Privacy Compliance Review

of

DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS Use of Unidirectional Social Media Applications Communications and Outreach

March 28, 2012

Contact Point
Kathleen McShea
Director of New Media and Web Communications
Office of Public Affairs
Department of Homeland Security
(202) 282-8166

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

I. BACKGROUND

DHS utilizes social media for communications, public affairs, and outreach purposes and has an official presence on many of the major social media platforms such as Facebook, Twitter, and YouTube. To ensure DHS' use of social media for communications/outreach/dialogue with the public adheres to privacy requirements, DHS developed two Department-wide privacy impact assessments (PIAs): a PIA for Department use of social networking interactions and applications; and a PIA for Department use of unidirectional social media.[1] If an initiative meets the PIA requirements, it is added to the Appendix of the appropriate PIA through the Social Media Privacy Threshold Analysis process. As noted in the PIAs, these initiatives are subject to Privacy Compliance Reviews (PCRs).

The DHS Privacy Office conducted this PCR to 1) determine whether selected DHS social media uses listed in the DHS-wide social media PIA appendices continue to meet the requirements as described in the PIAs and 2) to determine if the appendices of the DHS-wide social media PIAs reflect an accurate accounting of DHS users. To address our objectives, we reviewed official DHS user accounts on three major social media platforms against the requirements outlined in the DHS-wide social media PIAs, met with DHS Office of Public Affairs (OPA) officials, and analyzed OPA policies and procedures for social media. In addition, we compared the DHS-wide social media PIA Appendices against OPA's listing of official DHS user accounts and scanned Facebook, YouTube, and Twitter to identify whether the PIA Appendices reflected a full accounting of DHS social media uses.

II. SUMMARY

Official DHS user accounts on social media platforms meet most of the requirements as outlined in the PIAs but some practices could be improved. First, regarding DHS Use of Social Networking Interactions and Applications for Communications/Outreach/Public Dialogue:

- DHS official user accounts reviewed on Facebook, YouTube, and Twitter remain focused on external relations (communications/outreach/public dialogue) to provide information about or from the Department, and to provide customer service;
- All official DHS user accounts listed in the Appendix and identified through this PCR utilize the official DHS seal and account names that reflect an official DHS presence;

[1] See DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue (September 16, 2010) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_socialnetworkinginteractions.pdf and DHS/ALL/PIA-036 Use of Unidirectional Social Media Applications (March 8, 2011) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_unidirectionalsocialmedia.pdf.

- DHS user accounts are not actively seeking PII except in one instance where a DHS form hosted on a DHS server was embedded into an official DHS page on Facebook. This was subsequently resolved by the account owner by replacing the embedded form with a link to the official DHS.gov page consistent with PIA requirements;
- Appropriate privacy policies are either linked or posted on DHS official user accounts on Facebook but were not always on Twitter and YouTube;
- DHS official user accounts are not "friending" public users on Facebook and YouTube, but were found to be "following" non-governmental organizations on Twitter without obtaining a waiver from the DHS Privacy Office as required in the PIA. Notwithstanding, the "following" appeared to be related to the mission of the particular organization (e.g., the Federal Emergency Management Agency (FEMA) "likes" and "follows" the Red Cross). As of the signing of this report, FEMA has a waiver on file with the DHS Privacy Office.

Regarding DHS Use of Unidirectional Social Media for Communications and Outreach in compliance with PIA requirements:

- DHS social media uses listed in the PIA Appendix remain focused on one-way communications and outreach to the public about DHS initiatives.
- Unidirectional uses listed in the Appendix are not actively seeking PII;
- DHS users listed in the Appendix were not actively seeking PII, and complied with appropriate notice requirements.

Although DHS official accounts and uses for both interactive and unidirectional uses of social media met most requirements, practices for keeping DHS-wide PIAs up-to-date could be improved. Specifically, we found that both DHS-wide social media PIA Appendices do not reflect the full scope of uses by DHS. The DHS Privacy Office has taken steps to address this issue and updated the Appendix to the Use of Social Networking and Applications PIA on February 15, 2012 to more accurately reflect the scope of DHS users and is currently working on clarifying the scope and process for reflecting DHS approved uses in the unidirectional PIA. To improve compliance and clarify PIA requirements, the DHS Privacy Office is making several recommendations including those which it will take the lead on implementing.

III. SCOPE AND METHODOLOGY

The DHS Privacy Office conducted this PCR from January 26 to February 29, 2012. The DHS Privacy Office carried out the following activities to address its objectives:

- Interviewed OPA's New Media Analysts regarding OPA's use and management of official DHS accounts on social media platforms;

- Reviewed OPA policy and procedures for social media;
- Reviewed DHS-wide PIAs for DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue (September 16, 2010) and DHS Use of Unidirectional Social Media Applications Communications and outreach (March 8, 2011), respectively, to identify the requirements (e.g., official seals used, appropriate policies posted, no active PII collection) and reviewed DHS official user accounts listed on the Appendices for compliance with the requirements in the PIAs;
- Reviewed lists of approved accounts on the DHS-wide PIA Appendices and compared them against OPA's list of active social media uses for communications and outreach purposes available at http://www.dhs.gov/socialmedia.
- Searched Facebook, Twitter, and YouTube, to identify if additional official DHS user accounts not listed in the DHS-wide PIAs were in place.

IV. PRIVACY COMPLIANCE REVIEW

A. USE OF SOCIAL NETWORKING INTERACTIONS AND APPLICATIONS FOR COMMUNICATIONS/OUTREACH/PUBLIC DIALOGUE

Collection of Information

Requirements: When DHS uses social networking websites and applications, it shall not: 1) actively seek PII, and may only use the minimum amount of PII, that it receives, to accomplish a purpose required by statute, executive order, or regulation or 2) search social networking websites or applications for or by PII.

Review: We reviewed DHS official accounts listed on the DHS-wide Social Networking Interactions and Applications for Communications/Outreach/Public Dialogue PIA Appendix on Facebook, Twitter, and YouTube against the above stated PIA requirements for content and to ensure that PII was not actively sought.

Findings: The DHS official accounts reviewed on these social media platforms remain focused on the purposes of external relations (communications/outreach/public dialogue) to provide information about or from the Department, and to provide customer service. Official DHS accounts were not actively seeking PII but for one instance where a DHS form hosted on a DHS server was embedded into an official DHS page on Facebook. This was subsequently resolved by replacing the embedded form with a link to the official DHS.gov page.

Notice

Requirements: The Department shall establish official accounts that clearly state that they are managed by DHS. For example, the Department shall use the DHS seal on the social networking websites or applications. Employees responsible for managing such websites

or applications should clearly identify themselves, for example, using the name "DHS John Q. Employee," when interacting with the public. To the extent feasible, the Department must post a privacy notice on the social networking website or application itself.

Review: We reviewed official user accounts listed on the DHS-wide social media PIA Appendix as well as official user accounts identified on Facebook, Twitter, and YouTube through this PCR that were not on the Appendix, to identify whether official DHS seals and profile names signified an official DHS presence. We also examined official DHS user accounts to determine if appropriate privacy notices were either linked to or posted to the social networking website itself.

Findings: DHS is complying with requirements to establish accounts that clearly indicate they are managed by DHS, to the extent feasible, on the social media platform. DHS official accounts reviewed made use of official DHS seals and utilized profile names signifying an official DHS presence. For example, the DHS official pages on Facebook and Twitter prominently display the official DHS seal and profile names clearly denote a DHS presence (e.g., "Department of Homeland Security," "@DHSgov"). Official Component pages are also complying with these requirements using either the official DHS seal or an official component seal.

Appropriate privacy policies are either linked to or posted on DHS official user accounts on Facebook but compliance with the requirement to either post or link privacy policies was uneven for official DHS accounts on Twitter and YouTube. Only one official DHS account on Twitter included a link to its official website stating where its privacy policy and legal disclaimers could be found. None of the other DHS accounts reviewed posted or linked to their privacy policies. Character limitations on the Twitter platform prevent DHS official accounts from posting their privacy policies in full. Official DHS YouTube accounts did not always state or link to the agency's privacy policy. As part of the DHS Privacy Office's PCR and follow-up with the components, all of the components updated their profiles to include links to their policies. According to several account managers, recent template changes on YouTube may have been the cause of missing links to notices.

Recommendations: The DHS Privacy Office recommends that all DHS official accounts on the Twitter platform periodically "tweet" a link to their agency's privacy policy (e.g., every 2 months) to better inform the public. In addition, the DHS Privacy Office recommends that account managers for official DHS channels on YouTube periodically review their profiles and ensure privacy policies are linked or posted.

Official DHS Account Interactions with Non-Governmental Users

Requirement: DHS may not "friend" individual users proactively but may "friend" other U.S. federal, state, local, and tribal government agencies. DHS components wishing to "friend" other non-government entities, such as media outlets or mission-related non-governmental organizations (NGOs), must request a waiver of this requirement from the DHS Privacy Office.

Review: We reviewed official DHS accounts listed on the DHS-wide social media PIA Appendix and the extent to which connections were made with other public users on Facebook, YouTube, and Twitter platforms. This included identifying any proactive connections made through DHS accounts by "friending," "liking," "subscribing," or "following."

Findings: DHS is complying with requirements not to proactively "friend" users on the Facebook platform; however, many official DHS accounts are "following," "liking," and, in limited cases, "subscribing to" NGOs on Twitter, Facebook, and YouTube, respectively, without having obtained waivers for these activities. Nonetheless, we found official DHS accounts "following," "liking," and, "subscribing" activities to be largely consistent with the Component's mission. For example, FEMA "likes" and "follows" non-profit organizations related to its mission such as the Red Cross. As of the signing of this report, FEMA has a waiver on file with the DHS Privacy Office.

The DHS Privacy Office developed the waiver requirement to prevent DHS from improperly monitoring individual social media accounts, from gaining access to information that public account users designate as available only for their network (i.e., "friends") to see, and to prevent mission creep. Currently, OPA's guidance which permits "following" non-governmental organizations with a mission tie and the PIA waiver requirement are currently out of sync and the differences should be addressed.

Recommendations: Recognizing that social media platforms vary in what information is made available about their users when establishing connections to other accounts, the DHS Privacy Office will replace the waiver process with guidance developed in coordination with OPA on establishing appropriate connections with non-governmental organizations. Official DHS accounts should continue to refrain from "friending" private citizens.

The DHS Privacy Office is also recommending that DHS official account holders periodically review connections proactively made to NGOs to ensure such connections are appropriately tied to the component's mission.

Scope of Users Reflected in the DHS-wide Social Media PIA Appendix

Requirement: In order to be covered by the PIA for DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue, a component must submit a Social Media Privacy Threshold Analysis (SMPTA) to the DHS Privacy Office for review and approval before an initiative's addition to the PIA Appendix.

Review: We reviewed OPA's list of official DHS accounts listed on www.dhs.gov/socialmedia and compared it against the Appendix of the DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue PIA. In addition, we searched Facebook, Twitter, and You Tube to identify official DHS accounts not currently listed in the Appendix.

Findings: A comparison of the DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue PIA Appendix against the list of official social media sites listed on www.dhs.gov/socialmedia, and a search of Facebook, Twitter, and YouTube identified several official DHS users that were not accounted for in the Appendix. In some cases, the DHS Privacy Office had approved PTAs on file that pre-dated the publication of the DHS-wide social media PIAs but had not added them to the appendix. In other cases, the DHS Privacy Office had not received PTAs for initiatives. On February 15, 2012, the Privacy Office updated the Appendix for the DHS-wide PIA for Social Networking/Interactions/Applications to more fully reflect the scope of DHS users. For official accounts that are active but are still not listed on the appropriate Appendices, both OPA and DHS Privacy are working to have appropriate documentation completed.

Recommendation: Continue efforts to update the Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue Appendix to ensure they reflect the full scope of users.

B. UNIDIRECTIONAL USE OF SOCIAL MEDIA[2]

Collection of Information

Requirements: The Department may utilize unidirectional social media applications for external relations (communications and outreach) and to disseminate timely content to the public about DHS initiatives, public safety, and other official activities. DHS may use these unidirectional applications to inform the public on a range of topics including: 1)

[2] The primary distinction between the Social Media Interactions and Applications PIA and the PIA for Unidirectional use of Social Media PIAs is the level of interaction permitted between the Department and the public. The Interactions and Applications PIA permits, within defined limits, interactions such as allowing the public to comment on its postings, while the Unidirectional PIA permits only a one way dissemination of information without any such interactions.

airport security processing; 2) access to and security at federal buildings; 3) man-made and natural disaster preparedness; 4) transportation security; 5) pandemic outbreaks; 6) border access and security; and 7) other public safety purposes.

DHS programs using unidirectional social media applications are not permitted to actively seek PII.

Review: We reviewed DHS uses listed in the Appendix to the DHS-wide social media PIA for Use of Unidirectional Social Media Applications Communications and Outreach to identify whether content was limited to the purposes noted in the PIA, confirm that the use remained limited to one-way dissemination of information, and identify whether PII was actively sought.

Findings: The DHS official accounts reviewed on these social media platforms remain focused on the purposes of external relations and to disseminate timely content to the public about DHS initiatives, public safety, and other official activities. These initiatives are limited to one-way disseminations of information and none of the official DHS accounts reviewed are actively seeking PII. For example, FEMA has three uses listed in the PIA Appendix that are focused on informing the public about man-made and natural disaster preparedness. These uses are limited to a one-way dissemination of information, and none of the uses involved the active collection of PII.

Notice

Requirements: When using approved unidirectional social media applications for purposes of distributing DHS content DHS shall: 1) establish user names easily identifiable as DHS accounts; and 2) label/tag unidirectional social media applications with an official DHS logo. Additionally, to the extent feasible, the Department will post a privacy notice on the application itself.

Review: We reviewed DHS uses listed in the PIA Appendix to identify if they were appropriately identified as DHS accounts that utilized an official DHS logo and whether appropriate privacy notices were either posted or linked on the application itself (if hosted on a third party platform).

Findings: DHS users identified in the Appendix complied with notice requirements. The one-way dissemination uses listed on the Appendix were largely hosted on ".gov" websites and were easily identifiable as official DHS pages in both the address of the page and the use of official DHS seals.

Scope of Users Reflected in Appendix

Requirements: In order to be covered by the DHS-wide Unidirectional PIA, a component must submit a SMPTA to the DHS Privacy Office for review and approval and addition to the appropriate Appendix.

Review: We compared the DHS-wide Unidirectional PIA Appendix against official social media sites listed on www.dhs.gov/socialmedia.

Findings: The PIA Appendix does not reflect the full listing of users when compared with lists available through www.dhs.gov/socialmedia. For example, there are several DHS Really Simply Syndication (RSS) feeds that are linked to OPA's social media page, but none of these have been identified in the PIA Appendix. Although the PIA accurately describes the use of RSS feeds in the Department, it is unclear whether the PIA process was intended to require SMPTA submissions for items such as RSS feeds.

Recommendation: Clarify when Components should complete a SMPTA for their unidirectional social media applications and update the PIA Appendix. The DHS Privacy Office's Compliance Group may wish to simplify its process for documenting users by linking to www.dhs.gov/socialmedia as a mechanism for identifying some of these initiatives.

V. CONCLUSIONS AND RECOMMENDATIONS

DHS use of social media provides an opportunity to provide the public with robust information through many channels and to further engage the public in accordance with the President's Memorandum on Transparency and Open Government (January 21, 2009)[3] and the Director of the Office of Management and Budget's (OMB) Open Government Directive.[4] As noted in the PIAs, the Department concludes that the public user fully expects privacy protections while interacting with the Department and is mindful about concerns for potential misuse of social media. Recognizing these concerns, DHS established specific requirements through the PIA process on how the Department may engage in social media for communications/outreach/public dialogue purposes in a privacy sensitive way. This privacy compliance review has provided an opportunity to evaluate implementation of these requirements and identify areas for improvement and/or clarification. To strengthen privacy protections for DHS use of social media for communications/outreach purposes, the DHS Privacy Office is making

[3] President Barack Obama, Memorandum on Transparency and Open Government (January 21, 2009), available at http://www.gpoaccess.gov/presdocs/2009/DCPD200900010.pdf

[4] OMB Memorandum M-10-06, *Open Government Directive* (December 8, 2009), available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

five recommendations, including recommendations that it will take the lead on implementing. The DHS Privacy Office recommends that:

1. All DHS official accounts on the Twitter platform periodically "tweet" a link to their agency's privacy policy (e.g., every 2 months) to better inform the public;
2. Account holders for component official channels on YouTube periodically review and update their profiles to ensure privacy policies are stated or linked;
3. The waiver requirement be replaced with guidance on establishing appropriate connections to NGOs and incorporated into the DHS-wide social media PIA. The prohibition of "friending" private citizens remains;
4. DHS official account holders periodically review connections proactively made to NGOs to ensure such connections are appropriately tied to the component's mission; and
5. Efforts continue to update the Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue Appendix to reflect the full scope of users. As for the DHS-wide social media PIA for Use of Unidirectional Social Media Applications for Communications and Outreach, clarify the extent to which Component users should complete a SMPTA and update the PIA Appendix accordingly. The DHS Privacy Office's Compliance Group may wish to simplify its process for documenting users by linking to the www.dhs.gov/social media as a mechanism for identifying some of these initiatives.

VI. PRIVACY COMPLIANCE REVIEW APPROVAL

Responsible Official

Kathleen McShea
Direction of New Media and Web Communications
Office of Public Affairs
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security