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: October 11, 2017

Name of Component: National Protection and Programs Directorate, Federal Protective Service

Contact Information: (b)(6); (b)(7)(C) **Division Director, Protective Intelligence & Investigations;** (b)(6); (b)(7)(C)

Counsel[2] Contact Information: (b)(6); (b)(7)(C)

IT System(s) where social media data is stored: FPS Web Records Management System (WebRMS) will store social media data. At the time in which the FPS Law Enforcement Information Management System (LEIMS) becomes operational and replaces WebRMS, LEIMS will then become the system in which social media data is stored.

Applicable Privacy Impact Assessment(s) (PIA): ***Federal Protective Service Dispatch and Incident Record Management Systems*** **DHS/NPPD/FPS/PIA-010(c)**

Applicable System of Records Notice(s) (SORN): DHS/All 025 – Law Enforcement Authorities in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records (75 FR 5614, published February 3, 2010).

[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 Federal Protective Service (FPS) is an operational component within the National Protection and Programs Directorate (NPPD) that provides law enforcement and security services to approximately 9,000 federal facilities and persons thereon nationwide. FPS may also be directed by the Secretary of Homeland Security to perform other law enforcement duties necessary for the promotion of Homeland Security pertaining to the protection of Federal property and persons on the property. In accordance with Homeland Security Presidential Directive 7 (HSPD-7) and specified in the National Infrastructure Protection Plan, FPS is the Federal sector specific agency for government facilities and is responsible for collaborating with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conducting or facilitating vulnerability assessments of the sector; and encouraging risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. The FPS mission includes law enforcement activities for the purpose of rendering federal properties safe and secure for federal employees, officials, and visitors in a professional and cost effective manner. FPS Law Enforcement personnel may collect personally identifiable information from social media sources for the law enforcement activities of (1) criminal investigations and (2) law enforcement activities in carrying out its statutory mission.

(1) During the course of criminal investigations for violations of Federal and appropriate state law, FPS law enforcement personnel may use both government attributable and non-government attributable computers and other access tools in collecting personally identifiable information from social media sources. FPS law enforcement personnel will only use non-attributable computers and other access tools such as High Assurance Gateway tool, Anonymizer, Chameleon, and/or other non-attribution service or DHS standalone computer terminals upon establishment of a criminal predicate leading to the opening of a criminal investigation and pursuant to Federal law and FPS/DHS policies and guidelines relating to undercover criminal investigations.

(2) During the course of law enforcement intelligence activities for violations of Federal law and protection of Federal facilities and persons on the facilities, FPS law enforcement personnel may use both government attributable and non-government attributable computers and other access tools in collecting personally identifiable information from social media sources. FPS law enforcement personnel will only use non-attributable computers and other access tools such as High Assurance Gateway tool, Anonymizer, Chameleon, and/or other non-attribution service or DHS standalone computer terminals upon establishment that the information being collected is for the purpose of evaluation to determine if it is relevant to the identification of an individual who, or organization which, is reasonably suspected of involvement in criminal activity and the criminal activity in which it is involved, and pursuant to Federal law and FPS/ DHS policies and guidelines relating to undercover criminal investigations.

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

Section 1706 of the Homeland Security Act of 2002, codified at 40 U.S.C. § 1315, *Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property.*

Office of the Attorney General, *Guidelines For The Exercise Of Law Enforcement Authorities By Officers and Agents Of the Department Of Homeland Security Under 40 U.S.C. § 1315*, dated March 1, 2005.

DHS Delegation 17001, Rev. 01, *Delegation To The Under Secretary For National Protection and Programs*, dated October 25, 2013.

NPPD Delegation 17001.101, *Delegation To The Director For The Federal Protective Service*, dated May 10, 2016.

Secretary of Homeland Security Memorandum, *Acquisition of Security Guard Services*, dated July 2, 2007.

DHS Assistant Secretary for Policy Memorandum, *Use of Public and Non-Public Information for Law Enforcement, Situational Awareness, and Intelligence Purposes* dated September 15, 2010, whereby DHS adopts the DOJ 1999 guidelines *Online Investigative Principles For Federal Law Enforcement Agents.*

5 U.S.C. § 552a, Privacy Act 0f 1974, specific to section 5 U.S.C. §552a (e)(7) exemption for law enforcement activities.

Homeland Security Presidential Directive – 7, *Critical Infrastructure Identification, Prioritization, and Protection.*

Title 28, C.F.R. Part 23, *Guidelines for Criminal Intelligence Records Systems.*

Title 41 C.F.R. §102-74.15, requires occupants of facilities under the custody and control of Federal agencies to promptly report all crimes and suspicious circumstances occurring on federally controlled property first to the regional FPS.

Title 41, C.F.R. §102-85.35, requires FPS to provide general law enforcement to on GSA controlled property.

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?

☒ Yes. ☐ No.

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

☐ In development. ☒ Operational. Date first launched: November 2012

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

Please see 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;

☐ Yes. ☒ No.

If not, please explain: If not, please explain: FPS will, in most cases, use government attributable equipment when collecting personally identifiable information from social media sources. FPS, may, however, use non-government attributable equipment as such as the High Assurance Gateway tool, Anonymizer, Chameleon, and/or other non-attribution services offered through DHS for purposes of law enforcement investigative and intelligence activities. In some instances, FPS will use standalone computer terminals, which although are purchased using DHS funds, are not formally issued by the Department. FPS will use DHS issued aircards for connecting to the internet in remote locations. The purpose of using standalone computer terminals and aircards is so that FPS law enforcement personnel can access internet and social media sites that are normally blocked on the DHS/ICE network or government non-attribution is required for either a criminal investigation or law enforcement intelligence.

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. ☒ No. If not, please explain:

FPS law enforcement personnel will utilize covert/non-attributable screen names and email accounts in accordance with the specific use requirements as described in Question 1 above.

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

☐ Yes. ☒ No. If not, please explain:

FPS will interact with individuals who posted information on the internet in accordance with Federal law and FPS/ DHS policies and guidelines relating to criminal investigations and law enforcement intelligence' use of social media.

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

☐ Yes. ☒ No. If not, please explain:

FPS will, in most cases, only access publicly available information. However, in accordance with FPS' law enforcement authority, FPS law enforcement personnel may access information that is not publicly available to further criminal investigations and law enforcement intelligence activities as described in Question 1 above.

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;

☐ Yes. ☒ No. If not, please explain:

FPS will, in most cases, only access publicly available information. However, in accordance with FPS' law enforcement authority, FPS law enforcement personnel may access information that is not publicly available to further criminal investigations and law enforcement intelligence activities as described in Question 1 above.

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

☒ 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. ☐ No. If not, please explain:

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.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

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

☒ 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: (b)(6)

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/NPPD/FPS/PIA-010(c) Federal Protective Service Dispatch and Incident Record Management Systems
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☒ A SORN is required:
  - ☒ Covered by existing SORN. DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, June 14, 2017, 82 FR 27274
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

PRIV determines that NPPD/FPS has provided sufficient documentation to demonstrate compliance with the MD 110-01.

PRIV agrees with NPPD Privacy that PIA and SORN coverage is required and is provided by the FPS DIRMS PIA and Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the DHS SORN. DHS/NPPD/FPS/PIA-010(c) discusses the addition of LEIMS to allow FPS investigators and inspectors to document specific details and the outcome of all cases. DHS/ALL-025 covers all of FPS activities.

As part of this determination, PRIV requires that NPPD Privacy submit a PTA to discuss FPS law enforcement personnel use of the access tool, Chameleon, for the purpose of evaluation to determine if it is relevant to the identification of an individual who, or organization which, is reasonably suspected of involvement in criminal activity and the criminal activity in which it is involved, and pursuant to Federal law and FPS/ DHS policies and guidelines relating to undercover criminal investigations.