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: June 22, 2018

Name of Component: US Coast Guard

Contact Information: LCDR (b)(6) **Legal Counsel, CGIS** (b)(6)

Counsel[2] Contact Information: (b)(6) **Acting Legal Counsel, CGIS** (b)(6)

IT System(s) where social media data is stored: Field Activity Case Tracking System (FACTS)

Applicable Privacy Impact Assessment(s) (PIA): DHS/ALL/PIA-029 Field Activity Case Tracking System (FACTS)

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

- **DHS/ALL-020 Department of Homeland Security Internal Affairs**
- **DHS/ALL-023 Personnel Security Management**
- **DHS/ALL-029 Civil Rights and Civil Liberties Records**
- **DHS/ALL-038 Insider Threat Program**

[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.**

   Social Media may be collected as part of criminal investigations and law enforcement intelligence operations in accordance with the COMDTINST 5520.5 (series) and COMDINST M5527.1 (series). Law enforcement personnel communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when CG Policy would require such disclosure if the communication were taking place in person or over the telephone. Law enforcement personnel may communicate online under a non-identifying name or fictitious identity if CG policy would authorize such communications in the physical world. For purposes of CGIS undercover guidelines, each discrete conversation online constitutes a separate undercover activity or contact, but such a conversation may comprise more than one transmission between the law enforcement personnel and another person. CGIS policy requires significant documentation, planning, review and ultimately HQ approval for undercover activities.

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

   14 USC 95, 14 USC 89, COMDTINST 5520.5F, COMDTINST 5527.1F

   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: Unknown. Collection of social media has been a part of Coast Guard criminal investigations for longer than the term social media has been commonly used.

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

   See attached Director's Note 06-2012

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: Both - Criminal investigators authorized to use non-attributable accounts in the same manner as they are allowed to assume undercover identities in other contexts.

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:** Criminal investigators may interact with individuals in the same manner as they would over the phone or via mail if authorized in accordance with COMDTINSTM 5527.1 (series).

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

6. ☒ Yes. ☐ No. If not, please explain: Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space, e.g. consent, search warrant, etc.

a) *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:

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

☒ Yes. ☐ No. If not, please explain:

c) *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:

d) *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: 8/13/2019

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. USCG tracks whether agents execute the user agreement discussed in Director's Note 06-2012, Acceptable Use of Online Information and Information Technology by CGIS Law Enforcement Personnel.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ Covered by existing PIA. DHS/USCG/PIA-029 Field Activity Case Tracking System (FACTS)

☐ New.

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

☒ A SORN is required:

☒ Covered by existing SORN.

DHS/ALL-020 Department of Homeland Security Internal Affairs

DHS/ALL-023 Personnel Security Management

DHS/ALL-029 Civil Rights and Civil Liberties Records

DHS/ALL-038 Insider Threat Program

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

USCG is submitting this SMOUT to document the use of social media by the Coast Guard Investigative Service (CGIS). Social media may be collected as part of criminal investigations and law enforcement intelligence operations in accordance with the COMDTINST 5520.5 (series) and COMDINST M5527.1 (series). Law enforcement personnel communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when CG Policy would require such disclosure if the communication were taking place in person or over the telephone. Law enforcement personnel may communicate online under a non-identifying name or fictitious identity if CG policy would authorize such communications in the physical world. CGIS policy requires significant documentation, planning, review and ultimately HQ approval for undercover activities.

The DHS Privacy Office finds that both PIA and SORN coverage are required.

PIA coverage is provided by the recently approved DHS/USCG/PIA-029 Field Activity Case Tracking System (FACTS), which outlines the responsibilities of CGIS. SORN coverage is provided by the following SORNs: DHS/ALL-020 Department of Homeland Security Internal Affairs, DHS/ALL-023 Personnel Security Management, DHS/ALL-029 Civil Rights and Civil Liberties Records, and DHS/ALL-038 Insider Threat Program.

This SMOUT expires in 3 years.

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

I agree to comply with the following rules of behavior:

1. Use social media for operational purposes only when activities are authorized by statute, executive order, regulation, or properly promulgated policy;

2. Use only government-issued equipment, government accounts and only government issued email addresses and Coast Guard social media sites/feeds approved by Commandant (CG-0922) when engaging in the operational use of social media;

3. Use online screen names or identities that indicate an official Coast Guard affiliation and use Coast Guard email addresses to open accounts used when engaging in social medial in the performance of their duties.

4. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information. In exigent circumstances, USCG may interact with members of the public who contact USCG to be rescued. 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. USCG personnel will only collect the minimum amount of information needed to facilitate a rescue operation where safety of life is threatened.

5. Respect individual privacy settings and access only information that is publicly available unless the individual whose information I seek to access has given consent to access it;
6. Collect the minimum PII necessary for the proper performance of my authorized duties;
7. Protect PII as required by the Privacy Act and DHS privacy policy; and
8. Document the use of social media, including date, site(s) accessed, information collected, and how it was used, in the same manner that the Coast Guard would document information collected from any source in the normal course of business. For instance, when information obtained through the authorized operational use of social media is used in whole or in part to make decisions regarding an individual's rights, benefits, or privileges, I will document that fact in relevant records.
9. Copy and retain electronic or paper copies of CG social media communications in the SAR case package, which is part of the Marine Information for Safety and Law Enforcement (MISLE), a Coast Guard System of Records under the Privacy Act.

I acknowledge that I have read the Coast Guard Rules of Behavior for Social Media Operational Use for Situational Awareness and Search and Rescue Operations dated 7 Sep 2017; I understand them, and I will comply with them. I understand that failure to comply with these rules could administrative or legal action to include removal of access to Coast Guard social media and Coast Guard IT system (CGOne), reassignment to other duties, termination, and criminal or civil prosecution.

Name:_____
First, Middle Initial, Last

Rank:_____ **Title/Position:**_____

Signature:_____ **Date:**_____