The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement[1]:

a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications);

b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

[1] Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: February 20, 2018

Name of Component: Federal Emergency Management Agency

Contact Information: Christopher Blaz, Director, National Watch Center; Christopher.blaz@fema.dhs.gov; (b)(6)

Counsel[2] Contact Information: Robert Parker, Robert.parker@fema.dhs.gov; (b)(6)

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

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

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

[2] Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. **Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.**

   Background:

   The Federal Emergency Management Agency (FEMA), Office of Response and Recovery (OR&R), Response Directorate, operate FEMA's Watch Centers. These Watch Centers include the National Response Coordination Center (NRCC), the National Watch Center (NWC), ten Regional Response Coordination Centers (RRCCs), and ten Regional Watch Centers (RWCs). The FEMA Watch Centers' mission is to maintain timely, accurate, and actionable situational awareness of potential and actual incidents that may require a coordinated federal response to support FEMA and DHS leadership. They accomplish this mission through a continual cycle of information collection and analysis, report generation and dissemination, and collaboration with federal, state, local, and tribal stakeholders. This involves 2-way information sharing between stakeholders via email, phone, fax, video teleconference, and various information management systems. SharePoint, for example, is used for document sharing between Watch Centers similar to how the DHS Homeland Security Information Network (HSIN) is used to share documents throughout DHS and the interagency. The information provided by the FEMA Watch Centers support incident management and helps DHS fulfill its statutory responsibility under 6 U.S.C. § 313(b)(2)(a)-(h) to lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents. In addition, 6 U.S.C. § 321d(b)(1) provides responsibilities for situational awareness in the event of a natural disaster, while 6 U.S.C. §314(a)(17) makes FEMA responsible for the NRCC, and thusly, its role in providing situational awareness.

Purpose:

The purpose of this project is the collection of information from publically available traditional media, such as newspapers and television news, and new media sources, such as social media sites, websites, and blogs for situational awareness and to correlate with other FEMA reports. The FEMA Watch Centers operate 24/7 in 12 hour shifts and at any time during their shift, watch team members will manually search the internet using search terms to find out if there are any potential incidents or to gather amplifying information regarding ongoing incidents that may predicate a coordinated federal response. Information from the DHS National Operations Center (NOC) Media Monitoring

Reports, TV news broadcasts, official reports from local and/or state representatives, etc. may also act as a trigger for the FEMA Watch Centers to search for information.

FEMA will only view content that is accessible on public sites and will not access or view content behind locked accounts or where permission is needed in order to see the content.

FEMA will not collect or save content that is copyrighted, including, but not limited to, text, photos, or videos. In addition, FEMA will not collect, save, or record the actual posts of social media users. The information that FEMA could include in its reports includes: date, time, location, a synopsis of subject/content, and a link back to the source(s). The personally identifiable information (PII) that may be referenced is a person's public name, social media account, and/or additional contact information (email address/phone number), as it relates to the specific emergency situation because of the value in the information the person is posting publicly and/or because the person is in danger. Also, free text input provided by the social media users, such as status updates or tweets, could include PII, may be captured. FEMA may save this information in a document, spreadsheet, or report to ensure information is not lost, especially for those in danger. FEMA's situational awareness reports are not retrievable by PII, but by date and time group.

FEMA Watch Centers will use separate social media accounts from those used by the Office of External Affairs (EA), and all accounts will be approved by EA before they are created. All FEMA Watch Centers social media accounts will be clearly marked and identified as official FEMA accounts with a link to fema.gov, and a page on fema.gov will list all official accounts for the benefit of the public. The FEMA Watch Centers social media accounts will follow relevant emergency managers, agencies, organizations, and mission specific accounts.

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

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

6 U.S.C. § 313(b)(2)(a)-(h) "Federal Emergency Management Agency"

6 U.S.C. § 321d (b) (1) "National Operations Center"

6 U.S.C. §314(a) (17) "Authority and responsibilities (of the FEMA Administrator)"

a) Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?

☒ Yes. ☐ No.

3. Is this use of social media in development or operational?

☐ In development. ☒ Operational. Date first launched: May 2011

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

Included

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

a) *Equipment*. Use only government-issued equipment when engaging in the operational use of social media;

☒ Yes. ☐ No. If not, please explain:

b) *Email and accounts*. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

☒ Yes. ☐ No. If not, please explain:

c) *Public interaction*. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

☒ Yes. ☐ No. If not, please explain:

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

☒ Yes. ☐ No. If not, please explain:

e) *PII collection*: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

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

☒ Yes. ☐ No. If not, please explain:

g) *Documentation*. Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ Yes. ☐ No. If not, please explain:

h) *Training*. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 3/7/18

NAME of the DHS Privacy Office Reviewer: Hannah Burgess

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

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

SORN: DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness

1. **Category of Use:**

☐ Law Enforcement Intelligence;

☐ Criminal law enforcement investigations;

☐ Background investigations;

☐ Professional responsibility investigations;

☐ Administrative or benefit determinations (including fraud detection);

☒ Situational awareness; and

☐ Other. <Please explain "other" category of use here.>

2. **Has Component Counsel reviewed and determined that there is authority to engage in the above Category of Use?**

☒ Yes. ☐ No.

3. **Rules of Behavior Content: (Check all items that apply.)**

a. *Equipment.*

☐ Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

☒ Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. *Email and accounts*.

☐ Users do not have to use government email addresses or official DHS accounts online.

☒ Users must use government email addresses or official DHS accounts online.

c. *Public interaction*.

☐ Users may interact with individuals online in relation to a specific law enforcement investigation.

☒ Users may NOT interact with individuals online.

d. *Privacy settings*.

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage*:

☐ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here:

☒ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards*.

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☒ Only a minimal amount of PII is collected and safeguarded, consistent with DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative.

g. *Documentation*.

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training*.

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No, certification of training completion cannot be verified.

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☐ A PIA is required.

☐ New.

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

☐ A SORN is required:

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

FEMA is submitting this SMOUT to document its use of social media. The operational use of social media information and the manner in which PII is observed and/or acted upon in extremis situations has not changed. The DHS Privacy Office determines that FEMA has provided sufficient documentation to demonstrate compliance with MD 110-01.

Appendix A: Rules of Behavior

Rules of Behavior
Social Media Monitoring For Situational Awareness

I. Background

FEMA Watch Centers maintain timely, accurate, and actionable information for situational awareness of potential and actual incidents that may require a coordinated federal response to support DHS and FEMA leadership and the DHS National Operations Center (NOC). The term "Watch Centers" incorporates all FEMA watch and coordination center capabilities including: the National Watch Center (NWC), the National Response Coordination Center (NRCC) (under the authority of 6 U.S.C. §314(a) (17)), ten Regional Watch Capabilities (RWCs), ten Regional Response Coordination Centers (RRCCs), and five Mobile Emergency Response Support (MERS) Operations Centers (MOC). Situational Awareness, for the purposes of this document, is defined as a state of understanding from which decisions can be made. FEMA Watch Centers develop situational awareness based on information gathered from a variety of sources, including social media, and communicate the information to DHS and FEMA leadership, the DHS NOC, federal, state, local, and interagency partners, and stakeholders to form the basis for incident management decision-making.

FEMA Watch Centers maintain situational awareness through a continual cycle of information collection, analysis, and collaboration with federal, state, local, and interagency partners. Monitoring of social media by FEMA Watch Centers has two purposes. The first is to provide critical situational awareness to assist FEMA in fulfilling its statutory responsibility under 6 U.S.C. § 313(b)(2)(a)-(h) to lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents. The second purpose is to provide assistance to the DHS NOC in furtherance of its role as the principal operations center for the Department and in furtherance of its responsibility to provide situational awareness and a common operating picture for the entire Federal Government, and for state, local, and tribal governments, as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster, and ensuring that critical terrorism and disaster-related information reaches government decision-makers, as provided for in Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

II. Purpose

In accordance with DHS Instruction 110-01-001, this document covers the rules of behavior that must be followed by any analyst using social media for situational awareness purposes in FEMA Watch Centers. This includes the monitoring and reporting of publicly available traditional and new media (inclusive of social media) for situational awareness. These rules cover general internet searches that include social media results such as blogs

or Twitter feeds, the use of social media aggregators, and the use of publicly visible FEMA branded social media accounts that have been approved by FEMA's Office of External Affairs (EA).

III. Rules of Behavior

1) Equipment – FEMA Watch Centers may only use government-issued equipment when engaging in official monitoring of social media for situational awareness. Personal equipment may only be used for personal use of social media.

2) Social Media Accounts – Official FEMA Watch Centers branded social media accounts will be created after FEMA HQ External Affairs (EA) approval. Personal accounts are for personal use only in accordance with FEMA Directive 262-3 (FEMA Web 2.0 Policy).

    a. FEMA Watch Centers may use their official, EA approved accounts to follow social media users that fall into these categories:

        i. Emergency managers/agencies
        ii. Official government (state/local/tribal/territorial) personnel/agencies
        iii. Weather, news anchors, and news agencies
        iv. Known subject matter experts including disaster/emergency management volunteers and professionals such as civilian/public tornado spotters, CERT members, etc.

    b. FEMA Watch Centers shall not follow accounts in these categories:

        i. Private Individuals
        ii. Blocked Accounts
        iii. Accounts affiliated with a political party or campaign

3) Public Interaction – FEMA Watch Centers are prohibited from interacting with members of the public in their capacity as employees of FEMA when on duty in a FEMA Watch Center. EA approved social media accounts for FEMA Watch Centers are for monitoring only, to be used in accordance with the guidance in this document. Specifically, the following actions are prohibited:

    a. Posting messages using official, EA approved, social media accounts

b. Responding to posts, tweets, blogs, or other types of messages via social media. This does not include normal FEMA Watch Center communications protocols regarding telephone and email
c. Using personal social media accounts to conduct official FEMA Watch Center business

4) Privacy Settings – FEMA Watch Centers use of social media is limited to publicly available sites and sources. FEMA Watch Centers shall not access private or blocked information or sign up for any social media accounts not authorized by EA.

5) Personally Identifiable Information (PII) Collection – FEMA Watch Center's monitoring of publicly available traditional and Social Media is not designed to collect, store, or disseminate PII. PII is defined by the Office of Management and Budget as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (M-07-16). At no time should a person's name, address, date of birth, phone number, or address be recorded except in *in extremis* situations:

   a. During *in extremis* situations involving potential loss of life, FEMA Watch Centers may share the minimum PII necessary with a response authority via email, phone, or other immediate means of communication, in order to assist them in rendering emergency aid. This information may include the name of a person/s requesting help, their location, and contact information, among other relevant data points. Specific examples can be found in Appendix 1 "Scenarios for PII Collection in Extremis Circumstances".

   b. In no instance will FEMA Watch Centers create a permanent record with an individual's PII. However, FEMA Watch Centers duty logs may reference transmission of *in extermis* information. Such entries should only reference general location information, such as "forwarded to response authority location and name of individual trapped on roof in 5th Ward of New Orleans."

6) PII Safeguards – FEMA Watch Centers shall protect PII in accordance with the privacy law and policy framework at all times.

a. As mentioned in item 5 above, names (both social media handles and given names), positions, contact information, or other data points that might make it possible to identify an individual may only be included in reports related to *in extremis* situations. Only the minimum PII necessary for the proper performance of authorized duties will be used.

b. Addresses, such as "1234 Main Street," or approximate locations, such as the name of a neighborhood or town, may be included in the report or generalized to street blocks, such as "1200 block of Main Street." This information will also only be included *in extremis* situations, as noted in item 5 above.

7) Documentation – FEMA Watch Centers do not record or otherwise save social media posts, however, they are used for situational awareness. Links to a social media resource will be included in a list of open source resources, such as national social media, as shown in Appendix 2. For the purpose of distribution, the following rules apply to the inclusion of social media related information:

   a. Reports may only include a synopsis of the situation or issue being described, they may not directly reference or quote from a social media post.

   b. Links to social media posts used to inform a situational report may be included with links to other open sources such as national social media websites.

8) Training – the FEMA National Watch Center, FEMA Privacy Office, and FEMA Office of External Affairs are working together to provide training for all FEMA Watch Center personnel regarding the monitoring of publicly available traditional and social media for situational awareness. FEMA Watch Center personnel will be given training before using any publicly viewable social media accounts, and the training will be made available on an ongoing basis through the FEMA intranet. The annual training will include:
   a. Proper documentation of information to minimize and protect PII
   b. Rules of behavior listed here
   c. Use of official/EA approved accounts

9) If a FEMA Watch Center comes across a post/blog/etc that may require action from FEMA External Affairs, those posts should be forwarded to:
   a. From FEMA NWC/NRCC to FEMA-NEW-MEDIA@fema.gov

IV. Authorities

1) 6 U.S. C. § 313(b)(2)(a)-(h) "Federal Emergency Management Agency"
2) 6 U.S.C. § 321d(b)(1) "National Operations Center"
3) 6 U.S.C. §314(a)(17) "Authority and responsibilities (of the FEMA Administrator)"

APPENDIX 1: Scenarios for PII Collection in Extremis Circumstances

As mentioned above in Section III, 5, a, monitoring social media for situational awareness is not intended to collect, distribute, or store PII. However, in some extreme cases involving potential loss of life, FEMA Watch Centers may report on a social media user names, location, or other potentially identifiable information contained in a user's social media posts. Only the minimum PII necessary for performance of official duties will be used and such PII will be safeguarded and handled in accordance with the privacy law and policy framework at all times.

The following examples demonstrate how FEMA Watch Centers may collect this information in extreme cases and include potential PII in situational reports:

1) "Several users on Twitter are reporting earthquake damage at or near (location). Two users, who claim to be in the area, @username and @username, claim the apartment building across the street was flattened. We are working to verify this information through official channels."

2) "Not much activity on social media regarding coastal damages related to hurricane (name). However, a user claiming to be in (isolated location) has been posting photos of damages and claiming that water is rising while other people remain in the affected area."

3) "While traditional media reports are mentioning power outages in areas affected by the (location) severe storms, a few social media users claiming to be in the affected area are reporting a lack of water and basic services. @username, @username, and @username have said they do not have access to water and have no access to transportation. We are making our state and local counterparts aware of these reports in case further response is needed."

4) "Social media users are commenting on the dangerous rain and wind creating by hurricane (name). FEMA Watch Center officers have seen two social media posts from those claiming to be trapped in their home after not following local evacuation orders. As of (date), here are links to the two messages:

www.twitter.com/username/status/XXXXX
www.twitter.com/username/status/XXXXX

This information is being routed to our regional, state, and local counterparts in case further response is needed."

APPENDIX 2: Sample of a FEMA Watch Center Report

FEMA Region VI reported that the University of Somewhere has ordered an immediate evacuation due to a bomb threat that was called in this morning. The timeline the caller threatened to set the bomb off has already passed, however, buildings remain evacuated while the threat is being investigated. Multiple news agencies are reporting on the evacuation, and the University issued the immediate evacuation notice via twitter and other media. University of Somewhere public affairs released a statement stating that the caller had a middle eastern accent, stated he was with Al Qaeda, and that there were bombs in multiple buildings around the campus.

The FEMA Watch Center will continue to monitor and pass any additional information as it becomes available.

For more information see:
www.gonzalescannon.com
www.news.blogs.cnn.com
www.somewherenews.com
@UniversitySomewhere

APPENDIX B: Keywords

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

HAZMAT & Nuclear (cont'd)
Biological infection (or event)
Chemical
Chemical burn
Biological
Epidemic
Hazardous
Hazardous material incident
Industrial spill
Infection
Powder (white)
Gas
Spillover
Anthrax
Blister agent
Chemical agent
Exposure
Burn
Nerve agent
Ricin
Sarin
North Korea

Health Concern + H1N1
Outbreak
Contamination
Exposure
Virus
Evacuation
Bacteria
Recall
Ebola
Food Poisoning
Foot and Mouth (FMD)
H5N1
Avian
Flu
Salmonella

Health Concern + H1N1 (con't)

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

Airport (Regional and abbreviations)
Airplane (and derivatives)
Chemical fire
CIKR (Critical Infrastructure & Key Resources)
AMTRAK
Collapse
Computer infrastructure
Communications infrastructure
Telecommunications
Critical infrastructure (local and regional)
National infrastructure
Metro
WMATA
Subway
BART
MARTA
Port Authority
NBIC (National Biosurveillance Integration Center)
Transportation security
Grid
Power
Smart
Body scanner
Electric
Failure or outage
Black out
Brown out
Port
Dock
Bridge
Cancelled
Highway names and numbers
Bridge names
Key local infrastructure names

Infrastructure Security (con't)
Delays
Service disruption
Power lines

Weather/Disaster/Emergency
Emergency
Hurricane
Tornado
Twister
Tsunami
Earthquake
Tremor
Flood
Storm
Crest
Temblor
Extreme weather
Forest fire
Brush fire
Ice
Stranded/Stuck
Help
Hail
Wildfire
Tsunami Warning Center
Magnitude
Avalanche
Typhoon
Shelter-in-place
Disaster
Snow
Blizzard
Sleet
Mud slide or Mudslide
Erosion
Power outage
Brown out

Weather/Disaster/Emergency (con't)
Warning
Watch
Lightening
Aid
Relief
Closure
Interstate
Burst
Emergency Broadcast System

Cyber Security
Cyber security (cybersecurity)
Botnet
DDOS (dedicated denial of service)
Denial of service
Malware
Virus
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