Privacy Impact Assessment
for the

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

September 16, 2010

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

Abstract

Social networking interactions and applications includes a sphere of non-government websites and web-based tools that focuses on connecting users, inside and outside of the Department of Homeland Security (DHS or Department), to engage in dialogue, share information and media, and collaborate. Third-parties control and operate these non-governmental websites; however, the Department may use them as alternative channels to provide robust information and engage with the public. The Department may also use these websites to make information and services widely available, while promoting transparency and accountability, as a service for those seeking information about or services from the Department. This Privacy Impact Assessment (PIA) analyzes the Department's use of social networking and how these interactions and applications could result in the Department receiving personally identifiable information (PII). This PIA describes the information the Department may have access to, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information. Appendix A of this PIA will serve as a listing, to be updated periodically, of DHS social networking interactions and applications, approved by the Chief Privacy Officer, that follow the requirements and analytical understanding outlined in this PIA.[1]

The social networking interactions and applications list in Appendix A are subject to Privacy Compliance Reviews by the DHS Privacy Office.

Overview

In accordance with the President's Memorandum on Transparency and Open Government (January 21, 2009)[2] and the Director of the Office of Management and Budget's (OMB) Open Government Directive Memorandum (December 8, 2009),[3] the Department may utilize the opportunity that social networking presents to provide the public with robust information through many channels and to further engage the public. The Department may use certain non-government websites to make information and services widely available to the general public, while promoting transparency and accountability, as a service for those seeking information about or services from the Department.

It is imperative that the Department be transparent about the Department's use of social networking and applications to avoid concerns about unauthorized surveillance of these social networks. The Department must first engage these social networking websites and applications in a manner that protects privacy and respects the intent of users. Under this PIA, the Department is concluding that the public user fully expects privacy protections while interacting with the Department. In order to address these and other concerns, DHS has set forth specific requirements in this PIA on how the Department may engage in social networking including the use of applications in a privacy sensitive way.

---

[1] If a component of the Department has an operational need to use social networking interactions or applications that is outside the scope of the requirements and analytical understanding outlined in this PIA, a separate PIA must be written for that component's use of social networking interactions or applications to address the specific privacy concerns that are unique to that initiative for consideration by the Chief Privacy Officer.

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

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

This PIA analyzes the Department's potential activities on certain social networking websites and web-based applications that make up the range of social networking websites. Generally, social networking websites and applications are privately owned by third parties. These social networking websites and applications continue to grow in size and diversity. Because of the depth and diversity of this reach, the Department is planning for the potential use of a multitude of social networking initiatives.

In considering the different types of social networking websites and applications, DHS identified three general types that it may use, under the auspices of the requirements and analytical understanding outlined in this PIA, where an account is required and thus PII may transit and be displayed by the system during the sign-up/long-on transaction and subsequent interactions:

1) Social media where official DHS users and public users may have an account to use applications tailored to the specific website. This social media includes, but is not limited to, Facebook, MySpace, Ustream, LinkedIn, and GovLoop.

2) Video and Image websites where official DHS users may have an account to post but public users may not be required to have an account to see the video or image. In order for public users to comment, they may need an account. This social media includes, but is not limited to, YouTube, Flickr, Picasa, Blip.tv, and Ustream.

3) Blogs and similar websites where official DHS users may have an account to post but public users may not be required to have an account to see the blog. In order for public users to comment, they may need an account. This includes, but is not limited to, Twitter, Google Blogger, and Wordpress.

Each social networking website and application provides its own privacy policy, and while users are typically required to submit some PII during the registration process, the Department will not solicit or collect this PII. In advance of utilizing a social networking website or application, the Department will examine the social networking website or application privacy policy to evaluate the risks to determine whether the website is appropriate for the Department's use. Additionally, to the extent feasible, the Department will post a Privacy Notice on the social networking website or application website itself.[4] If an agency posts a link that leads to a social networking or application website, the agency will provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of the agency's official website. If PII is posted on a social networking or applications site or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per the appropriate records retention policies. The Department will only collect the information necessary for the proper performance of official Departmental functions.

Additionally, official DHS accounts across social networking websites and applications will be identified by the component or Department seal as well as an anonymous, easily identifiable user name account displaying a DHS presence, such as "DHS John Q. Employee."

[4] OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.

Unless otherwise directed by statute, executive order, or regulation the Department's public affairs officials will serve as the primary account holders for all social networking websites and applications across the Department and will manage and approve all DHS content posted on these public-facing networks. All content disseminated through official Department accounts must be approved by the Department's public affairs officials prior to posting.[5] The Department's public affairs officials will ensure that all posted content falls within the appropriate requirements for publicly available information and materials. OPA will, when necessary, act as the final authority on what content is acceptable for posting.

When DHS uses those social networking websites and applications listed in Appendix A, it shall not: 1) actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements and analytical understanding outlined in this PIA); 2) search social networking websites or applications for or by PII; and 3) "friend"[6] public users proactively; exclusion is made to "friending" 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 NGOs, may submit a waiver from this requirement to the DHS Privacy Office at pia@dhs.gov. Such waivers will be noted in the Appendix A under the applicable program.

When DHS uses those social networking websites and applications listed in Appendix A, it may: 1) establish user names and passwords to form profiles, so long as they are easily identifiable as DHS accounts; 2) accept "friend" requests from public user accounts; and 3) interact on social networking websites or applications on official Department business.

The three categories outlined above make up the Department's use of social networking websites and applications covered under this PIA and are intended for external relations (communications/outreach/public dialogue), to provide information about or from the Department, and to provide customer service. This PIA, for example, is not intended to cover other social media activity such as monitoring initiatives, law enforcement and intelligence activities, and other similar operations. For more information on the Department's use of social media, visit www.dhs.gov/privacy.

[5] The Secretary's Efficiency Review, Section III, Office of Public Affairs Cross-Component Coordination Task Force Directive *available at* http://dhsconnect.dhs.gov/policies/Efficiency Review Materials/90_ER_-_DHS_Communications_-final_guidance_intranet.pdf.

[6] Friending in this PIA is defined as linking, connecting, fanning, following individuals with whom the Department or the public would like to remain closely in contact with, as a defined audience, which is distinct from the public at large. This privilege is controlled by the user.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The President's Transparency and Open Government Memorandum[7] (January 21, 2009) and the OMB Director's Open Government Directive Memorandum[8] (December 8, 2009) direct federal departments and agencies to harness new technologies to engage the public and serve as one of the primary authorities motivating the Department's efforts to utilize social networking websites and applications.

The Secretary of Homeland Security's Efficiency Review,[9] Section III, Office of Public Affairs Cross-Component Coordination Task Force Directive requires all Departmental social networking websites and applications to be coordinated with OPA, unless otherwise directed by statute, executive order, or regulation.

When DHS uses those social networking websites and applications listed in Appendix A, it is not permitted to actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements and analytical understanding outlined in this PIA). As a requirement of this PIA, PII may not be retrieved by personal identifier, outside the scope of previously published Privacy Act System of Records Notices, thus, a Privacy Act System of Records Notice is not required.

Authorities supporting the Department's use of social networking websites and applications include:

A. 6 U.S.C. § 112, "Secretary; functions;"

B. 6 U.S.C. § 142, "Privacy Officer;"

C. 5 U.S.C. § 301, the Federal Records Act;

D. 5 U.S.C. § 552a, the Privacy Act of 1974;

E. Section 208 of the E-Government Act of 2002;

F. Section 222 of the Homeland Security Act of 2002;

---

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

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

[9] The Secretary's Efficiency Review, Section III, Office of Public Affairs Cross-Component Coordination Task Force Directive *available at* http://dhsconnect.dhs.gov/policies/Efficiency Review Materials/90_ER_-_DHS_Communications_-final_guidance_intranet.pdf.

G. The President's *Memorandum on Transparency and Open Government*, January 21, 2009;

H. The OMB Director's *Open Government Directive* Memorandum, December 8, 2009;

I. OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010;[10]

J. OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, April 7, 2010;[11]

K. The Secretary's Efficiency Review, Section III, Office of Public Affairs Cross-Component Coordination Task Force Directive;

As a result of this new technological relationship between the Department and the public, it is imperative that DHS engage the public in a manner that complies with federal accessibility, privacy, information security and records laws. To ensure that the Department's use of social media complies with federal laws, executive orders, regulations, and policies, and to apply standards consistently across the entire Department, the Office of the General Counsel (OGC), Office for Civil Rights and Civil Liberties (CRCL), Privacy Office (PRIV), Office of Public Affairs (OPA), Chief Information Security Office (CISO), and Office of Records Management (Records) will collaborate to ensure that all documents related to social media are cleared to ensure that compliance issues are considered and coordinated before implementation.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

As a requirement of this PIA, PII may not be retrieved by personal identifier, outside the scope of previously published Privacy Act System of Records Notices. Components may input information into the Departments systems of records that is relevant to official Department duties and for purposes previously approved and outlined in SORNs published in the Federal Register. For example, if a public user contacted the Department to obtain records, the Department would maintain that information under DHS/ALL-001 Department of Homeland Security Freedom of Information Act (FIOA) and Privacy Act (PA) Record System (October 28, 2009, 74 FR 25938). Or if a public user asks the Department to contact them regarding a public relations matter, the Department would maintain that information under DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System (November 25, 2008, 73 FR 71659).

[10] OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.
[11] OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (*April 7, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Social networking websites and applications are external and third-party hosted. Therefore, no internal system security plan is currently required. Users should also consult the website security policies of social networking websites and applications they subscribe to for more information as they apply.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The Department's Office of Records Management, Office of General Counsel, and other components are working internally, as well as with NARA, to determine the records schedule. Until the records schedule is approved, records are maintained indefinitely. Once approved, the Department will follow that approved records schedule.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Whether or not the Department's use of social networking websites and applications triggers the PRA is circumstantial. [12]

Certain uses of social networking websites and applications will be exempt from the PRA. For example, the Department may use web-based technologies, such as blogs, wikis, and social networks, as a means of publishing solicitations for public comment and for conducting virtual public meetings. Items collected by social networking websites and applications that are not collecting information on behalf of the federal government are not subject to the PRA. Additionally, if the Department authorizes website users to share contact information, such as "send to a friend" using a web form, this authorization is not covered by the PRA unless the agency collects additional information from the "friend."

However, if the Departments uses social networking websites and applications to post surveys of any kind, including web polls and satisfaction surveys that pose identical, specific questions, including pop-up windows, the PRA may apply. Requesting information from respondents' beyond name and email or mailing address would

[12] OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (*April 7, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf.

implicate the PRA and require OMB approval because it seeks information beyond what is "necessary" for self-identification of the respondent.

The PRA applies whether the obligation to respond to a collection of information is mandatory, voluntary, or required to obtain a benefit.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Under this PIA, the Department may utilize social networking websites and applications for external relations (communications/outreach/public dialogue), to provide information about or from the Department, and to provide customer service. The Department uses these non-government websites to make information and services widely available, while promoting transparency and accountability. DHS may use these websites to inform the public on a range of topics from information on airport security to preparedness measures in the event of a hurricane. A public user's information will only be viewed by the Department when the user posts on DHS social networking websites or applications.

Those DHS programs using the social networking websites and applications listed in Appendix A are not permitted to actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, regulation, or executive order (all other PII received will be managed in accordance with the requirements and analytical understanding outlined in this PIA). Many social networking websites and applications request PII at the time of registration. This collection will vary. Frequently users can provide optional information in addition to the required registration information. For example, users can include optional information on: interests, birthday, religious and political views, family members and relationship status, education and work, photos, alias, contact information (phone, email, address), and hometown to name a few. The Department does not automatically have access to, and will not seek, the public's registration information unless the information used during registration pre-populates a public profile when interacting with a user, if the users' privacy settings allow this display. If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies. Through use of social networking websites and applications, DHS users and public users may have an account and, by nature of the program, PII may transit and be displayed by the system during the sign-up/long-on transaction and subsequent interactions.

Through use of videos, images, and blogs, DHS users may have an account to post information but public users need not need to have an account to see or participate in the video, image, or blog. By registering, users have the ability to post information such as comments, pictures, videos, and external links. If public users comment, and the social networking website or application requires an account, PII, by nature of the program, may transit and be displayed by the system during the sign-up/long-on transaction and subsequent interactions. The Department has the same information access, abilities, and restrictions as any public user.

Department users, acting in their official capacity, may accept "friend"[13] requests from public user accounts for external relations (communications/outreach/public dialogue), to provide information about or from the Department, and to provide customer service. The Department uses these non-government websites to make information and services widely available, while promoting transparency and accountability. The Department shall not "friend" public users proactively; exclusion is made to "friending" 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 NGOs may submit a waiver from this requirement to the DHS Privacy Office at pia@dhs.gov. Such waivers will be noted in the Appendix A under the applicable program. Practices such as "friending" may allow Department employees access to information that public account users designate as available only for their network (i.e., "friends") to see.

2.2 What are the sources of the information and how is the information collected for the project?

Social networking website and application users may be required to submit PII to the social networking website or application service at the time of registration. As noted above, users may voluntarily submit additional optional information to further identify or categorize themselves if they so choose. This may also happen during social networking sessions with the Department. If the Department accepts a friend request from a public user, additional information is viewable by the Department that users have designated for their network to see. This information is collected and maintained by the social networking website or application service provider, but may be viewed by the Department. The Department may view user comments in instances of bi-directional communication between a DHS user and another public user. If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies. The use of a social networking website or application to conduct communications and transactions on behalf of the Department does not preclude the Department's responsibility for potentially managing it as a federal record.

[13] See footnote 6.

When DHS uses those social networking websites and applications listed in Appendix A, it is not permitted to actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements in this PIA). DHS will not actively "friend" a public user (exclusion is made to "friending" other U.S. federal, state, local, and tribal government agencies) but may accept invitations to be "friended" by public users. If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Social networking websites and applications permit users to "add value" to the network by voluntarily submitting information about themselves that is then stored by the service. These social networking websites and applications compile the information into "profiles," often searchable in various fields that allow users to interact with others on a web-based platform provided by the host. Social networking websites and applications may, among other uses, also employ user-defined data to advertise products.

2.4 Discuss how accuracy of the data is ensured.

Information posted by public users on a social networking website or application is submitted voluntarily. The public user controls accuracy of the information. The Department does not make assumptions about informational accuracy nor will it verify its accuracy. However, the Department may correct inaccurate information about the Department's programs that are posted on publicly available pages.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Risk: There is a risk that Department users, acting in their official capacity, may "friend" public users without the public users being aware of it. This could lead public users to believe the Department is inappropriately engaging with the public.

Mitigation: To mitigate this risk, the Department has established requirements in this PIA that no Department user, acting in his/her official capacity, may actively "friend" a public user; exclusion is made to "friending" 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 NGOs may submit a waiver from this requirement to the DHS Privacy Office at pia@dhs.gov. Such waivers will be

noted in the Appendix A under the applicable program. Department users may only accept requests from the public to be "friended."

Risk: Given the nature of social networking websites and applications, PII may transit and be displayed by the system during the sign-up/long-on transaction and subsequent interactions. All interactions may expose Department users to PII and that information may be inappropriately incorporated into Departmental files. In instances where bi-directional communication with the Department (chat/comment) is initiated by a public user, those remarks may be collected by the Department. If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies. Another risk is that public users may post inappropriate content on DHS-sponsored pages.

Mitigation: To mitigate this risk, the Department recommends public users not post PII on a social networking website or application or share it with the Department. In instances where bi-directional communication (chat/comment) is initiated by a public user, those remarks may be collected by the Department.[14] Additionally, if inappropriate comments (vulgar/profanity) are posted on DHS-sponsored pages the Department may first attempt to remove it from the page, but it may remain a federal record in Departmental files in accordance with moderation and use policies.

Risk: Public users may post specific information, including PII, to DHS asking about why a particular benefit has or has not been provided.

Mitigation: DHS will post a notice on all social networking websites and applications stating that if PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies. The use of a social networking website or application to conduct communications and transactions on behalf of the Department does not preclude the Department's responsibility for potentially managing it as a federal record.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The Department may utilize certain social networking websites and applications for external relations (communications/outreach/public dialogue), to provide information about or from the Department, and to provide customer service. The Department uses these non-government websites to make information and services widely available, while promoting transparency and accountability. The social networking website or

[14] The Office of Public Affairs, in coordination with OGC, will facilitate development of moderation/comment policies along with the Department's components.

application, and the user information that resides within it, will be used in order to facilitate interaction with the public. When DHS uses those social networking websites and applications listed in Appendix A, it is not permitted to actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements in this PIA). If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies. The use of a social networking website or application to conduct communications and transactions on behalf of the Department does not preclude the Department's responsibility for potentially managing it as a federal record.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The Department will not dictate what applications will be used by various social networking websites and applications to analyze data that users voluntarily submit. The Department will not produce data except, potentially, in instances where bi-directional communication occurs. In these instances, basic identifiers such as name or pseudonym, time stamp, and communication of the exchange may be recorded.

3.3 Are there other components with assigned roles and responsibilities within the system?

Information may be shared internally within DHS to those who demonstrate a need-to-know in the performance of their official duties. This may involve public user-posted comments shared with appropriate officials in order to improve the way the Department uses social networking websites or applications and for external relations (communications/outreach/public dialogue), to provide information about or from the Department, and to provide customer service. The Department uses these non-government websites to make information and services widely available, while promoting transparency and accountability. PII should only be shared internally where the information received was for a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements in this PIA).

3.4 Privacy Impact Analysis: Related to the Uses of Information

Risk: PII posted on a social networking website or applications or sent to the Department in connection with the transaction of public business may become a federal

record and, if so, the Department is required to maintain a copy per its records retention policies.

Mitigation: To mitigate the risk, users should not post or send PII to the Department. Users should limit use of PII to that which is absolutely necessary.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The Department shall set-up official accounts which clearly establish that the accounts are managed by DHS. For example, the Department shall use the DHS seal on the social networking websites or applications. In addition, employees responsible for managing such websites or applications should clearly identify themselves, such as "DHS John Q. Employee," when interacting with the public. The Department's public affairs officials are content approvers for the Department.

If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies.

In advance of utilizing a social networking website or application, the Department will examine the privacy policy of the social networking website or application to evaluate the risks to determine whether it is appropriate for the Department's use. Additionally, to the extent feasible, the Department will post a Privacy Notice on the social networking website or application itself. If an agency posts a link that leads to a social networking or application website, the agency will provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of the agency's official website. Users should also consult the privacy policies of social networking websites and applications they subscribe to for more information as they apply. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

In advance of utilizing a social networking website or application, the Department will examine the website's or application's privacy policy to evaluate the

risks and to determine whether the it is appropriate for the Department's use. Additionally, to the extent feasible, the Department will post a Privacy Notice on the social networking website or application itself. If an agency posts a link that leads to a social networking or application website, the agency will provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of the agency's official website. Users should also consult the privacy policies of social networking websites and applications they subscribe to for more information as they apply. Many social networking websites and applications provide privacy controls that allow users to adopt a "layered" approach to others' access to their profile information. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

The Department does not ask individuals to post information on social networking websites or applications. Information that individuals voluntarily submit as part of the registration process is not the property of DHS and the Department will not solicit this information. PII posted on a social networking website or application or sent to the Department in connection with the transaction of public business, may become a federal record and if so the Department is required to maintain a copy.

As the information collected by the social networking website or application is submitted voluntarily by individuals, the Department cannot provide an opportunity to decline to provide information. With regard to the rights users may have on the social networking website or application, individuals should consult the privacy policies of the websites they subscribe to for more information.

4.3 Privacy Impact Analysis: Related to Notice

The Department shall set-up official accounts which clearly establish that the accounts are managed by DHS. For example, the Department shall use the DHS seal on the social networking websites or applications. In addition, employees responsible for managing such websites or applications should clearly identify themselves, such as "DHS John Q. Employee," when interacting with the public. The Department's public affairs officials are content approvers for the Department.

In advance of utilizing a social networking website or application, the Department will examine the privacy policy to evaluate the risks to determine whether it is appropriate for the Department's use. Additionally, to the extent feasible, the Department will post a Privacy Notice on the social networking website or application itself. Users should also consult the privacy policies of social networking website or application they subscribe to for more information as they apply. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Those social networking websites and applications listed in Appendix A are not permitted to actively seek PII, and may only use the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation (all other PII received will be managed in accordance with the requirements and analytical understanding outlined in this PIA). If PII is posted on a social networking website or application or sent to the Department in connection with the transaction of public business, it may become a federal record and if so the Department is required to maintain a copy per its records retention policies.

The Department's Office of Records Management, Office of General Counsel, and other components are working internally, as well as with the National Archives and Records Administration, to determine the records schedule. Until the records schedule is approved, records are maintained indefinitely. Once approved, the Department will follow that approved records schedule.

Records may also be maintained by the social networking website or application. Check specific social networking websites and applications for details on records retention.

5.2 Privacy Impact Analysis: Related to Retention

Risk: Retaining information for longer than is relevant and necessary can introduce privacy risks such as unauthorized use and disclosure.

Mitigation: To mitigate this risk, the Department will only maintain information posted on the social networking website or application sent to the Department in connection with the transaction of public business. The Department's Office of Records Management, Office of General Counsel, and other components are working internally, as well as with the National Archives and Records Administration, to determine the records schedule. Once approved, the Department will follow that approved records schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The information posted on social networking websites and applications will be available to the provider and any and all users on a social networking website or application who are able to access the public-facing side of an account. The Department may share information posted on a DHS-sponsored page if there is a demonstrated need to know, and will only post information after it has been appropriately approved and vetted by the Department's public affairs officials.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Department employees may share only as much information as necessary in the performance of official Department duties with those who have a need-to-know inside the Department. The Department's employees and contractors will be trained on the appropriate use and sharing of social networking information.

6.3 Does the project place limitations on re-dissemination?

Department employees may re-distribute only as much information as necessary in the performance of official Department duties with those who have a need-to-know inside the Department. The Department's employees and contractors will be trained on the appropriate use and sharing of social networking information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Content posted on the Department's social networking websites and applications is publicly available therefore it will be accessible to anyone with an internet connection. Information may also be shared by other electronic means and in paper form. In doing so, the Department's policies and procedures for handling information remain in place.[15] The Department's public affairs officials are content approvers for the Department. This includes sharing of information outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

Risk: Sharing too much information, particularly bi-directional communication records is a risk inherent in this process.

Mitigation: Department employees share only as much information as necessary in the performance of official Department duties with those who have a need-to-know.

[15] *Available at* http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf.

The Department's employees and contractors will be trained on the appropriate use and sharing of social networking information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

As a general matter, the Department is not collecting information on individuals and so there is no information that an individual could access. Nevertheless, the Department's public affairs officials will post their contact information on the social networking website or application to allow any individual to contact the Department regarding any information posted. Individuals should also consult the privacy policies of the social networking website or application they subscribe to for more information related to those social networking sites and applications own access provisions.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As noted above, the Department is not collecting information about an individual and so will generally not have a record that needs to be corrected. In most instances the individual is able to correct information on the social networking or application website directly. The Department's public affairs officials will post its contact information on the website or application to allow any individual to contact the Department regarding any information posted. Individuals should also consult the privacy policies of the websites they subscribe to for more information related to those social networking sites and applications own access provisions. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

7.3 How does the project notify individuals about the procedures for correcting their information?

As noted above, the Department is not collecting information about an individual and so will generally not have a record that needs to be corrected. In most instances the individual is able to correct information on the social networking or application website directly. The Department's public affairs officials will post their contact information on the website or applications to allow any individual to contact the Department regarding any information posted. Individuals should also consult the privacy policies of the websites they subscribe to for more information related to those social networking sites

and applications own access provisions. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

7.4 Privacy Impact Analysis: Related to Redress

As designed under this PIA, the Department will not be collecting PII. In most instances the social networking or application website is designed so that the individual has direct control over his/her information and can make any corrections required. Nevertheless, the Department's public affairs officials will post their contact information on the website or applications to allow any individual to contact the Department regarding any information posted. This contact information, in most cases, will be in the form of standard email and physical mailing addresses. The information available on social networking websites and applications is largely user-generated, meaning the individual chooses the amount of information available about himself or herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should be able to redress any concerns through the social networking website or application. Individuals should also consult the privacy policies of the social networking websites and applications they subscribe to for more information related to those social networking sites and applications own access provisions. The Department's privacy policy can be viewed at http://www.dhs.gov/xutil/gc_1157139158971.shtm.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The social networking websites and applications listed in Appendix A are subject to Privacy Compliance Reviews by the DHS Privacy Office.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

The Department's federal employees and contractors are provided annual privacy training. Content approvers and posters are provided additional training by the Department's public affairs officials.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The Department does not own or control social networking websites and applications, and accesses them only as a user. However, passwords for Department

accounts will be controlled by the Department's public affairs officials and will ensure that only authorized individuals have access to the accounts. The Department must set-up an official account which clearly establishes that the account is managed by DHS. For example, components should use the DHS seal on the social networking website or application. In addition, employees responsible for managing such websites and applications should clearly identify themselves, such as "DHS John Q. Employee," when interacting with the public.

As part of their official contractual duties, when supervised by a federal employee, contractors may provide support for to the Department's social networking websites and applications.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

As a result of this new technological relationship between the Department and the public, it is imperative that DHS engage the public in a manner that complies with federal accessibility, privacy, information security and records laws. To ensure that the Department's use of social media complies with federal laws, executive orders, regulations, and policies, and to apply standards consistently across the entire Department, OGC, CRCL, PRIV, OPA, CISO, and Records will collaborate to ensure that all documents related to social networking websites and applications are cleared to ensure compliance issues are considered and coordinated before implementation.

Appendix A of this PIA will serve as a listing, to be updated periodically, of DHS social networking interactions and applications, approved by the Chief Privacy Officer, that follow the requirements and analytical understanding outlined in this PIA

Responsible Officials

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

Approval Signature

Final signed version on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Social networking interactions and applications covered by this PIA include: