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: April 3, 2018

Name of Component: National Protection and Programs Directorate

Contact Information: (b)(6)

Counsel[2] Contact Information: (b)(6)

IT System(s) where social media data is stored: Social media data is not expected to be stored, as the National Infrastructure Coordinating Center (NICC) will only use social media to enhance situational awareness.

Applicable Privacy Impact Assessment(s) (PIA): PIA is not required because PII will not be collected.

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.**

Operational Use of Social Media Proposal:

Within the National Protection and Programs Directorate (NPPD), the National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. The NICC is part of NPPD's Office of Infrastructure Protection and the DHS National Operations Center.

This SMOUT is being updated and renewed in an effort to specifically document the NICC's social media activities. The NICC does not conduct its own media monitoring or searches, but instead accesses select social media sites to view information being disseminated from other Federal, state, local, tribal, and territorial (FSLTT) as well as critical infrastructure partners and official news sources. The social media applications the NICC currently use include, but are not limited to, Twitter, Facebook, and YouTube. The use of social media will be limited to:

- Enhancing situational awareness of critical infrastructure during steady-state;
- Enabling timely and consistent receipt of information and engagement during incident management activities; and
- Ensuring information is received from the NICC's critical infrastructure partners who use social media as a regular form of communication.

Personnel requesting access include employees within the National Infrastructure Coordinating Center (NICC). All employees with access to social media for these purposes are trained by the NPPD Office of Privacy so that there is a clear understanding on what uses are appropriate under this template and associated rules of behavior.

Background:

The NICC is both an operational component of NPPD/IP and a watch operations element of the DHS National Operations Center. The NICC maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares all-hazards information in support of the greater IP mission. The NICC is also co-located with the National Cybersecurity and Communications Integration Center (NCCIC) allowing enhanced support to critical infrastructure protection.

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

- **Privacy Policy for Operation Use of Social Media, MD 110-01**
- **Title II of the Homeland Security Act of 2002 (Public Law 107-296), as amended, March 2006**
- **PPD-8, National preparedness, March 2011**
- **PPD-17, Countering Improvised Explosive Devices, June 2012**
- **PPD-21, Critical Infrastructure Security and Resilience, February 2013**
- **EO 13636, Improving Critical Infrastructure Cybersecurity, February 2013**
- **EO 13650, Improving Chemical Facility Safety and Security, August 2013**
- **National Infrastructure Protection Plan, December 2013**
- **National Protection and Programs Directorate, Office of Infrastructure Protection Strategic Plan:2012-2016, August 2012**
- **The National Protection and Programs Directorate Strategic Plan for Fiscal years 2014-2018, May 2013**
- **National Mitigation Framework, May 2013**

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: January 2014

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: The NICC's social media activities do not permit the collection of PII and therefore there will not be an active attempt to collect PII.

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

☒ Yes. ☐ No. If not, please explain:

Safeguards will be followed in the event of an incidental collection of PII.

g) *Documentation*. Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ 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: April 12, 2018

NAME of the DHS Privacy Office Reviewer: Max Binstock

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: <If applicable, include PIA name and number here.>

SORN: <If applicable, include SORN name and number here.>

1. **Category of Use:**

☐ Law Enforcement Intelligence;

☐ Criminal law enforcement investigations;

☐ Background investigations;

☐ Professional responsibility investigations;

☐ Administrative or benefit determinations (including fraud detection);

☒ Situational awareness; and

☐ Other. <Please explain "other" category of use here.>

2. **Has Component Counsel reviewed and determined that there is authority to engage in the above Category of Use?**

☒ Yes. ☐ No.

3. **Rules of Behavior Content: (Check all items that apply.)**

a. *Equipment.*

☐ Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

☒ Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. *Email and accounts*.

☐ Users do not have to use government email addresses or official DHS accounts online.

☒ Users must use government email addresses or official DHS accounts online.

c. *Public interaction*.

☐ Users may interact with individuals online in relation to a specific law enforcement investigation.

☒ Users may NOT interact with individuals online.

d. *Privacy settings*.

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage*:

The NICC's social media activities do not permit the collection of PII and therefore there will not be an active attempt to collect PII.

☐ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here:

☐ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards*.

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

Safeguards will be followed in the event of an incidental collection of PII.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative.

g. *Documentation.*

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training.*

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ 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, certification of training completion cannot be verified.

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.

☐ New.

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

☐ A SORN is required:

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

The NICC does not conduct its own media monitoring or searches, but instead accesses select social media sites to view information being disseminated from other Federal, state, local, tribal, and territorial (FSLTT) as well as critical infrastructure partners and official news sources. The social media applications the NICC currently use include, but are not limited to, Twitter, Facebook, and YouTube. No PIA or SORN is required because no PII will be collected. All employees will be trained on appropriate use.