Privacy Impact Assessment
for the

Office of Operations Coordination and Planning

Publicly Available Social Media Monitoring and Situational Awareness Initiative

June 22, 2010

Contact Point
Donald Triner, Director (Acting), National Operations Center
Office of Operations Coordination and Planning
(202) 282-8611

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), will launch and lead the Publicly Available Social Media Monitoring and Situational Awareness (Initiative) to assist the Department of Homeland Security (DHS) and its components involved in fulfilling OPS statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)) to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate. The NOC and participating components[1] may also share this de-identified information with international partners and the private sector where necessary and appropriate for coordination. While this Initiative is not designed to actively collect Personally Identifiable Information (PII), OPS is conducting this Privacy Impact Assessment (PIA) because the Initiative could potentially involve PII or other information received in an identifiable form. In the event PII comes into the Department's possession under this Initiative, the NOC will redact all PII prior to further dissemination of any collected information. In the event of an *in extremis* situation involving potential life and death, OPS will share certain PII with the responding authority in order for them to take the necessary actions to save a life, such as name and location of a person calling for help buried under rubble, or hiding in a hotel room when the hotel is under attack by terrorists.

Reference is made to previous social media event monitoring initiative PIAs conducted by OPS to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers consistent with Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). Those OPS PIAs include: 1) Haiti Social Media Disaster Monitoring Initiative (January 21, 2010); 2) 2010 Winter Olympics Social Media Event Monitoring Initiative (February 10, 2010); and 3) April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative (April 29, 2010). For more information on these OPS PIAs, visit www.dhs.gov/privacy. Going forward, individual PIAs on social media monitoring will not be issued, instead, they will be covered by this overarching PIA.

This PIA will be reviewed every six months to ensure compliance. This will be done in conjunction with a Privacy Office-led Privacy Compliance Review of the Initiative and of OPS social media monitoring Internet-based platforms and information technology infrastructure.

Overview

Federal law requires the NOC to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. *See* Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). The law defines the term "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision-making." OPS is launching and leading this Initiative to fulfill its legal mandate to provide situational awareness and establish a common operating picture. In doing so, OPS is working with select components within the Department to achieve

[1] OPS is working with select components within the Department to provide situational awareness and establish a common operating picture for the federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers consistent with Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

this statutory mandate.

The NOC will use Internet-based platforms that provide a variety of ways to follow activity related to monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators[2] the NOC will monitor activities on the social media sites listed in Appendix A for information that the NOC can use to provide situational awareness and establish a common operating picture. Appendix A is a current list of sites that the NOC will use as a starting point under this Initiative. Initial sites listed may link to other sites not listed. The NOC may also monitor those sites if they are within the scope of this Initiative. The NOC will gather, store, analyze, and disseminate relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture. Under this initiative, OPS will not: 1) actively seek personally identifiable information (PII); 2) post any information; 3) actively seek to connect with other internal/external personal users; 4) accept other internal/external personal users' invitations to connect; or 5) interact on social media sites. However, OPS is permitted to establish user names and passwords to form profiles and follow relevant government, media, and subject matter experts on social media sites listed in Appendix A in order to use search tools under established criteria and search terms such as those listed in Appendix B for monitoring that supports providing situational awareness and establishing a common operating picture.

The NOC will identify and monitor only information needed to provide situational awareness and establish a common operating picture. The NOC will use this information to fulfill the statutory mandate set forth above to include the sharing of information with foreign governments and the private sector as otherwise authorized by law.

The Department may use social media for other purposes including interacting with the public, disseminating information to the public, as well as law enforcement, intelligence, and other operations covered by applicable authorities and PIAs. For more information on these social media PIAs, visit www.dhs.gov/privacy.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Third-party service providers offer an array of applications that provide social media services along with publicly-available online forums, blogs, public websites, and message boards. See Appendix A for a current list of the types of sites that may be viewed for information. See Appendix B for current search terms used under this Initiative. The NOC will review information posted by individual account users on third-party social media websites of activities and events necessary to provide situational awareness and establish a common operating picture. The NOC will access these web-based platforms to identify content posted by public users for the purpose of providing situational awareness and establishing a common

[2] Content aggregators generally provide a consolidated view of web content in a single browser display or desktop application.

operating picture. The NOC will assess information identified to assist decision-makers.

The NOC shall not actively collect data on the individuals posting information to third-party service providers, about individual users, or PII. Should PII come into the NOC's possession, the NOC shall redact it prior to further dissemination of any collected information. In the event of an *in extremis* situation involving potential life and death, DHS will share certain PII with the responding authority in order for them to take the necessary actions to save a life, such as name and location of a person calling for help buried under rubble, or hiding in a hotel room when the hotel is under attack by terrorists.

1.2 What are the sources of the information in the system?

Members of the public as well as first responders, press, volunteers, and others provide publicly available information on social medial sites including online forums, blogs, public websites, and message boards. OPS is permitted to establish user names and passwords to form profiles on social media sites listed in Appendix A and to use search tools under established criteria and search terms such as those listed in Appendix B for monitoring that supports providing situational awareness and establishing a common operating picture.

1.3 Why is the information being collected, used, disseminated, or maintained?

The NOC will identify, use, disseminate, and maintain this information to comply with its statutory mandate to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate and to ensure that this information reaches government decision makers. The aggregation of data published via social media sites should make it possible for the NOC to provide more accurate situational awareness, a more complete common operating picture, and more timely information for decision makers.

1.4 How is the information collected?

The NOC will identify information directly from third-party social media services. The NOC will access and collect information from various informational streams and postings that the NOC, as well as the broader public, view and monitor. See Appendix A for a list of the types of sites that may be viewed for information. See Appendix B for the types of search terms used in social media monitoring.

1.5 How will the information be checked for accuracy?

The NOC will identify information from third-party social media services submitted voluntarily by members of the public and compares that information with information available in open source reporting and through a variety of public and government sources. By bringing together and comparing many different sources of information, the NOC will attempt to provide a more accurate picture of contemporaneous activities.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Congress requires the NOC "to provide situational awareness and establish 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 manmade disaster; and ensure that critical terrorism

and disaster-related information reaches government decision-makers." Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)). While the NOC may receive PII, PII is not actively collected and is not retrieved by personal identifier so a Privacy Act System of Records Notice is not required.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that the NOC will receive PII or other identifiable information that is not relevant to this Initiative. The NOC has a clear policy in place that any PII incidentally received will be redacted immediately. Also, under this initiative OPS will not: 1) actively seek PII; 2) post any information; 3) actively seek to connect with other internal/external personal users; 4) accept other internal/external personal users' invitations to connect; and 5) interact on social media sites. Information collected to provide situational awareness and establish a common operating picture originates from publicly available social media sites and is available to the public.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The NOC will use Internet-based platforms that provide a variety of ways to follow activities by monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the NOC will continuously monitor activities on social media sites, such as those listed in Appendix A, using search terms, such as those listed in Appendix B, for information. The NOC will gather, store, analyze, and disseminate relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners requiring and authorized to receive situational awareness and a common operating picture.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NOC analysts will be responsible for monitoring and evaluating information provided on social media sites and will use tools offered by third-party social media sites to aid them in this overall effort. The final analysis will be used to provide situational awareness and establish a common operating picture.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Publicly available, user-generated data can be useful to decision-makers as it provides "on-the-ground" information to help corroborate information received through official sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk is that PII will be sent to the NOC unintentionally. This has been mitigated by the clear policy that any PII inadvertently collected shall be redacted immediately before further use and sharing. The Department is providing notice of all uses of information under this Initiative through this PIA. the NOC will not actively collect or use any PII.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The NOC will retain only user-generated information posted to publicly available online social media sites. Information posted in the public sphere that the Department uses to provide situational awareness or establish a common operating picture becomes a federal record and the Department is required to maintain a copy. However, the Department is working with the National Archives and Records Administration (NARA) on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA, as well as to maintain records necessary for further use by the Department.

3.2 How long is information retained?

The NOC will retain information only long enough to provide situational awareness and establish a common operating picture. Information posted in the public sphere that the Department uses to provide situational awareness or establish a common operating picture becomes a federal record and the Department is required to maintain a copy. The Department is working with NARA on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA, as well as to maintain records necessary for further use by the Department.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The Office of Records Management is working with NARA to establish an approved retention and disposal policy.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk associated with retention of information is that PII will be retained when it is not necessary and that the information will be kept longer than is necessary. The NOC has mitigated this risk by redacting PII it inadvertently collects and is working with NARA on a retention schedule to immediately delete PII, upon the approval of this schedule by NARA, as well as to maintain records necessary for further use by the Department.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information will be shared within the NOC and with government leadership who have a need to know. The NOC is sharing this information for the statutorily mandated purpose of providing situational awareness and establishing a common operating picture.

4.2 How is the information transmitted or disclosed?

Information will be transmitted via email and telephone and by other electronic and paper means within the NOC and to government leadership where necessary and appropriate. PII will not actively be collected, but if pushed to the NOC, it will be redacted by the NOC before information is shared. The remaining data is analyzed and prepared for reporting.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk associated with sharing this information is that PII will be inadvertently collected and shared. The NOC has mitigated this risk by establishing effective policies to avoid collection of PII and to redact it if collected inadvertently. The NOC will only monitor publicly accessible sites where users post information voluntarily.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The NOC will use this Initiative to fulfill its statutory responsibility to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision makers. Information may also be shared with private sector and international partners where necessary, appropriate, and authorized by law.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable

information outside of DHS.

PII will not actively be collected. However, if pushed to the NOC, the PII will be redacted. Information is only collected to provide situational awareness and to establish a common operating picture.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information will be shared by phone, email, and other paper and electronic means.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

External sharing risks are minimal as the Initiative will not share PII; only information collected to provide situational awareness and to establish a common operating picture is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The Department may publicize its use of social media. The NOC does not, however, provide notice to specific public users who voluntarily provide user-generated information on publicly accessible social media sites. The NOC may retrieve public information from the social media sites, but will not interact with individual personal users.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Information posted to social media websites is publicly accessible and voluntarily generated. Thus, the opportunity not to provide information exists prior to the informational post by the user.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals voluntarily post information on social media sites and have the ability to restrict access to their posts as they see fit. Any information posted publicly can be used by the NOC in providing situational awareness and establishing a common operating picture.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is no requirement to provide notice to individuals under the framework applied under this

Initiative. Information posted to social media approved for monitoring under this Initiative is publicly accessible and voluntarily generated.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Social media are public websites. All users have access to their own information through their user accounts. Individuals should consult the privacy policies of the services they subscribe to for more information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this. However, the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information.

7.3 How are individuals notified of the procedures for correcting their information?

There is no specified procedure for correcting information to DHS; if there was, it relates to a social media- provided process and not a DHS process. Individuals may change their PII on the sites as well as the accessibility of their content posts at any time they wish through their user account management tools on social media sites.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is no specified procedure for correcting information to DHS; if there was, it relates to a social media-provided process and not a DHS process. Individuals may change their PII as well as the accessibility of their content posts at any time they wish through their user account management tools on the social media sites. Individuals should consult the privacy policies of the services to which they subscribe for more information.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The information available on social networking websites is largely user-generated, which means that the individual chooses the amount of information available about himself/herself as well as the ease with which it can be accessed by other users. Thus, the primary account holder should be able to redress

any concerns through the third-party social media service. Individuals should consult the privacy policies of the services they subscribe to for more information.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

No procedures are in place. Social media sites are publicly available, third-party services.

8.2 Will Department contractors have access to the system?

Yes, as it is required in the performance of their contractual duties at DHS.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS employees and contractors are required to take annual privacy training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No. Social media sites are publicly available, third-party services.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

This PIA will be reviewed every six months to ensure compliance. This will be done in conjunction with a Privacy Office-led Privacy Compliance Review of the Initiative and of OPS social media monitoring internet based platforms and information technology infrastructure.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

These social media sites are publicly available, third-party services. Information is collected by the service itself to establish an account. Thereafter, users determine their level of involvement and decide how "visible" they wish their presence on any given service to be. The ability to choose how much information to disclose, as well as the short period of retention for any information collected by the NOC serves to mitigate any privacy risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any

technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

Third-parties control and operate social media services. Users should consult with representatives of the service provider in order to make themselves aware of technologies utilized by the system.

9.2 What stage of development is the system in and what project development lifecycle was used?

Social media is active at all times and is third-party owned and operated.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Individuals should consult the privacy policies of the services they subscribe to for more information.

Responsible Officials

Donald Triner
Director (Acting), National Operations Center
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Social Media Web Sites Monitored by the NOC

This is a representative list of sites that the NOC will start to monitor in order to provide situational awareness and establish a common operating picture under this Initiative. Initial sites listed may link to other sites not listed. The NOC may also monitor those sites if they are within the scope of this Initiative.

Tool	Link	User/Password Required
General Search		
Collecta	http://collecta.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 Aggs		
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 Cybercrime Topic Center	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

Terms Used by the NOC When Monitoring Social Media Sites

This is a current list of terms that will be used by the NOC 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 will not use PII in searching for relevant mission-related information.

DHS & Other Agencies
Department of Homeland Security (DHS)
Federal Emergency Management Agency (FEMA)
Coast Guard (USCG)
Customs and Border Protection (CBP)
Border Patrol
Secret Service (USSS)
National Operations Center (NOC)
Homeland Defense
Immigration Customs Enforcement (ICE)
Agent
Task Force
Central Intelligence Agency (CIA)
Fusion Center
Drug Enforcement Agency (DEA)
Secure Border Initiative (SBI)
Federal Bureau of Investigation (FBI)
Alcohol Tobacco and Firearms (ATF)
U.S. Citizenship and Immigration Services (CIS)
Federal Air Marshal Service (FAMS)
Transportation Security Administration (TSA)
Air Marshal
Federal Aviation Administration (FAA)
National Guard
Red Cross
United Nations (UN)

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)
National preparedness initiative
Militia
Shooting
Shots fired
Evacuation
Deaths
Hostage
Explosion (explosive)
Police
Disaster medical assistance team (DMAT)
Organized crime
Gangs
National security
State of emergency
Security
Breach
Threat
Standoff
SWAT
Screening
Lockdown
Bomb (squad or threat)
Crash
Looting
Riot
Emergency Landing
Pipe bomb
Incident
Facility

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
Anthrax
Blister agent
Chemical agent
Exposure
Burn
Nerve agent
Ricin
Sarin
North Korea

Health Concern + H1N1
Outbreak
Contamination
Exposure
Virus
Evacuation
Bacteria
Recall
Ebola
Food Poisoning
Foot and Mouth (FMD)
H5N1
Avian
Flu
Salmonella
Small Pox
Plague
Human to human
Human to Animal
Influenza
Center for Disease Control (CDC)
Drug Administration (FDA)
Public Health
Toxic
Agro Terror
Tuberculosis (TB)
Agriculture
Listeria
Symptoms
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

Southwest Border Violence
Drug cartel
Violence
Gang
Drug
Narcotics
Cocaine
Marijuana
Heroin
Border
Mexico
Cartel
Southwest
Juarez
Sinaloa
Tijuana
Torreon
Yuma
Tucson
Decapitated
U.S. Consulate
Consular
El Paso
Fort Hancock
San Diego
Ciudad Juarez
Nogales
Sonora
Colombia
Mara salvatrucha
MS13 or MS-13
Drug war
Mexican army
Methamphetamine
Cartel de Golfo
Gulf Cartel
La Familia
Reynosa
Nuevo Leon
Narcos
Narco banners (Spanish equivalents)
Los Zetas
Shootout
Execution
Gunfight
Trafficking
Kidnap
Calderon
Reyosa
Bust
Tamaulipas
Meth Lab
Drug trade
Illegal immigrants
Smuggling (smugglers)
Matamoros
Michoacana
Guzman
Arellano-Felix
Beltran-Leyva
Barrio Azteca
Artistic Assassins
Mexicles
New Federation

Terrorism
Terrorism
Al Qaeda (all spellings)

Terror
Attack
Iraq
Afghanistan
Iran
Pakistan
Agro
Environmental terrorist
Eco terrorism
Conventional weapon
Target
Weapons grade
Dirty bomb
Enriched
Nuclear
Chemical weapon
Biological weapon
Ammonium nitrate
Improvised explosive device
IED (Improvised Explosive Device)
Abu Sayyaf
Hamas
FARC (Armed Revolutionary Forces Colombia)
IRA (Irish Republican Army)
ETA (Euskadi ta Askatasuna) Basque Separatists
Hezbollah
Tamil Tigers
PLF (Palestine Liberation Front)
PLO (Palestine Liberation Organization
Car bomb
Jihad
Taliban
Weapons cache
Suicide bomber
Suicide attack
Suspicious substance
AQAP (AL Qaeda Arabian Peninsula)
AQIM (Al Qaeda in the Islamic Maghreb)
TTP (Tehrik-i-Taliban Pakistan)
Yemen
Pirates
Extremism
Somalia
Nigeria
Radicals
Al-Shabaab
Home grown
Plot
Nationalist
Recruitment
Fundamentalism
Islamist

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