles, ICE directorates and program offices may establish guidance and/or modify existing guidance, as necessary, or reference the DHS Privacy Policy as applicable to the activities in question.

ICE Principles for Non-Law Enforcement Use of Public Online Information:

1. Use of Equipment. Personnel may only use government-issued equipment when engaging in the use of online information in the performance of their non-law enforcement duties.

2. Use of Email and Accounts. Personnel must use screen names or identities that indicate an official DHS affiliation, and use DHS email addresses to open accounts when engaging in the use of the Internet to include social media in the performance of their non-law enforcement duties.

3. Public Interaction. Except with the consent of the individual or when necessary for training activities and professional social networking, personnel engaged in non-law enforcement activities may access publicly available information only by reviewing posted information and may not interact with the individuals who posted the information.

4. Privacy Settings. When engaged in non-law enforcement activities, personnel must respect individuals' privacy settings and access only information that is publicly available on the Internet, to include social media.

5. PII Collection. Personnel generally may collect only the minimum personally identifiable information (PII) necessary for the proper performance of their authorized non-law enforcement duties.

6. PII Safeguards. Personnel will protect PII as required by the Privacy Act, if applicable, and DHS privacy policy.

7. Documentation. Personnel will retain the contents of their use of the Internet, including social media, if they would have retained that information had it been written on paper. These contents should be preserved in appropriate ICE recordkeeping systems in accordance with office procedures and in a manner authorized by the relevant records schedule.

8. Online Communications Generally. Personnel may use online services to communicate in the same way that they are authorized to use other types of communication tools, such as the telephone and the mail.

9. Activity during Personal Time. While not on duty, personnel are generally free to engage in personal online pursuits. If, however, the off-duty online activity on government issued or personal equipment directly and substantially relates to a work-related matter, personnel are bound by the same restrictions regarding the use of online information as would apply when on duty.

No Private Right of Action

This memorandum is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable by law by any party in any administrative, civil, or criminal matter.