The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, 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, the Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

## SUMMARY INFORMATION

**Date submitted for review:** December 3, 2013

**Name of Component:** National Protection and Programs Directorate

**Contact Information:** (b)(6) Chief of Staff for the Office of Infrastructure Protection, (b)(6)

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

**IT System(s) where social media data is stored:** Social media will be used to enhance situational awareness, and information is not expected to be stored.

**Applicable Privacy Impact Assessment(s) (PIA):** Not required at this time.

**Applicable System of Records Notice(s) (SORN):** Not required at this time.

[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:

The National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience issues. The office conducts and facilitates vulnerability assessments and maintains a suite of additional tools and resources to enable critical infrastructure owners and operators, as well as other Federal, state, local, tribal, and territorial (FSLTT) partners, to enhance the security and resilience of their critical infrastructure. IP provides partners with information on emerging threats and hazards to inform mitigation and protection activities.

Given the vast responsibilities of IP regarding information sharing, critical infrastructure protection and resilience, engagement with FSLTT governments and private sector owners and operators during steady-state and incident management operations, the use of social media is a valuable tool and resource to the mission. IP is not looking to conduct its own media monitoring or searches, but instead would like access to select social media sites to view information being disseminated from other FSLTT and critical infrastructure partners and official news sources. The social media applications IP would like to 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 IP's partners who use social media as a regular form of communication.

Personnel requesting access include: all IP employees within each division, as well as IP Senior Leadership and the Office of the Assistant Secretary staff. All employees with access to social media for these purposes will be 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:

IP consists of the following divisions:

- Infrastructure Information Collection Division (IICD)
- Infrastructure Analysis & Strategy Division (IASD)
- Infrastructure Security Compliance Division (ISCD)
- National Infrastructure Coordinating Center (NICC)
- Protective Security Coordination Division (PSCD)
- Sector Outreach and Programs Division (SOPD)

IICD provides the IT solutions for the collection, protection, and sharing of critical infrastructure protection data, as well as manages the Protected Critical Infrastructure Information (PCII) program, which provides congressionally mandated protections from public disclosure for qualifying critical infrastructure information. The work IICD does involves daily interaction with Federal, state and local governments, as well as private sector owners and operators.

IASD manages the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a center of excellence for critical infrastructure risk analysis focusing on the consequences to critical infrastructure from a threat or incident. Information developed by HITRAC includes an understanding of the dependencies, interdependencies, and cascading effects to critical infrastructure. IASD's analysis helps to inform NPPD's leadership and its partners in the public and private sector on critical infrastructure risk. This analysis helps them make more informed decisions on preparedness, prevention, protection, response, and recovery actions to improve the overall resilience and security of the Nation's critical infrastructure.

SOPD oversees the Department's support of partnership councils, education and outreach, planning and preparedness exercises, and information sharing related to critical infrastructure protection and resilience. SOPD also performs Sector-Specific Agency (SSA) responsibilities specified by the National Infrastructure Protection Plan for six of the 16 critical infrastructure sectors (Chemical Sector, Commercial Facilities Sector, Critical Manufacturing Sector, Dams Sector, Emergency Services Sector, and Nuclear Reactors, Materials, and Waste Sector). SOPD leads the Department's programs to unify public and private sector operations to secure and prepare these six sectors for impacts from such events as terrorist attacks or natural disasters.

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

stakeholders. The NICC's capabilities and requirements directly support NPPD/IP Senior Leadership and field operations.

PSCD works closely with the Department's public and private sector partners to reduce the risk to the Nation's critical infrastructure by conducting site vulnerability assessments, coordinating bombing prevention programs, and facilitating preparedness, response, and recovery. The PSCD Protective Security Advisors (PSAs) are a critical conduit of information on critical infrastructure response, recovery, and reconstitution of resources, in addition to supporting incident management activities and leading IP's voluntary programs from across the country. They advise the Department on interdependencies, cascading effects, and damage assessments concerning impacted areas, and enable owners and operators, and other critical partners the ability to share and receive information more timely and effectively. To inform decision-making, they provide real time data across all levels of government and within the department, via the NICC. PSCD's Office for Bombing Prevention leads the Department's efforts to implement the National Policy for Countering Improvised Explosive Devices and enhance the Nation's ability to prevent, protect against, respond to, and mitigate the terrorist use of explosives against critical infrastructure, the private sector, and FSLTT entities.

ISCD leads the National implementation of the Chemical Facility Anti-Terrorism Standards (CFATS). As part of the implementation process of the CFATS program, the Chemical Security Inspectors are required to serve as a conduit between private sector owners and operators and the Department on all compliance information specific to the regulated community and chemical facility safety and security. This includes timely access to information, especially during incident management activities in support of the Federal Emergency Management Agency (FEMA) National Response Framework and in close coordination with PSAs and the NICC.

IP's field personnel, consisting of PSCD's PSAs, working IP's voluntary programs, and ISCD's Chemical Security Inspectors, leading the regulatory chemical-security program, are strategically located across the country. They are often the first personnel to engage with state, local, and private sector partners during an incident, and are deployable personnel to Emergency Operations Centers and at the FEMA Joint Field Offices.

Additionally, IP Office of the Assistant Secretary staff work with each of the divisions within IP to support IP's mission and to maintain strategic relationships and partnerships with stakeholder organizations, congressional offices, and the media.

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

- Privacy Policy for Operational 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, January 2009
- National Protection and Programs Directorate, Office of Infrastructure Protection FY 2012 Expenditure Plan: Fiscal Year 2012 Report to Congress, July 2012
- 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:

**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: IP use of social media is strictly for viewing information being disseminated from other FSLTT and critical infrastructure partners and official news sources related to critical infrastructure protection and incident management, not for the purposes of seeking to identify individuals. IP will not be collecting data, including PII, through this use of social media.

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

☐ Yes. ☒ No. If not, please explain: IP use of social media is strictly for viewing information being disseminated from other FSLTT and critical infrastructure partners and official news sources related to critical infrastructure protection and incident management, not for the purposes of seeking to identify individuals. IP will not be collecting data, including PII, through this use of social media.

**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: January 6, 2013**

**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.
  - ☐ 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**

No PIA or SORN required because no PII will be collected.

IP is only accessing social media sites to view information. The use is limited and focused. No PII will be collected and all employees will be trained on appropriate use.