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: 6 Sep 2017

Name of Component: U.S. Coast Guard

Contact Information: Mr. Brian Burns, CIO and Component Privacy Officer, Deputy Assistant Commandant for C4IT, (b)(6)

Counsel[2] Contact Information: CAPT Chris Mooradian, (b)(6) (b)(6)

IT System(s) where social media data is stored: Marine Information for Safety and Law Enforcement (MISLE)

Applicable Privacy Impact Assessment(s) (PIA):

DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) 2009

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

DHS/USCG-013 - Marine Information for Safety and Law Enforcement (MISLE), 74 Fed Reg 30305 (June 25, 2009), Final Rule for Privacy Act Exemptions 74 Fed Reg 63948 (December 4, 2009).

[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 U.S. Coast Guard primarily and traditionally relies on VHF-FM, HF and other radiofrequency and digital telecommunications for receipt and response to maritime search and rescue (SAR) distress calls, including in flooded inland areas. Receipt of distress communications on official CG official social media sites (U.S. Coast Guard webpages, Facebook, and Twitter) has rapidly emerged as a means the public is increasingly using to contact the Coast Guard and request assistance. Although not a preferred means to receive distress calls, the use of official social media the below ways following ways may increase the effectiveness of the Coast Guard's lifesaving mission, especially where the primary means of communicating a distress call (e.g. VHF-FM radio or 911 telephone calls) are unavailable to the public, for example during a large-scale natural disaster or man-made incident. The Coast Guard will use social media for official purposes through the internet from a limited number of designated Coast Guard standard computers on its wide area network (CGOne) located within operational command centers (at the National Command Center, Area command centers, District command centers, and Sector command centers). This will include 2 CGOne terminals in each of 49 command centers, which provides redundant capacity in the event that one of the terminals fails. These computers will be accessed by one watch stander at a time, with the watch standers rotating to sustain the watch during a 24x7 basis. The total number of watch standers who would have access would be 400 (not simultaneously); CG Cyber Command would be able to track who is logged into any particular computer at any specific time.

The use is limited to government employees (military, civilian and Coast Guard Auxiliary personnel) who log on as official users with clear Coast Guard affiliation to conduct the following actions: (a) Monitoring, Receiving, and Managing Coast Guard Official social media sites/feeds to respond to distress calls received on those sites/feeds; (b) conduct official searches of publicly available (non-private) social media sites/feeds for SAR PRECOM and SAR EXCOM Purposes as described in Coast Guard Search and Rescue Policy, Commandant Instruction M16130.2F. PRECOM and EXCOM are a means of gathering available information to determine whether there is justification to launch operational assets to conduct a search. USCG personnel will only conduct searches of publicly available, non-private commercial social media sites/feeds for information regarding a potential person(s) in distress

after a report of an overdue or missing person, vessel or aircraft who may be in distress at sea or when an individual contacts the USCG through USCG social media sites/feeds. In such cases, the Coast Guard must gather information to decide when it is appropriate to launch Coast Guard boats, cutters, and aircraft to begin an active search for a potential mariner, vessel or aircraft in distress.

Coast Guard personnel monitoring social media sites/feeds shall only collect PII when it is provided directly by an individual to the Coast Guard social media/site for the purpose of communicating a distress. Only the minimum PII will be collected and Coast Guard personnel shall copy and retain electronic or paper copies of CG social media communication, including PII, in the SAR case package, which is part of the Marine Information for Safety and Law Enforcement (MISLE). At no time should a person's name, address, date of birth, phone number, or address, or other PII be recorded except where it can be reasonably be determined that the person is in distress and their safety of life is a risk or *in extremis* situations. Unless USCG is required to keep the PII by law or regulation and the information is maintained in a Privacy Act-compliant system, USCG will redact PII once USCG responds to the incident or the information has been transmitted to the responding authority. USCG will only use the information for a purpose compatible with the purpose for which it was collected. USCG will not ask for individual PII on the public page. If USCG requires additional information, USCG will contact the individual directly using the contact information provided by the requesting individual.

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

6 U.S.C. 888(a) preserves the Coast Guard Search and Rescue Missions.

14 U.S.C. 88 establishes the Coast Guard's authority to render aid to distressed persons, vessels, and aircraft on waters over which the United States has jurisdiction and specifically authorizes the Coast Guard to perform "any and *all acts* necessary to rescue and aid persons and protect and save property." 14 U.S.C. 88(a)(1) (emphasis added).

14 U.S.C. 93 (Commandant, general powers). Pursuant to this authority, the Commandant "may accept and utilize, in times of emergency in order to save life or protect property, such voluntary services as may be offered to the Coast Guard."

14 U.S.C. 141 (Cooperation with other agencies, States, territories, and political subdivisions).

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: 7 Sept 2017

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

Attachment (1) U.S. Coast Guard Rules of Behavior for Operational of Social Media Use for Situational Awareness and Search and Rescue Operations.

Attachment (2) U.S. Coast Guard Rules of Behavior for Operational Use of Social Media for Situational Awareness and Search and Rescue Operations—Access Agreement

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:

While generally use will be limited to looking at social media communications to the Coast Guard's social media platforms, there could be occasions where that platform is used to communicate with the person seeking assistance in order to ascertain additional information to inform the nature of the distress and the appropriate search and rescue response.

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:

The Coast Guard Privacy Officer and CG Public Affairs, with assistance of the Office of Information and Intelligence Law, will develop and distribute appropriate training to be provided to Command Center personnel regarding the use and monitoring of social media for SAR purposes. The annual training will include:

a. Proper documentation of information to minimize and protect PII
b. Rules of behavior listed here
c. Use of official Coast Guard social media sites/feeds accounts.

Mechanisms will be put 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: 9/7/2017

SMOUT expiration date: 11/30/2017

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. Interim coverage under DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE)

☐ New.

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

☒ A SORN is required:

☒ Covered by existing SORN. Interim coverage under DHS/USCG-013 - Marine Information for Safety and Law Enforcement (MISLE), June 25, 2009 74 FR 30305

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

USCG submits this SMOUT in response to an emergency need for the 2017 hurricane season. USCG is requesting the use of social media for search and rescue purposes. Members of the public in need of rescue are using social media to contact USCG, particularly when 911 or other traditional means of receiving an emergency response are not working. USCG may also use social media when it receives a report of a missing person. USCG will follow the baseline rules with the exception that it may contact the individual when needed to get additional information to conduct the rescue.

PRIV finds that both PIA and SORN coverage is required. PRIV finds interim coverage for USCG's use of social media for search and rescue purposes under the MISLE PIA and SORN.

Although PRIV finds interim coverage for this operational use of social media, this coverage is only temporary. PRIV requires USCG update or provide a new SMOUT for the operational use of social media for rescues beyond 11/30/2017. In order to create an operational program, PRIV requires USCG review its use of social media to scrub the data and remove any unnecessary PII. PRIV will also require USCG develop specialized training and publish a new PIA and SORN (SORN coverage will likely be the forthcoming Marine Safety and Non-Law Enforcement Records SORN). PRIV and USCG will also revisit the Operational Rules and Rules of Behavior.

This SMOUT expires on 11/30/2017.