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: 08/24/2017

Name of Component: National Protection and Programs Directorate (NPPD)

Contact Information: Anthony Militano, anthony.militano@hq.dhs.gov, 703-235-8929

Counsel[2] Contact Information: Matthew Slowik, Matthew.Slowik@hq.dhs.gov, 703-235-9441

IT System(s) where social media data is stored: Social Media Data will not be stored in an IT System. The NPPD Office of Cyber and Infrastructure Analysis (OCIA) will only use social media in an effort to enhance situational awareness. Some information may be used in assessments supporting NPPD watch operations.

Applicable Privacy Impact Assessment(s) (PIA): N/A

Applicable System of Records Notice(s) (SORN): N/A

[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 National Protection and Programs Directorate (NPPD) Office of Cyber and Infrastructure Analysis (OCIA) develops and uses analytic capabilities to inform decisions by DHS, and public- and private-sector partners to improve the security and resilience of infrastructure and understand their interdependencies. OCIA analysis helps NPPD frame policy and programs, prioritize its operational activities and maximize operational effectiveness through more efficient use of resources. In addition, OCIA also manages the Integrated Analysis Cell (IAC), established in PPD-21, Critical Infrastructure Security and Resilience, which serves at the intersection of NPPD's two operational centers, the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC)

   OCIA wishes to use social media data from Facebook, Instagram, and Twitter to maintain real-time situational awareness and track official company statements as they relate to crisis response. At no time will OCIA personnel post statements on behalf of NPPD or DHS to social media platforms. Any information obtained from social media sites used in OCIA assessments would be prefaced with a comment identifying the source as open-source media and/or social media.

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

   Title II, Section 201(d) of the Homeland Security Act, 6 U.S.C. § 121, provides the Secretary with authority *to access*, receive, and analyze law enforcement information and *other information from* agencies of the Federal government, state, local, tribal, and territorial government agencies (including law enforcement agencies), and *private sector entities, and to integrate such information in order to identify and assess the nature and scope of terrorist threats to the homeland*, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland. These statutory authorities were delegated down to NPPD in DHS Delegation 17001.

   Further, Presidential Policy Directive 21 declared implementation of an Integration and Analysis Function as a strategic imperative for DHS, which led to OCIA establishing and

leading the IAC. The IAC provides the NICC and the NCCIC with near real-time consequence analysis that leverages and includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure. Access to social media for situational awareness purposes directly enables the Department's statutory mission and PPD-21's direction, as critical information about an on-going event or incident relevant to NPPD's analytical functions can in some cases be derived from and furthered by social media data.

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:

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

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:

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:

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:

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

☒ 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;

☒ Yes. ☐ No. If not, please explain:

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: 10/18/17

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. <Please include the name and number of PIA here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☐ A SORN is required:
  - ☐ Covered by existing SORN. <Please include the name and number of SORN here.>
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

OCIA IAC will review corporate social media feeds/postings and other open source content. In certain circumstances, OCIA will rely on that open source information

along with information from social media posts (Neither will include PII) to develop an assessment. OCIA IAC would then send the assessment to the DHS/NPPD/Office of Infrastructure Protection/National Infrastructure Coordinating Center (NICC) in the body of an email for inclusion in their situational reporting. The social media will not be otherwise stored and any information that is collected as part of the assessments sent to the NICC would not retrievable by personal identifiers since PII will not be collected. PRIV finds that no PIA or SORN is required because oo PII will be collected.