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 OCIAL 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: July 31, 2017

Name of Component: Federal Emergency Management Agency

Contact Information: (b)(6)

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

IT System(s) where social media data is stored:

Applicable Privacy Impact Assessment(s) (PIA): DHS/FEMA/PIA-041 FEMA Operational Use of Publicly Available Social Media for Situational Awareness (March 10, 2016).

Applicable System of Records Notice(s) (SORN): DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness, 81 Fed. Reg. 23,503 (April 21, 2016).

[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.**

FEMA ORR launched its Publicly Available Social Media Sources for Situational Awareness Initiative to leverage FEMA Watch Centers[3] in support of the FEMA Administrator's responsibility under the Homeland Security Act[4], and to assist the DHS National Operations Center (NOC) in its mission[5] to establish the National Common Operating Picture, for which FEMA is a primary source of information during natural disasters. This effort provides situational awareness for federal and international partners as well as state, local, tribal, and territorial (SLTT) governments to maintain and enable timely and actionable decision-making. The term "situational awareness" in this context refers to a state of understanding from which decisions can be made.

FEMA Watch Centers maintain timely, accurate, and actionable situational awareness of potential and actual incidents that may require a coordinated federal response in support of FEMA leadership and the DHS NOC[6] through a continuous cycle of information collection, analysis, and collaboration with federal and international partners as well as SLTT governments.

During large scale disasters, FEMA Watch Centers, operate as a part of the National Response Coordination Center (NRCC) and Regional Response Coordination Centers (RRCC), to gather information from a variety of sources, including social media, and communicate the information to emergency managers and government officials to form the basis for incident management decision-making. The purposes of this initiative is to provide critical situational awareness in support of FEMA's mission to reduce the loss of life and property, as well as protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters.[7] FEMA also assists the DHS NOC in providing situational awareness and a common operating picture for governments and partners at all levels.

---

[3] The term "Watch Centers" incorporates all watch and coordination center capabilities for FEMA including: the National Watch Center (NWC), the National Response Coordination Center (NRCC), ten Regional Watch Capabilities (RWC), ten Regional Response Coordination Centers (RRCC), and five Mobile Emergency Response Support (MERS) Operations Centers (MOC).
[4] 6 U.S.C. § 313(c)(4)(A).
[5] 6 U.S.C. § 313d(b)(1).
[6] DHS/OPS/PIA-004(f) Publicly Available Social Media Monitoring and Situational Awareness Initiative (May 13, 2015).
[7] 6 U.S.C. § 313(b)(1).

FEMA is adopting a new means of monitoring social media through the use of Dataminr's News Alerting tool. While this will not change the operational use of social media, nor the manner in which PII is observed and/or acted upon *in extremis*[8] situations, FEMA would like to document the use of this tool, which belongs to a category of social media tools, known as Social Media Aggregators (SMAs).

SMAs automate many of the previous processes that FEMA used for monitoring and observing trends found on social media to inform the mission of the FEMA Watch Centers. The adoption of an SMA will not alter the types of PII that the FEMA Watch Centers collect, maintain, store, share, or use to make operational decisions. Importantly, Dataminr does not allow an individual user to search for a particular user's user name or "handle," which prevents Dataminr users from targeting individuals' First Amendment-protected rights

While previous tools that were used to monitor social media required targeted keywords, Dataminr uses proprietary algorithms and machine learning to identify and categorize breaking news events, then deliver them to users based on individualized preferences. User's settings, which consist of geographic location and up to 37 predetermined topics, determine the kind of alerts they will receive. In addition, Dataminr's Custom Alerts capability allows users to receive breaking news alerts based on specific keywords. The FEMA Watch Centers can configure their settings to monitor events based on significance or importance to the Agency. As in previous efforts, these topics, hashtags, and trends will center on natural and manmade disasters, all-hazards, or acts of terrorism. The National Watch Center (NWC) will focus on those events of national importance or impact, while the Regional Watch Centers (RWCs) will focus their monitoring efforts on more localized events. While there may be some variance in the types of topics that the RWCs focus on, such as local bridges, airports, or other infrastructure, the RWCs monitoring efforts will not deviate from the approach to monitoring than that of the NWC. The RWCs will not collect or maintain PII on individuals in any way that differs from the NWC. The NWC and the RWCs will commit to a set of keywords that permit them to fulfill their mission, but that will not lead to targeting individual social media users.

FEMA may collect, through publicly available sites and sources, information from members of the public, first responders, press, volunteers, and others that provide publicly available information on social media sites including online forums, blogs, public websites, and message boards. FEMA may collect any of the following from these individuals:

- Individual's name;
- Social media account information including: Email address, Login ID, Handle, User Name, or Alias;

[8] In *in extremis* cases, FEMA sends the information through email to the appropriate entity that can assist in the situation, such as Urban Search and Rescue or an Incident Management Assistance Team (IMAT). FEMA does not store or retain the PII once the information is transmitted to the appropriate responding entities.

- Address or approximate location (via geo-coded submission);
- Job title or Position;
- Phone numbers, email address, or other contact information included in, or associated with a user profile;
- Date and Time of post; and
- Additional details relevant to an in extremis situation (e.g., details of an individual's physical condition).

Additional Information Created As Part of This Initiative

- Reports related to incidents or updates seen via social media;
- Links to original social media content described in reports (See Appendix A for examples of sites from which content could potentially be linked and described in a report); and
- Links to other open source media such as a publicly available website (e.g., npr.org).

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

- The Homeland Security Act of 2002, § 515 at 6 U.S.C. § 321d(b)(1)
- The Homeland Security Act of 2002, § 503 at 6 U.S.C. § 313(b)(2)(A)-(H).
- The Homeland Security Act of 2002, § 504 at 6 U.S.C. § 314(a)(17), describing responsibility for the NRCC under "Authority and responsibilities (of the FEMA Administrator).".
- The Homeland Security Act of 2002, § 503 at 6 U.S.C. § 313(b)(2)(B).

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.

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: 8/29/17

SMOUT expiration date: 11/29/17

NAME of the DHS Privacy Office Reviewer: Hannah Burgess

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. DHS/FEMA/PIA-041 Operational Use of Publicly Available Social Media for Situational Awareness

☐ New.

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

☒ A SORN is required:

☒ Covered by existing SORN. DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness, April 21, 2016, 81 FR 23503

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

FEMA is submitting this SMOUT to document the use of the tool Dataminr, which is a Social Media Aggregator. FEMA's use of this tool will not change the operational use

of social media, nor the manner in which PII is observed and/or acted upon in extremis situations. Dataminr will identify breaking news events and deliver them to FEMA based on a user's settings, which consist of geographic location and up to 37 predetermined topics. Dataminr also allows users to receive breaking news alerts based on specific keywords. The DHS Privacy Office determines that FEMA has provided sufficient documentation to demonstrate compliance with MD 110-01. However, the DHS Privacy Office requires that FEMA re-submit documentation for Dataminr in the regular PTA template instead of the SMOUT template by November 29, 2017.

Domestic Security

Assassination

Attack

Domestic security

Drill

Exercise

Cops

Law enforcement

Authorities

Disaster assistance

Disaster management

DNDO (Domestic Nuclear Detection Office)

National preparedness

Mitigation

Prevention

Response

Recovery

Dirty bomb

Domestic nuclear detection

Emergency management

Emergency response

First responder

Domestic Security (con't)

Homeland security

Maritime domain awareness (MDA)

HAZMAT & Nuclear

Hazmat

Nuclear

Chemical spill

Suspicious package/device

Toxic

National laboratory

Nuclear facility

Nuclear threat

Cloud

Plume

Radiation

Radioactive

Leak

Biological infection (or event)

Chemical

Chemical burn

Biological

HAZMAT & Nuclear (con't)

Epidemic

Hazardous

Hazardous material incident

Industrial spill

Infection

Powder (white)

Gas

Spillover

Anthrax

Blister agent

Chemical agent

Exposure

Burn

Nerve agent

Ricin

Sarin

North Korea

Health Concern + H1N1

Outbreak

Contamination

Exposure

Virus

Evacuation

Bacteria

Recall

Ebola

Food Poisoning

Foot and Mouth (FMD)

H5N1

Avian

Flu

Salmonella

Small Pox

Plague

Human to human

Human to Animal

Influenza

Center for Disease Control (CDC)

Drug Administration (FDA)

Public Health

Toxic

Agro Terror

Tuberculosis (TB)

Agriculture

Listeria

Symptoms

Health Concern + H1N1 (con't)

Mutation

Resistant

Antiviral

Wave

Pandemic

Infection

Water/air borne

Sick

Swine

Pork

Strain

Quarantine

H1N1

Vaccine

Tamiflu

Norvo Virus

Epidemic

World Health Organization (WHO) (and components)

Viral Hemorrhagic Fever

E. Coli

Infrastructure Security

Infrastructure security

Airport (Regional and abbreviations)

Airplane (and derivatives)

Chemical fire

CIKR (Critical Infrastructure & Key Resources)

Infrastructure Security (con't)

AMTRAK

Collapse

Computer infrastructure

Communications infrastructure

Telecommunications

Critical infrastructure (local and regional)

National infrastructure

Metro

WMATA

Subway

BART

MARTA

Port Authority

NBIC (National Biosurveillance Integration Center)

Transportation security

Grid

Power

Smart

Body scanner

Electric

Failure or outage

Black out

Brown out

Port

Dock

Bridge

Cancelled

Highway names and numbers

Bridge names

Key local infrastructure names

Infrastructure Security (con't)

Delays

Service disruption

Power lines

Weather/Disaster/Emergency

Emergency

Hurricane

Tornado

Twister

Tsunami

Earthquake

Tremor

Flood

Storm

Crest

Temblor

Extreme weather

Forest fire

Brush fire

Ice

Stranded/Stuck

Help

Hail

Wildfire

Tsunami Warning Center

Magnitude

Avalanche

Weather/Disaster/Emergency (con't)

Typhoon

Shelter-in-place

Disaster

Snow

Blizzard

Sleet

Mud slide or Mudslide

Erosion

Power outage

Brown out

Warning

Watch

Lightening

Aid

Relief

Closure

Interstate

Burst

Emergency Broadcast System

Cyber Security

Cyber security (cybersecurity)

Botnet

DDOS (dedicated denial of service)

Denial of service

Malware

Virus

Cyber Security (con't)

Trojan

Keylogger

Cyber Command

2600

Spammer

Phishing

Rootkit

Phreaking

Cain and abel

Brute forcing

Mysql injection

Cyber attack

Cyber terror

Hacker

China

Conficker

Worm

Scammers

Social media

Other

Breaking News