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[1] and to assist the DHS National Operations Center (NOC)[2] 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[3] in support of the FEMA Administrator's responsibility under the Homeland Security Act[4], and to assist the DHS 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 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 continual cycle of information collection,

[1] 6 U.S.C. § 313(c)(4)(A)
[2] 6 U.S.C. § 321d(b)(1)
[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. § 321d(b)(1)
[6] 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_Apri

analysis, and 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.[7] 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."[8] 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

---

l2013.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.

[7] FEMA's mission is defined in Section 503 of the Homeland Security Act of 2002, *as amended*.

[8] https://www.dhs.gov/xlibrary/assets/foia/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf

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.[9]

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 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.[10] 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

[9] 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.

[10] 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."

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.

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,[11] 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,[12] 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,[13] 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,[14] 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

[11] 6 U.S.C. § 321d(b)(1).
[12] 6 U.S.C. § 313(b)(2)(A)-(H).
[13] 6 U.S.C. § 314(a)(17), describing responsibility for the NRCC under "Authority and responsibilities (of the FEMA Administrator)."
[14] 6 U.S.C. § 313(b)(2)(B).

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.[15]

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?

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:

[15] 6 U.S.C. § 313(c)(4)(A).

- 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 medial 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.[16]

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.

[16] FEMA does not store or retain the PII once the information is transmitted to the appropriate responding entities. For 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."

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 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 Watch Centers

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

General Search Tool	Link	User/Password Required
Collecta	http://collecta.com	No
Cable News Network	http://cnn.com	No
RSSOwl	http://www.rssowl.org/	No
Social Mention	http://socialmention.com/	No
Spy	http://www.spy.appspot.com	No
Who's Talkin	http://www.whostalkin.com/	No
Shrook RSS reader	http://www.utsire.com/shrook/	No
Video		
Hulu	http://www.hulu.com	No
iReport.com	http://www.ireport.com/	No
Live Leak	http://www.liveleak.com/	No
Magma	http://mag.ma/	No
Time Tube	http://www.dipity.com/mashups/timetube	No
Vimeo	http://www.vimeo.com	No
Youtube	http://www.youtube.com	No
MySpace Video	http://vids.myspace.com/	No
Maps		
Global Incident Map	http://globalincidentmap.com/	No
Google Flu Trends	http://www.google.org/flutrends/	No

Health Map	http://www.healthmap.org/en	No
IBISEYE	http://www.ibiseye.com/	No
Stormpulse	http://www.stormpulse.com/	No
Trends Map	http://www.trendsmap.com	No

Photos

Flickr	http://www.flickr.com/	No
Picfog	http://picfog.com/	No
Twicsy	http://www.twicsy.com	No
Twitcaps	http://www.twitcaps.com	No
Twitter/API Twitter/API	http://www.twitter.com	Yes

Twitter Search

Monitter	http://www.monitter.com/	No
Twazzup	http://www.twazzup.com	No
Tweefind	http://www.tweefind.com/	No
Tweetgrid	http://tweetgrid.com/	No
Tweetzi	http://tweetzi.com/	No
Twitter Search	http://search.twitter.com/advanced	No

Twitter Trends

Newspapers on Twitter	http://www.newspapersontwitter.com/	No
Radio on Twitter	http://www.radioontwitter.com/	No
Trendistic	http://trendistic.com/	No
Trendrr	http://www.trendrr.com/	No
TV on Twitter	http://www.tvontwitter.com/	No
Tweet Meme	http://tweetmeme.com/	No
TweetStats	http://tweetstats.com/	No

Twellow	http://www.twellow.com/	No
Twendz	http://twendz.waggeneredstrom.com/	No
Twitoaster	http://twitoaster.com/	No
Twitscoop	http://www.twitscoop.com/	No
Twitturly	http://twitturly.com/	No
We Follow	http://wefollow.com/	No
Facebook		
It's Trending	http://www.itstrending.com/news/	No
Facebook	http://www.facebook.com	Yes
MySpace	http://www.myspace.com	Yes
MySpace (limited search)	http://www.myspace.com	No
Blogs		
ABCNews Blotter	http://abcnews.go.com/Blotter/	No
al Sahwa	http://al-sahwa.blogspot.com/	No
AllAfrica	http://allafrica.com/	No
Avian Flu Diary	http://afludiary.blogspot.com/	No
BNOnews	http://www.bnonews.com/	No
Borderfire Report	http://www.borderfirereport.net/	No
Borderland Beat	http://www.borderlandbeat.com/	No
Brickhouse Security	http://blog.brickhousesecurity.com/	No
Chem.Info	http://www.chem.info/default.aspx	No
Chemical Facility Security News	http://chemical-facility-security-news.blogspot.com/	No
ComputerWorld	http://www.computerworld.com/s/topic/82/Cybercrime+and+Hacking	No
Counter-Terrorism Blog	http://www.counterterrorismblog.com/	No

Crisisblogger	http://crisisblogger.wordpress.com/	No
Cryptome	http://cryptome.org/	No
Danger Room	http://www.wired.com/dangerroom/	No
Drudge Report	http://drudgereport.com/	No
El Blog Del Narco	http://elblogdelnarco.blogspot.com/	No
Emergency Management Magazine	http://www.emergencymgmt.com	No
Foreign Policy Passport	http://blog.foreignpolicy.com/	No
Global Security Newswire	http://gsn.nti.org/gsn/	No
Global Terror Alert	http://www.globalterroralert.com/	No
Global Voices Network	http://globalvoicesonline.org/-/world/americas/haiti/	No
Google Blog Search	http://blogsearch.google.com	No
Guerra Contra El Narco	http://guerracontraelnarco.blogspot.com/	No
H5N1 Blog	http://crofsblogs.typepad.com/h5n1/	No
Homeland Security Today	http://www.hstoday.us/	No
Homeland Security Watch	http://www.hlswatch.com/	No
Huffington Post	http://huffingtonpost.com/	No
Hurricane Information Center	http://gustav08.ning.com/	No
HurricaneTrack	http://www.hurricanetrack.com/	No
InciWeb	http://www.inciweb.org/	No
Informed Comment	http://www.juancole.com/	No
Jihad Watch	http://www.jihadwatch.org/	No
Krebs on Security	http://krebsonsecurity.com/	No
LA Now	http://latimesblogs.latimes.com/lanow/	No
LA Wildfires Blog	http://latimesblogs.latimes.com/lanow/wildfires/	No
Livesay Haiti Blog	http://livesayhaiti.blogspot.com/	No
LongWarJournal	http://www.longwarjournal.org/	No
Malware Intelligence Blog	http://malwareint.blogspot.com/	No
MEMRI	http://www.memri.org/	No

MexiData.info	http://mexidata.info/	No
MS-13 News and Analysis	http://msthirteen.com/	No
Narcotrafico en Mexico	http://narcotraficoenmexico.blogspot.com/	No
National Defense Magazine	http://www.nationaldefensemagazine.org	No
National Terror Alert	http://www.nationalterroralert.com/	No
NEFA Foundation	http://www.nefafoundation.org/	No
Newsweek Blogs	http://blog.newsweek.com/	No
Nuclear Street	http://nuclearstreet.com/blogs/	No
NYTimes Lede Blog	http://thelede.blogs.nytimes.com/	No
Plowshares Fund	http://www.ploughshares.org/news-analysis/blog/	No
Popular Science Blogs	http://www.popsci.com/	No
Port Strategy	http://www.portstrategy.com/	No
Public Intelligence	http://publicintelligence.net/	No
ReliefWeb	http://www.reliefweb.int	No
RigZone	http://www.rigzone.com/	No
Science Daily	http://www.sciencedaily.com/	No
STRATFOR	http://www.stratfor.com/	No
Technorati	http://technorati.com/	No
Terror Finance Blog	http://www.terrorfinance.org/the_terror_finance_blog/	No
The Latin Americanist	http://ourlatinamerica.blogspot.com/	No
Threat Level	http://www.wired.com/threatlevel/	No
Threat Matrix	http://www.longwarjournal.org/threat-matrix/	No
Tickle the Wire	http://www.ticklethewire.com/	No
Tribuna Regional	http://latribunaregional.blogspot.com/	No
TruckingInfo.com	http://www.truckinginfo.com/news/index.asp	No
United Nations IRIN	http://www.irinnews.org/	No
Ushahidi Haiti	http://haiti.ushahidi.org/	No
War on Terrorism	http://terrorism-online.blogspot.com/	No

WikiLeaks	http://wikileaks.org/	No
WireUpdate	http://wireupdate.com/	No

APPENDIX B:

FEMA Keyword Search Terms for Publicly Available Social Media

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. 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

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

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

Epidemic

Hazardous

Hazardous material incident

Industrial spill

Infection

Powder (white)

Gas

Spillover

Health Concern + H1N1

Anthrax

Blister agent

Chemical agent

Exposure

Burn

Nerve agent

Ricin

Sarin

North Korea

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
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
Airplane (and derivatives)
Chemical fire
CIKR (Critical Infrastructure & Key Resources)
AMTRAK
Collapse
Computer infrastructure
Communications infrastructure
Telecommunications
Critical infrastructure
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
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
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
Botnet
DDOS (dedicated denial of service)
Denial of service
Malware
Virus
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

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 the area.