



Privacy Impact Assessment  
for the  
FEMA Operational Use of Publicly Available Social Media for  
Situational Awareness

**DHS/FEMA/PIA-041**

**March 10, 2016**

**Contact Point**

**Christopher Blaz**  
**Director, FEMA National Watch Center**  
**Federal Emergency Management Agency**  
**Response Directorate**  
**(202) 646-7940**

**Reviewing Official**

**Karen L. Neuman**  
**Chief Privacy Officer**  
**Department of Homeland Security**  
**(202) 343-1717**



## Abstract

The Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR) has launched an initiative using publicly available social media for situational awareness purposes in support of the FEMA Administrator’s responsibility under the Homeland Security Act<sup>1</sup> and to assist the DHS National Operations Center (NOC)<sup>2</sup> by helping to shape its mission to provide situational awareness during emergency and disaster situations, during which, FEMA is a primary source of information. The initiative assists FEMA’s efforts to provide situational awareness for federal and international partners as well as state, local, tribal, and territorial (SLTT) governments. FEMA’s Watch Centers collect information from publicly available traditional media, such as newspapers and television news, and new media sources, such as social media websites and blogs for situational awareness purposes. While this initiative is not designed to actively collect personally identifiable information (PII), FEMA is conducting this Privacy Impact Assessment (PIA) because FEMA’s Watch Centers may collect, maintain, and disseminate limited amounts of PII *in extremis* situations to prevent the loss of life or serious bodily harm.

## Overview

FEMA ORR launched its Publicly Available Social Media Sources for Situational Awareness Initiative to leverage FEMA Watch Centers<sup>3</sup> in support of the FEMA Administrator’s responsibility under the Homeland Security Act<sup>4</sup>, and to assist the DHS NOC in its mission<sup>5</sup> 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 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<sup>6</sup> through a continual cycle of information collection, analysis, and

---

<sup>1</sup> [6 U.S.C. § 313\(c\)\(4\)\(A\)](#)

<sup>2</sup> [6 U.S.C. § 321d\(b\)\(1\)](#)

<sup>3</sup> 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).

<sup>4</sup> [6 U.S.C. § 313\(c\)\(4\)\(A\)](#)

<sup>5</sup> [6 U.S.C. § 321d\(b\)\(1\)](#)

<sup>6</sup> The DHS National Operations Center (NOC) PIA (*available at [http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy\\_pia\\_ops\\_NOC%20MMC%20Update\\_April2013.pdf](http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_ops_NOC%20MMC%20Update_April2013.pdf)*) describes its operation in greater detail. The System of Records Notice (SORN) covering its records (*available at <http://www.gpo.gov/fdsys/pkg/FR-2011-02-01/html/2011-2198.htm>*) describes the records that the DHS NOC collects and maintains under its Social Media Monitoring Initiative. FEMA Watch Centers are responsible to both the DHS NOC and FEMA leadership. Unlike the DHS NOC, FEMA Watch Centers work and communicate directly with the states, which assists them with state and local emergency response and preparedness.



collaboration with federal and international partners as well as SLTT governments. FEMA Watch Centers, including the National Response Coordination Center (NRCC) and Regional Response Coordination Centers (RRCC), 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.<sup>7</sup> FEMA also assists the DHS NOC in providing situational awareness and a common operating picture for governments and partners at all levels.

In DHS *Management Instruction Number 110-01-001*, DHS defines "social media" as a "sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact."<sup>8</sup> This definition includes web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies, while excluding internal Department intranets or applications. Appendix A includes an illustrative though not exhaustive list of sites that FEMA monitors.

As part of this initiative, Watch Centers only gather information from publicly available sites and sources. Watch Centers do not access private or blocked information, or sign up for any social media accounts not authorized by FEMA External Affairs and other appropriate FEMA offices (e.g., Office of the Chief Information Officer (OCIO) and Office of the Chief Counsel (OCC)). In addition, Watch Center analysts use only government-issued equipment and official FEMA Watch Center-branded social media accounts when engaging in monitoring social media for situational awareness. As part of this Initiative, Watch Center analysts may follow users such as: emergency managers or agencies, official government (SLTT) agencies or personnel, weather sources, news agencies, and known subject matter experts (emergency management volunteers, tornado spotters, or Community Emergency Response Team (CERT) members). FEMA uses relevant social media postings from these individuals for situational awareness and to establish a clear common operating picture. FEMA's Watch Centers neither follow private individuals (those individuals not in one of the aforementioned categories), nor do FEMA's Watch Center analysts interact with members of the public through social media in their capacity as FEMA employees when performing Watch Center duties. In other words, FEMA Watch Centers does not post tweets, retweets, messages, or other postings to individual social media users.<sup>9</sup>

FEMA Watch Center analysts typically monitor and review publicly available Internet social media (see Appendix A) and use a set of keywords (see Appendix B) to find and retrieve content relevant to FEMA for situational awareness purposes. FEMA aggregates information to share with internal and external partners as appropriate using this social media content and other publicly

---

<sup>7</sup> FEMA's mission is defined in Section 503 of the Homeland Security Act of 2002, *as amended*.

<sup>8</sup> [https://www.dhs.gov/xlibrary/assets/foia/Instruction\\_110-01-001\\_Privacy\\_Policy\\_for\\_Operational\\_Use\\_of\\_Social\\_Media.pdf](https://www.dhs.gov/xlibrary/assets/foia/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf)

<sup>9</sup> Note that the FEMA Office of External Affairs may interact with the public, consistent with their mission to communicate with external entities on behalf of the Agency.



available content. This may include a FEMA-written narrative of the situation being described through various media or social media outlets, as well as links or Uniform Record Locators (URL) to the publicly available open source resources that FEMA references.

FEMA's social media monitoring under this Initiative is neither designed nor intended to collect PII from members of the public; however, given the unpredictable nature of disasters coupled with the voluntary and unrestricted nature of social media, it is possible during *in extremis* situations for FEMA to collect a limited amount of PII from the public through its monitoring of Internet social media.

An *in extremis* situation is one which there is an imminent threat of loss of life or serious bodily harm. Under these scenarios, the collection of PII occurs through the same monitoring and reporting process used by the Watch Center analysts to produce situational awareness reports as noted above; however, any collection of PII is limited to what is necessary to respond and provide assistance to the individual. For example, FEMA may collect an individual's name; social media user name, handle, or alias; address or approximate location; phone number, email address, or other contact information that is made publicly available on social media; and possibly details of the individual's relevant circumstances.

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.<sup>10</sup> If FEMA includes information regarding the situation in duty log reports or any additional reports, it will redact any PII and only include general location and incident information. Appendix C contains examples of how FEMA uses PII collected from the public during *in extremis* situations. The keywords used to search publicly available social media sites on a regular basis expressly do not include PII.

FEMA Watch Centers may share their reports of information from social media sources with SLTT emergency management agencies to maintain timely, accurate, and actionable situational awareness of potential and actual incidents. This information sharing informs FEMA's counterparts of social media content pertinent to our partners' operations or impact and may also relate to *in extremis* situations when the appropriate responding authority should be notified. FEMA may share this information with its response partners via email or phone. If FEMA shares this information, the response partner is provided a disclaimer that the information contained in the email message or situation report is provided for official use only and any PII should not be saved, recorded, or shared outside the distribution list.

---

<sup>10</sup> The Watch Center duty logs in WebEOC may reference the transmission of information collected during *in extremis* situations since duty logs include "important events" that occur during a watch. Such entries only reference general location information; any PII is redacted prior to entering the information into WebEOC, such as "Forwarded to response authority location and name of individual trapped on roof in 5th Ward of New Orleans."



## Section 1.0 Authorities and Other Requirements

### 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- Section 515 of the Homeland Security Act,<sup>11</sup> established the NOC as the principal operations center for the Department, and charges it with providing situational awareness and a common operating picture for the entire Federal Government. FEMA provides situational awareness and aids in the establishment of a common operating picture for the Federal Government, and for SLTT governments, as appropriate;
- Section 503 of the Homeland Security Act,<sup>12</sup> broadly charges FEMA’s Administrator with developing and administering a program to prepare for and respond to all hazards, including (C), which charges FEMA with developing a federal response capability that can act effectively and rapidly to deliver assistance essential to saving lives or protecting property or public health and safety in an emergency. The activities described in this section require the visibility and coordination that is provided by FEMA Watch Centers;
- Section 504 of the Homeland Security Act,<sup>13</sup> which outlines the authorities and responsibilities of the FEMA Administrator, including developing a national emergency management system that is capable of preparing for, protecting against, responding to, recovering from, and mitigating against catastrophic incidents; and
- Section 503 of the Homeland Security Act,<sup>14</sup> which allows for the partnering with state, local, and tribal governments and emergency response providers, with other federal agencies, with the private sector, and with nongovernmental organizations to build a national system of emergency management that can effectively and efficiently utilize the full measure of the nation’s resources to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.<sup>15</sup>

### 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

FEMA is publishing a new System of Records Notice concurrent with this PIA.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

---

<sup>11</sup> 6 U.S.C. § 321d(b)(1).

<sup>12</sup> 6 U.S.C. § 313(b)(2)(A)-(H).

<sup>13</sup> 6 U.S.C. § 314(a)(17), describing responsibility for the NRCC under “Authority and responsibilities (of the FEMA Administrator).”

<sup>14</sup> 6 U.S.C. § 313(b)(2)(B).

<sup>15</sup> 6 U.S.C. § 313(c)(4)(A).



No. There is no underlying IT system for this initiative. The media sites that FEMA monitors, including the social media sites, are publicly available, third-party services.

#### **1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

FEMA's ORR is collaborating with FEMA Records Management Division and NARA to establish an approved retention and disposal policy for any records created through this initiative.

#### **1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

The information collected as part of this initiative is not covered by the Paperwork Reduction Act.

## **Section 2.0 Characterization of the Information**

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

#### **2.1 Identify the information the project collects, uses, disseminates, or maintains.**

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;
- 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).

## **2.2 What are the sources of the information and how is the information collected for the project?**

The sources of the information FEMA collects for its Operational use of Publicly Available Internet Social Media for Situational Awareness Initiative may include 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.

## **2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

Yes. As noted, FEMA uses publicly available data from third-party social media sources (those listed in Appendix A) to corroborate information from other official reporting channels or to report to the appropriate responding authority. This information is provided voluntarily by social media users. It is at the user's discretion to make this information available on a third party social media site.

## **2.4 Discuss how accuracy of the data is ensured.**

FEMA Watch Center analysts relies on information from third-party Internet social media services submitted voluntarily by users of those sites and compare it with information available through open source reporting, as well as a variety of public and government sources. Watch Center analysts attempt to provide a more accurate picture of on-the-ground activities by bringing together and comparing many different sources of information.

## **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk**: There is a risk that the information collected from social media is inaccurate.

**Mitigation**: This risk is partially mitigated. FEMA manages this risk by leveraging publicly available data posted on other social media and news services, as well as a variety of traditional media and government sources to corroborate the information it receives through its media monitoring activities. FEMA strives to collect the most relevant and accurate information but there is always a risk that publicly available data is inaccurate.

**Privacy Risk**: There is a risk that FEMA could collect PII through unauthorized interactions with the public or through unauthorized social media accounts.



**Mitigation:** FEMA partially manages this risk by adhering to the FEMA Web 2.0 Policy and DHS Privacy Policy for Operational Use of Social Media, which limits the creation and use of social media accounts for only authorized purposes. All social media account creation and use must be approved by the FEMA Office of External Affairs, in consultation with the OCIO, OCC, Privacy Office, and Records Management Division. The policy also requires that all FEMA social media accounts be clearly identified as FEMA-owned account. In addition, FEMA strictly limits social media interactions for situational awareness to FEMA Watch Centers. FEMA reinforces its policy of limiting PII collection only during *in extremis* situations by providing annual training and rules of behavior with Watch Center analysts so that they are aware of the appropriate use of social media. If PII is inadvertently distributed, FEMA recalls the message that was sent and sends a corrected version that is free of PII.

## Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

### 3.1 Describe how and why the project uses the information.

FEMA may collect the information listed in section 2.1 to provide situational awareness that supports accurate and timely decision making. This operation is neither designed nor intended to collect PII as a regular function. Rather, FEMA Watch Centers search publicly available sources and Internet-based platforms to understand the full scope of a situation.

FEMA uses the collected information to remain timely advised of a situation that potentially threatens life or property. FEMA may share critical, time sensitive, information from these efforts with federal and international partners as well as SLTT governments verbally, via email, or in paper-based report form to facilitate appropriate action by an agency with authority to respond to an incident or emergency situation.

Given the unpredictable scope of disasters, coupled with the voluntary and unrestricted nature of social media, it is possible during *in extremis* situations for FEMA Watch Centers to collect a limited amount of PII from the public in order to provide life-saving assistance to the individual. FEMA may collect an individual's name; social media user name, handle, or alias; address or approximate location; phone number, email address, or other contact information that is made publicly available on social media; and possibly details of the individual's relevant circumstances. FEMA sends the information through email to the appropriate entity that can assist in the situation, such as Urban Search and Rescue or an IMAT. FEMA does not store or retain the PII once the information is transmitted to the appropriate responding entity. FEMA provides the responding entity with a disclaimer indicating that information contained in the email message or situation report is provided for official use only and any PII should not be saved, recorded, or shared outside the distribution list. If FEMA includes the situation in a duty log report, it will redact any PII and only include general description of the situation and location information.<sup>16</sup>

---

<sup>16</sup> FEMA does not store or retain the PII once the information is transmitted to the appropriate responding entities. For





**3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.**

No.

**3.3 Are there other components with assigned roles and responsibilities within the system?**

Other DHS Components do not have assigned roles or responsibilities; however, FEMA shares all reports with the DHS NOC.

**3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a risk that FEMA could use the information for purposes other than that for which it was collected.

**Mitigation:** FEMA mitigates this risk by limiting the use of this information to only those in its Watch Centers that have a demonstrated “need to know,” and further limits the collection of this information to *extremis* situations. FEMA also leverages Internet social media training, privacy training, and rules of behavior to enforce its limits on the use of information collected through this initiative.

## Section 4.0 Notice

The following questions seek information about the project’s notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

**4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

FEMA is providing notice in this PIA and supporting SORN that it collects the information of individual’s during *in extremis* situations. FEMA also uses appropriate branding during its use of social media for this purpose. Additionally, FEMA has posted privacy notices and policies on its social media sites.

**4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?**

Members of the public voluntarily post publicly available information on social media sites or otherwise make information publicly available online. Individuals retain the right and the ability

---

example, Watch Center duty logs in WebEOC may reference the transmission of information collected during in *extremis* situations since duty logs include “important events” that occur during a watch. Such entries only reference general location information; any PII is redacted prior to entering the information into WebEOC, such as “Forwarded to response authority location and name of individual trapped on roof in 5th Ward of New Orleans.”



to refrain from making information public or, in most cases, to remove previously posted information from their respective social media accounts. In addition, individual users of social media may choose to keep private the information they share through their respective accounts. FEMA monitors Internet social media outlets and may collect and use information as necessary to promote the agency's situational awareness as described in this PIA.

An individual cannot "opt out" of this initiative once content is made publicly available through the various social media outlets, except under the circumstances discussed above. As noted above, individuals may adjust the privacy settings on their various social media platforms to avoid making information publicly available.

### **4.3 Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** There is a risk that individuals whose data is collected by FEMA during its media monitoring activities will not receive notice prior to the collection.

**Mitigation:** This risk is partially mitigated. FEMA provides notice in this PIA and supporting SORN, but it lacks a public education or awareness campaign that explains the FEMA may collect the information of individuals in *in extremis* situations.

Because it is difficult to provide notice to individuals prior to collection *in extremis* situations, FEMA takes other measures to provide transparency. FEMA clearly identifies all social media accounts as FEMA owned and operated. FEMA uses appropriate branding during its use of social media for this purpose. FEMA will only monitor social media for situational awareness purposes and will only review publicly posted information. FEMA encourages disaster victims to contact their local emergency management agencies for immediate assistance.

Social media users may change their privacy settings for their individual accounts or postings at any time, consistent with that website's policy. Additionally, FEMA has posted privacy notices and policies on its social media sites.

## **Section 5.0 Data Retention by the project**

The following questions are intended to outline how long the project retains the information after the initial collection.

### **5.1 Explain how long and for what reason the information is retained.**

As noted in section 1.4, FEMA is collaborating with NARA to establish an approved retention and disposal policy for any records created through this initiative. FEMA Watch Centers retain only user-generated information posted to publicly-available online social media sites. The reports that FEMA generates to provide situational awareness or establish a common operating picture become federal records and FEMA is required to maintain a copy. However, all PII from reports are redacted once the information is sent to the appropriate first responders *in extremis* situations.

The Watch Center duty logs in WebEOC may reference the transmission of information collected during *in extremis* situations since duty logs include "important events" that occur during a



watch. Such entries only reference general location information; any PII is redacted prior to entering the information into WebEOC, such as “Forwarded to response authority location and name of individual trapped on roof in 5th Ward of New Orleans.”

## **5.2 Privacy Impact Analysis: Related to Retention**

**Privacy Risk:** There is a risk that FEMA retains the information it collects for a longer period than is necessary.

**Mitigation:** While FEMA is working with NARA to establish an approved retention and disposal policy for any records created through this initiative, FEMA manages this risk by redacting all PII from reports prior to loading them into WebEOC. FEMA is drafting a retention policy that is in line with the mission-driven needs of the agency. Currently, FEMA follows the DHS NOC retention schedule of five years. In addition, FEMA leverages training and other documentation (such as standard operating procedures) to inform Watch Center personnel of proper record retention standards.

## **Section 6.0 Information Sharing**

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

### **6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.**

Yes. FEMA Watch Centers may share information from social media sources with state, local, and/or tribal emergency management agencies, in some instances. This information sharing informs FEMA’s counterparts of social media content pertinent to our partner’s operations or impact. It may also relate to *in extremis* situations where the appropriate responding authority should be notified. FEMA may share its situational awareness reports outside of DHS by email or phone. In these instances FEMA provides a disclaimer that the information contained in the email message or situation report is provided for official use only and any PII should not be saved, recorded, or shared outside the distribution list.

### **6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.**

FEMA only shares information collected through this initiative outside of FEMA in accordance with the routine uses published in the newly issued DHS/FEMA-013 Operational Use of Publicly Available Social Media for Situational Awareness System of Records. Typically, information (non-PII) is only shared externally to achieve FEMA’s situational awareness purposes for which the information was collected. Any PII shared through this initiative is used to address *in extremis* situations involving a potential loss of life.



### **6.3 Does the project place limitations on re-dissemination?**

The information is only shared externally to achieve FEMA’s situational awareness purposes for which the information was collected and to address *in extremis* situations involving a potential loss of life. FEMA only shares this information externally based on a strict “need to know” of its partner agencies. The partners are informed to limit re-dissemination of FEMA’s situational awareness reports to only those stakeholders with a demonstrated “need to know,” such as responding to a potential *in extremis* situation involving a potential loss of life. While the distribution of information gathered under this effort is intended to be limited, the point of this project is to rapidly disseminate information from public sources to help shape the situational awareness of key personnel at the federal, state, local and tribal levels of the homeland security enterprise. When FEMA’s sharing may result in email or phone communication outside of the agency, it provides a disclaimer that the information contained in the email message or situation report is provided for official use only and any PII should not be saved, recorded, or shared outside the distribution list.

### **6.4 Describe how the project maintains a record of any disclosures outside of the Department.**

As identified in the SORN listed under Section 6.2 above, requests for records associated with initiative should be made to the FEMA Disclosure Officer, which maintains the accounting of what records are disclosed and to whom.

### **6.5 Privacy Impact Analysis: Related to Information Sharing**

**Privacy Risk:** There is a risk that the information collected and disseminated under this initiative could be erroneously disclosed.

**Mitigation:** FEMA manages this risk by strictly limiting the sharing of this information according to the routine uses contained in the DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records, and to only those individuals who are involved as stakeholders of FEMA’s situational awareness information or who may have a role in responding during an *in extremis* situation involving the potential loss of life. Furthermore, information sharing allowed under this initiative is restricted to individuals requiring a “need to know” for the specific data.

## **Section 7.0 Redress**

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.



## **7.1 What are the procedures that allow individuals to access their information?**

A user can access his or her social media content at any time because this data is generated by the user. Specifically regarding FEMA, any individual who may desire to access whatever information FEMA may have collected under this initiative may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to the FEMA Disclosure Branch. The DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records contains instructions for accessing information under the “Notification Procedure” section.

## **7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

As noted above in Section 7.1, users of social media generate the content that FEMA reviews, may collect, and/or summarizes in its reports. The users may edit, delete, or modify the content under their control. Those persons included in the limited category of individuals about whom PII may be collected and who are seeking access to any record collected under this initiative may submit a FOIA or PA request. The DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records contains instructions for accessing information under the “Notification Procedure” section.

## **7.3 How does the project notify individuals about the procedures for correcting their information?**

FEMA notifies individuals of the redress procedures for this initiative through this PIA and through the DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness System of Records System of Records Notice.

## **7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** None, however, an individual whose information is collected and disseminated during *in extremis* situations will be unable to obtain redress prior to dissemination.

## **Section 8.0 Auditing and Accountability**

The following questions are intended to describe technical and policy based safeguards and security measures.

### **8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?**

FEMA ensures that the practices stated in this PIA are followed by leveraging training, policies, Rules of Behavior, information sharing access agreements, auditing, and accountability.





FEMA provides an annual, required training program to teach its analysts how to properly monitor publicly available social media sites in accordance with privacy and records policies. Furthermore, each analyst is required to sign a confirmation that he or she has received and understood the training. Each Watch Center location also has a point of contact for social media who ensures each staff member has appropriate training and is following the procedures in this PIA.

## **8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.**

A regularly scheduled training program is in place to teach Watch Center analysts how to properly monitor publicly available social media sites and to do so in accordance with privacy and records policies. This training is an annual requirement for Watch Center analysts, and each analyst must sign a confirmation that he/she has received and understood the training. The annual training is made up of two parts: 1) individual review of privacy awareness training and Operational Use of Social Media slides; and 2) participation in interactive training conducted via Adobe Connect.

## **8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?**

For the majority of social media monitoring activities that do not collect PII, information is available to Watch Center and ORR staff with a “need to know”. This information is disseminated through FEMA’s email systems, in accordance with FEMA Directive 262-2, “Information Transmitted Via Email.” During *in extremis* situations when PII is put into an email and recorded, only users with a “need to know” are given the information. As noted above, this could include the appropriate responding authority at the state, local, or tribal level. This may result in email or phone communication outside of FEMA’s system, with a disclaimer that the information contained in the email message or situation report is provided for official use only, and any PII should not be saved, recorded, or shared outside the distribution list.

## **8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?**

Currently, this initiative does not require information sharing agreements or MOUs; however, the project has a process to review such agreements as necessary. This process involves program stakeholders, the Office of Chief Counsel, and the FEMA Privacy Office. Similarly, FEMA leverages its stakeholders in the process of reviewing and approving any new uses for the project. If FEMA contemplates new uses for the initiative or its information, the agency will update the required privacy compliance documentation.

## **Responsible Officials**

Eric M. Leckey



Privacy Officer  
Federal Emergency Management Agency  
U.S. Department of Homeland Security

## **Approval Signature**

Original signed copy on file with the DHS Privacy Office.

---

Karen L. Neuman  
Chief Privacy Officer  
U.S. Department of Homeland Security



APPENDIX A:

Publicly Available Sites Monitored by FEMA

(Updated July 2023)

This is an illustrative, but not exhaustive, list of sites that FEMA ORR and OEA may monitor in order to provide situational awareness and establish a common operating picture. Initial sites listed may link to other sites not listed. FEMA may also monitor those sites if they are within the scope of this Initiative.

This list is divided into two sections: Sites Monitored and Monitoring Tools. Sites Monitored contains social media websites with user generated posts that may be monitored by FEMA employees conducting searches, while Monitoring Tools aggregate social media posts from the Sites Monitored to make it easier to review search results.

Monitoring Tools	Link	User/Password Required
Hootsuite	<a href="https://hootsuite.com">https://hootsuite.com</a>	Yes
Crowdtangle	<a href="https://crowdtangle.com">https://crowdtangle.com</a>	Yes
Brandwatch	<a href="https://brandwatch.com">https://brandwatch.com</a>	Yes
Tweetdeck	<a href="https://tweetdeck.twitter.com">https://tweetdeck.twitter.com</a>	Yes
Trends Map	<a href="https://www.trendsmap.com">https://www.trendsmap.com</a>	Yes

Sites Monitored	Link	User/Password Required
<b><u>Social Media</u></b>		
Facebook	<a href="https://www.facebook.com">https://www.facebook.com</a>	Yes
Twitter	<a href="https://www.twitter.com">https://www.twitter.com</a>	No
Instagram	<a href="https://www.instagram.com">https://www.instagram.com</a>	Yes
LinkedIn	<a href="https://www.linkedin.com">https://www.linkedin.com</a>	Yes
Nextdoor	<a href="https://nextdoor.com">https://nextdoor.com</a>	Yes
Pinterest	<a href="https://www.pinterest.com">https://www.pinterest.com</a>	Yes

<b><u>Video</u></b>		
Vimeo	<a href="https://www.vimeo.com">https://www.vimeo.com</a>	No
YouTube	<a href="https://www.youtube.com">https://www.youtube.com</a>	No



## Maps

Global Incident Map	<a href="https://globalincidentmap.com">https://globalincidentmap.com</a>	No
Google Flu Trends	<a href="https://www.google.org/flutrends/">https://www.google.org/flutrends/</a>	No
GasBuddy	<a href="https://tracker.gasbuddy.com/">https://tracker.gasbuddy.com/</a>	No
Health Map	<a href="https://www.healthmap.org/en">https://www.healthmap.org/en</a>	No
Stormpulse	<a href="https://www.stormpulse.com">https://www.stormpulse.com</a>	No

## Photos

Flickr	<a href="https://www.flickr.com">https://www.flickr.com</a>	No
--------	---	----



## APPENDIX B:

### FEMA Keyword Search Terms for Publicly Available Social Media

*(Updated July 2023)*

This is a current list of terms that may be used when monitoring social media sites to provide situational awareness and establish a common operating picture. The program conducts searches for and analyzes discussions related to a range of topics about FEMA programs and events that the agency has authority to respond to. Due to the unpredictable nature of disaster response and the variety of non-Stafford Act incidents that FEMA may also support responses to, specific keywords being searched may vary and be altered throughout the course of a response to ensure resulting analysis may be thorough and effective. As natural or manmade disasters occur, new search terms may be added. The new search terms do not use Personally Identifiable Information (PII) in searching for relevant mission-related information.

#### *Domestic Security*

Assassination  
Attack  
Authorities  
Blast  
Bomb  
Cops  
Crowd  
DNDO (Domestic Nuclear Detection Office)  
Domestic nuclear detection  
Domestic security  
Drill  
Emergency management  
Emergency response  
Exercise  
Explosion(s)  
Fired  
First responder  
Gathering  
Gunfire  
Gunshots  
Homeland security  
Law enforcement  
Lone wolf  
Maritime domain awareness (MDA)  
Shots  
Shooter  
Terrorist  
Terrorism  
Threaten  
Threatened





Threatening  
Truck  
Van

## **HAZMAT & Nuclear**

Anthrax  
Biological Epidemic Hazardous  
Biological infection (or event)  
Chemical Burn  
Cloud  
Facility  
Gas  
Hazardous material incident  
Hazmat Nuclear Spill  
Industrial spill Infection Powder(white)  
Leak  
National laboratory Nuclear  
Package/device  
Plume  
Radiation Radioactive  
Spillover  
Suspicious  
Toxic

## **Health Concern**

Agriculture Listeria Symptoms  
Agro Terror Tuberculosis (TB)  
Anthrax Blister agent  
Antiviral  
Avian Flu  
Bacteria  
Center for Disease Control (CDC)  
Chemical agent Exposure  
Contamination  
Coronavirus  
COVID  
COVID19  
COVID-19  
Diagnosed  
Drug Administration (FDA)  
E. Coli  
Ebola  
Emergency Department  
Emergency Room  
Epidemic  
Exposed  
Exposing



First report  
Food Poisoning  
Foot and Mouth (FMD) H5N1  
H1N1  
H2H  
Hospital  
Human to Animal Influenza  
Human to human  
Infection  
Medical Center  
Mutation  
Nerve agent Ricin  
North Korea Outbreak  
Norvo Virus  
Nursing home  
Pandemic  
Patient(s)  
Pork  
Public Health Toxic  
Quarantine  
Recall  
Resistant  
Salmonella Smallpox Plague  
Sarin  
Sick  
Strain  
Swine  
Tamiflu  
Vaccinated  
Vaccination  
Vaccine  
Vaccine  
Viral Hemorrhagic Fever  
Virus  
Water/air borne  
Wave  
World Health Organization (WHO) (and components)

## **Infrastructure Security**

Airplane (and derivatives)  
Airport  
AMTRAK  
Bank(s)  
BART  
Black out  
Blocked  
Body scanner  
Brown out Port



Bus(es)  
Cancelled Delays  
Chemical fire  
CIKR (Critical Infrastructure & Key Resources)  
Closed  
Collapse  
Communications infrastructure  
Computer infrastructure  
Dam(s)  
Dock Bridge  
Downed  
Electric  
Electricity  
Failure  
Gas station  
Grid  
Grocery store  
Highway  
Infrastructure  
Infrastructure security  
Levee(s)  
MARTA  
Metro  
NBIC (National Biosurveillance Integration Center)  
Outage  
Port Authority  
Power lines  
Power plant  
Power Smart  
Public transportation  
Road  
Service disruption  
Subway  
Telecommunications  
Transportation security  
Water treatment  
WMATA

## **Weather/Disaster/ Emergency**

911  
Avalanche  
Blizzard  
Burst  
Closure  
Collapse  
Crest  
Damage(d)  
Destroy(ed)



Destruction  
Disaster  
Donated  
Donation(s)  
Earthquake  
Emergency  
Emergency  
Erosion  
Evacuate  
Evacuated  
Evacuating  
Evacuation  
Extreme weather  
Fire  
Flood  
Flooded  
Flooding  
Floods  
Hail  
Hurricane  
Ice  
Interstate  
Lightening/Lightning  
Magnitude  
Mandatory  
Missing  
Mold  
Muck(ing)  
Mud slide/ Mudslide  
Prepare(d)  
Quake  
Ready  
Rescue  
Rescue(d)  
Ripped  
River  
Roof  
Search and rescue  
Shelter(s) Loss(es)  
Shelter-in-place  
Sleet  
Snow  
Storm  
Storm surge  
Stranded  
Stuck  
Supplies  
Supply  
Task force



Temblor  
Tore  
Tornado(es)  
Trapped  
Tremor  
Tsunami  
Twister  
Typhoon  
USAR  
Volunteer(s)  
Volunteered  
Volunteering  
Warning  
Watch  
Wildfire

## **Federal Disasters**

Aid  
Appeal  
Appealing  
Application  
Apply  
Declaration  
Denied  
Disaster assistance  
Disaster management  
Distributed  
Distribution  
DRC  
Federal emergency  
FEMA  
FIMA  
Mitigation  
National preparedness  
Prevention  
Recovery  
Register  
Registered  
Registration  
Rejected  
Relief  
Response

## **Cyber Security**

Cyber terror  
Cyber attack  
Hacker





## *Equity/Vulnerable Populations*

Access  
Accessibility  
ASL  
Assisted living  
Autistic  
Blind  
Deaf  
Dementia  
Diabetes  
Dialysis  
Disability  
Disabled  
Elderly  
Functional needs  
Handicapped  
Insulin  
Low income  
Medical equipment  
Medication  
Nursing home  
Senior  
Sign language  
Vision impaired  
Vulnerable  
Wheelchair



## **APPENDIX C:**

### ***In Extremis* Examples Where PII May Be Collected**

- 1) “Two users in the area (location), @username and @username, claim their family members are trapped in a collapsed building.”
- 2) “User @username is reporting significant flooding in his neighborhood (location). User claims to be in the area and stuck on the roof of the house with no way to evacuate”