The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement[1]:

a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications);

b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

[1] Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review:

July 11, 2017

Name of Component:

United States Secret Service

Contact Information:

(b)(6) **Protective Intelligence & Assessment Division**

Counsel[2] Contact Information:

Chief Counsel (b)(6) **Office of the Chief Counsel**

(b)(6)

IT System(s) where social media data is stored:

Protective Threat Management System (PTMS)

Applicable Privacy Impact Assessment(s) (PIA):

DHS/USSS/PIA-003 Protective Threat Management System (PTMS)

Applicable System of Records Notice(s) (SORN):

DHS/USSS-004 Protection Information System

[2] Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. **Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.**

   The Secret Service, as part of its protective intelligence mission and certain protective operations, searches open source social media content for information related to the identification of threats to Secret Service protectees, as well as to identify events potentially disruptive to Secret Service protected facilities and venues. These searches are conducted using a base set of key terms and incorporate protectee schedules in order to more narrowly tailor the results for situational awareness.

2. **Based on the operational use of social media listed above, please provide the appropriate authorities.**

   The collection of social media information is authorized by 18 USC §§ 3056, Powers, authorities, and duties of United States Secret Service.

   a) **Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?**

      X Yes. ☐ No.

3. **Is this use of social media in development or operational?**

   ☐ In development. X Operational. Date first launched: 2010

4. **Please attach a copy of the Rules of Behavior that outline the requirements below.**

   A copy of the Rules of Behavior that outline the requirements below are attached.

5. **Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:**

   a) *Equipment*. Use only government-issued equipment when engaging in the operational use of social media;

      X Yes. ☐ No. If not, please explain:

   b) *Email and accounts*. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

☐ Yes. X No. If not, please explain:

This rule is followed in all situations except those where the use of an official government affiliation/email address would impede or prevent the performance of the operational purpose. In order to access certain social media sites for undercover operations, for example, it may be necessary for the Secret Service to establish non-DHS accounts in order to gain access to publically available content. The purpose of the non-DHS account is for access only and not for interaction with individuals.

c) *Public interaction*. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

X Yes. ☐ No. If not, please explain:

d) *Privacy settings*. Respect individuals' privacy settings and access only information that is publicly available;

X Yes. ☐ No. If not, please explain:

e) *PII collection*: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

X Yes. ☐ No. If not, please explain:

f) *PII safeguards*. Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

X Yes. ☐ No. If not, please explain:

g) *Documentation*. Document operational use of social media, including date, site(s) accessed, information collected and how it was used in the same manner as the component would document information collected from any source in the normal course of business.

☐ Yes. X No. If not, please explain:

The use of social media in protective intelligence investigations is documented in incident reports and/or investigative reporting and may be entered into PTMS. In certain instances, the operational use of social media may be only informational in nature for situational awareness and may not be formally documented.

h) *Training*. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials

provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

X Yes. ☐ No. If not, please explain:

Users will complete annual privacy training on the acceptable operational uses of social media. Mechanisms are (or will be) in place to verify that users have completed training.

X Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

X Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 11/1/17

NAME of the DHS Privacy Office Reviewer: (b)(6)

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ Covered by existing PIA. DHS/USSS/PIA-003 Protective Threat Management System (PTMS)

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☒ Covered by existing SORN. DHS/USSS-004 Protection Information System, October 28, 2011, 76 FR 66940

☐ New.

☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

PRIV determines that USSS Privacy has provided sufficient documentation to demonstrate compliance with MD 110-01. The searches conducted by USSS are using a base set of key terms and incorporate protectee schedules in order to more narrowly

tailor the results for situational awareness. The Rule of Behavior from 2012 provides for an exception to use DHS affiliated email addresses for "operational necessity" and in the case of certain undercover communications when in accordance with DOJ 1999 Online Investigative Principles for FLEA and USSS guidelines for evaluation of undercover operations. The Operational Use of Social Media is circulated annually to all USSS employees and further all employees using Social Media operationally are required to provide annual recertification.

While PRIV notes that USSS Privacy has met the minimum standard to comply with the Instruction MD 110-01, PRIV recommends USSS Privacy implement a mechanism to confirm recipients (USSS employees) of the official message have read and understand the requirements for the Operational Use of Social Media and Rules of Behavior. One suggested recommendation is to use the voting buttons in Microsoft Outlook. Recipients receive an email asking for a response to the statement "I read, understand, and will comply with the notice."