Privacy Impact Assessment

for the

Office of Operations Coordination and Planning

Publicly Available Social Media Monitoring and Situational Awareness Initiative Update

April 1, 2013

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), leads the Publicly Available Social Media Monitoring and Situational Awareness Initiative (also referred to in this PIA as "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.

After conducting the fourth Privacy Compliance Review (PCR) (Media Monitoring Initiative) the Privacy office determined that this PIA should be updated to reflect changes recommended to and implemented by the NOC. These include improvements in tracking of searches conducted to identify relevant reports, incorporation of additional guidance into standard operating procedures (SOP) concerning the appropriate use of the NOC Media Monitoring Capability (MMC) Twitter profile, and clarification of language in the Analyst's Desktop Binder and SOPs to emphasize that information in NOC MMC reports must be operationally relevant to DHS in all cases. DHS is replacing the 2011 published DHS/OPS/PIA-004(d) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update PIA with this PIA.

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 has launched 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 this statutory mandate.

The NOC MMC uses 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[1] the NOC MMC monitors activities on the social media sites for information that can be used to provide situational awareness and establish a common operating picture. Appendix A contains a list of sites that the NOC MMC uses as a starting point under this Initiative. Initial sites listed may link to other sites not listed in the appendix. The NOC MMC may also monitor those sites if they are within the scope of this Initiative. The NOC gathers, stores, analyzes, and disseminates 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 does not: (1) post any information on social media sites; (2) actively seek to connect with other individual social media users, whether internal or external to DHS; (3) accept invitations to connect from other individual social media users, whether internal or external to DHS; or (4) interact on social media sites. However, OPS is permitted to establish user names and passwords to form profiles and connect with operationally relevant government, media, and subject matter experts on social media sites (such as those 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. Furthermore, personally identifiable information (PII) on the following categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners: (1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; (2) senior U.S. and foreign government officials who make public statements or provide public updates; (3) U.S. and foreign government spokespersons who make public statements or provide public updates; (4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; (5) names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed; (6) current and former public officials who are victims of incidents or activities related to Homeland Security; and (7) terrorists, drug cartel leaders, or other persons known to have been involved in major crimes of Homeland Security interest, (e.g., mass shooters such as those at Virginia Tech) who are killed or found dead.

Due to this authorized collection of PII and the ability of retrieval by personal identifier, a

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

system of records notice (SORN) is necessary. While DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN [75 FR 69,689 (November 15, 2010)] provides coverage as part of the second PCR, DHS also published DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative SORN [76 FR 5603 (November 27, 2012)] to provide additional transparency.

The NOC identifies and monitors only information needed to provide situational awareness and establish a common operating picture. The NOC uses 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.

To monitor social media, NOC Media Monitoring analysts only use publicly available search engines, content aggregators, and site-specific search tools to find items of potential interest to DHS. Once the analysts determine an item or event is of sufficient value to DHS to be reported, they extract only the pertinent, authorized information, and put it into a specific web application (MMC application)[2] to build and format their reports. The unused information for each item of interest is not stored or filed for reference and is lost when the webpage is closed or deleted. The MMC application also facilitates tracking previous reports to help avoid duplicative reporting and ensures further development of reporting on ongoing issues. It allows analysts to electronically document details using a customized user interface, and disseminate relevant information in a standardized format. Using the MMC application, NOC MMC analysts can efficiently and effectively catalog the information by adding meta-tags such as location, category, critical information requirement, image files, and source information. The application empowers NOC MMC analysts to have a better grasp of the common operating picture by providing the means to quickly search for an item of interest using any of the above-mentioned meta-tags as well as enabling them to respond to requests for information from other collaborating entities in a timely fashion.

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

DHS is replacing the January 6, 2011 DHS/OPS/PIA-004(d) Publicly Available Social

[2] The MMC application does not document any raw information reviewed during the collection phase. It is also important to note that any data collected from the raw information is free of PII as defined in this document.

Media Monitoring and Situational Awareness Initiative Update PIA with this PIA to account for the following clarifications: improvements in tracking of searches conducted to identify relevant reports, incorporation of additional guidance into SOPs concerning the appropriate use of the NOC MMC Twitter profile, clarification of language in the Analyst's Desktop Binder and SOPs to emphasize information in MMC Reports must be operationally relevant to DHS in all cases, and establishing the requirement of an annual PCR and self-certification submitted to the DHS Privacy Office.

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. Appendix A lists of the types of sites that may be viewed for information, and Appendix B contains a representative list of search terms used under this Initiative. The NOC MMC reviews 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 MMC accesses these web-based platforms to identify content posted by public users for the purpose of providing situational awareness and establishing a common operating picture. The NOC MMC assesses information identified to assist decision-makers.

PII on the following categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners: (1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; (2) Senior U.S. and foreign government officials who make public statements or provide public updates; (3) U.S. and foreign government spokespersons who make public statements or provide public updates; (4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; (5) names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep

their audience situationally aware and informed; (6) current and former U.S. and foreign public officials who are victims of incidents or activities related to Homeland Security; and (7) terrorists, drug cartel leaders, or other persons known to have been involved in major crimes of Homeland Security interest, (e.g., mass shooters such as those at Virginia Tech) who are killed or found dead. PII on these individuals may include: (1) full name, (2) affiliation, (3) position or title, and (3) publicly-available user ID. Analysts are trained to use only approved PII that falls within these categories. Analysts are trained to identify this type of PII and to ignore and exclude any non-authorized PII. Should PII apart from these categories come into the NOC's possession , the NOC redacts it prior to further dissemination of any collected information.

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

Sources of information come from members of the public as well as first responders, press, volunteers, and others who may 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 identifies, uses, disseminates, and maintains 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. This information is also used 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 MMC identifies information directly from third-party social media services. The NOC MMC accesses and collects information from various informational streams and postings that the NOC, as well as the broader public, view and monitor. Appendix A provides a list of the types of sites that may be viewed for information; Appendix B provides the types of

search terms used in social media monitoring.

1.5 How will the information be checked for accuracy?

The NOC MMC identifies 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 MMC attempts 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." 6 U.S.C. § 321d(b)(1). Most of the data within this system does not pertain to an individual; rather, the information pertains to locations, geographic areas, facilities, and other things or objects that are operationally relevant, but not related to individuals. Most information is stored as free text and any word, phrase, or number is searchable. The NOC MMC does not actively seek or collect PII, but PII may be collected during *in extremis* situations.

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 MMC could receive PII that is not relevant to this Initiative. The NOC has a clear policy in place that any PII incidentally received outside the scope of the discrete set of categories discussed above is immediately redacted. Also, under this initiative, OPS does not: (1) actively seek PII; (2) post any information; (3) actively seek to connect with other individual social media users, whether internal or external to DHS; (4) accept invitations to connect from other individual social media users, whether internal or external to DHS; or (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. As a result of the fourth PCR, the Privacy Office made recommendations that further identify and mitigate privacy risks associated with this initiative. These mitigation strategies include implementing a logging mechanism to account for searches conducted to

identify relevant reports, and incorporating additional guidance into SOPs and the Analyst's Desktop Binder concerning the appropriate use of the official Twitter Profile. NOC MMC has also established 13 event categories[3] that are consistent with its statutory mandate to provide situational awareness, a more complete common operating picture, and more timely information for decision makers. NOC MMC SOPs reinforce policy and also include guidance on the use of the Twitter account with specific provisions for the periodic review of "following" to ensure that individuals are not "followed." The NOC MMC Twitter profile is permitted to "follow" only other government agencies, media outlets, and other non-governmental organizations that are potential sources for the NOC MMC Initiative in providing situational awareness. SOPs and the Analyst's Desktop Binder describe a review process that requires NOC MMC analysts to seek approval from the Watch Lead and the NOC Senior Watch Officer before "following" another Twitter profile.

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 MMC uses 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 MMC continuously monitors 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 continues to gather, store, analyze, and disseminate relevant and appropriate information to federal, state, local, and foreign governments, and to 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

[3] OPS/NOC established 13 event categories that are consistent with their statutory mandate to provide situational awareness, a more complete common operating picture, and more timely information for decision makers. Analysts are required to tag reports using the MMC application to one or more of these categories to enable reporting and trend analysis. The event categories are as follows: Cyber Security, Fire, HAZMAT, Health Concerns, National/International, Immigration, Infrastructure, National/International Security, Nuclear, Public Safety, Terrorism, Trafficking/Border Control Issues, Transportation Security, and Weather/Natural Disasters/Emergency.

may be produced?

NOC MMC analysts are responsible for monitoring and evaluating information provided on social media sites and use tools offered by third-party social media sites to aid them in this overall effort. The final analysis is 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.

The NOC MMC uses 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. Publicly available, user-generated data can be useful to decision-makers as they provide "on-the-ground" information to help corroborate information received through official sources. The use of publicly available data helps the Department meet its requirements according to Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

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.

There is a risk is that PII could be sent to the NOC unintentionally. This risk is mitigated by the clear policy that inadvertently collected PII that is outside the scope of the discrete set of categories discussed above shall be redacted immediately before further use. The Department is providing notice of all uses of information under this Initiative through this PIA. The NOC MMC does not actively collect or use any PII outside the scope of the discrete set of categories discussed above.

The NOC continues to improve its SOPs and technology in order to reduce the privacy risks and concerns. The NOC has also taken several responsive actions to ensure that controls are in place to guarantee that information is handled in accordance with the uses described in the PIA.

Since the January 6, 2011, publishing of the PIA, NOC MMC has implemented an automated logging mechanism to account for searches conducted to identify relevant reports. This provides further assurance that the NOC MMC is not creating profiles of individuals or searching its reports using PII. The log captures the date and time of the search, the analyst user

ID, and the character search term. The purpose of such searches is to locate a previously issued MMC report. The purpose of the search function is also documented in SOPs and the Analyst's Desktop Binder. The logging mechanism also captures numeric search terms (e.g., NOC Number) to provide further assurance that all search activities are recorded.

The second action NOC MMC has incorporated is providing additional guidance into its SOPs and the Analyst's Desktop Binder concerning the appropriate use of the official Twitter Profile that incorporates a review process. This review process requires the MMC analyst to seek approval from the Watch Lead and the Senior Watch Officer before "following" another Twitter profile.

The third responsive action taken by NOC MMC is clarification of the language in the Analyst's Desktop Binder and SOPs to emphasize that in all cases information in MMC Reports must be operationally relevant to DHS. This action ensures the implementation of the NOC MMC in a privacy-sensitive manner. Any language suggesting that NOC MMC engages in monitoring of First Amendment protected activities for public dissent has been removed because NOC MMC does not engage in such monitoring.

Lastly, the NOC MMC must perform two types of annual reporting to the DHS Privacy Office to show how the controls described in this PIA are ensuring information is handled in accordance with the described uses.

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 MMC retains 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.

3.2 How long is information retained?

The NOC MMC retains information for no more than five years to provide situational awareness and establish a common operating picture. This five-year retention schedule is based on the operational needs of the Department.

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

Yes.

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 is retained when it is not necessary and that the information could be kept longer than is necessary. The NOC MMC has mitigated this risk by redacting PII outside the scope of the discrete set of categories discussed above that it inadvertently collected. The NOC MMC is working with NARA on a retention schedule to immediately delete PII upon its approval of this schedule. NOC MMC is also working with NARA 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 is shared within the NOC and with DHS 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 is transmitted via email, telephone, and by other electronic and paper means. Information is transmitted within the NOC and to DHS leadership when necessary and appropriate to provide situational awareness and establish a common operating picture. PII is not actively collected outside the scope of the discrete set of categories discussed above.

However, if PII is inadvertently pushed to the NOC, it is redacted by the NOC MMC. The remaining data are 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 outside the scope of the discrete set of categories discussed above and to redact it if collected inappropriately. The NOC MMC only monitors 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 uses 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 when 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.

The NOC MMC does not actively seek or collect PII. However, if pushed to the NOC and outside the scope of the discrete set of categories discussed above, the PII is redacted. Any

sharing of information is compatible with DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN [75 FR 69,689 (November 15, 2010)] and the Department of Homeland Security Office of Operations Coordination and Planning – 004 Publicly Available Social Media Monitoring and Situational Awareness Initiative SORN [76 FR 5603 (November 27, 2012)]. 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 is shared by phone, email, and other paper and electronic means. Policies and procedures described throughout this PIA serve as pertinent security measures that safeguard the transmission of information outside the Department.

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 only shares PII on a narrowly tailored category of individuals; only information collected to provide situational awareness and to establish a common operating picture is shared. Any sharing is compatible with DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN [75 FR 69,689 (November 15, 2010)]. The Department published DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative SORN [76 FR 5603 (November 27, 2012)] to provide additional transparency to the Initiative.

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?

Notice is provided through this PIA and through DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion SORN [75 FR 69,689 (November 15, 2010)], and the Department of Homeland Security Office of Operations Coordination and

Planning – 004 Publicly Available Social Media Monitoring and Situational Awareness Initiative SORN [76 FR 5603 (November 27, 2012)].

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 user posting information.

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?

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

For those included in the limited category of individuals about whom PII may be collected, who are seeking access to any record containing information that is part of a DHS system of records or seeking to contest the accuracy of its content, they may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to DHS. Given the nature of some of the information in the Senior Watch Officer and NOC Tracker Logs (sensitive law enforcement or intelligence information), DHS may not always permit the individual to gain access to or request amendment of his or her record. However, requests processed under the PA are also processed under FOIA; requesters are always given the benefit of the statute with the more liberal release requirements. The FOIA does not grant an absolute right to examine government documents; FOIA establishes the right to request records and to receive a response to the request. Instructions for filing a FOIA or PA request are available at: http://www.dhs.gov/xfoia/editorial_0316.shtm.

The FOIA/PA request must contain the following information: Full Name, current address, date and place of birth, and telephone number. Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. § 1746. Please refer to the DHS FOIA web site for more information at www.dhs.gov/foia.

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

See Section 7.1.

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

Individuals are notified through this PIA, the DHS/OPS-003 SORN, and the DHS/OPS-004 SORN.

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. 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?

All NOC Media Monitoring analysts have access to media feed aggregation tools and sites which are publicly available. The analysts also have access to the MMC application which is only accessible via a physical connection to an isolated private network established at the NOC Media Monitoring Watch room. In addition to the physical security, the program requires an assigned username and password for access. The system cannot be remotely accessed.

8.2 Will Department contractors have access to the system?

Yes, as it is required in the performance of their contractual duties at DHS. However, access to the MMC application is limited to NOC-authorized analysts who are physically present at the NOC Media Monitoring Watch desk.

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. In addition, media monitoring analysts receive job-specific PII training.

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

No. Tools and sites being used for information collection are publicly available, third-party services. Certification and accreditation has not been completed for MMC application since the system is housed on non-government furnished equipment on an isolated private network. Since social media sites are third-party services, no certification and accreditation is required. DHS does not plan to complete the certification and accreditation process for this program.

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

This initiative will undergo a Privacy Compliance Review (PCR) every 12 months to ensure compliance. The PCR is a Privacy Office-led review of the Initiative, and of OPS social media monitoring internet-based platforms and information technology infrastructure. Previously, PCRs were conducted every six months; however, as a result of the fifth PCR and NOC MMC's history of strong performance and compliance during previous PCRs, the Privacy Office now plans to conduct an annual PCR. In addition to an annual PCR, NOC will self-certify a set of questions administered by the DHS Privacy Office on an annual basis approximately six months after the annual PCR is completed.

As recommended by the Privacy Office, the NOC MMC has implemented an auditing capability at the router level for all outbound http(s) traffic and generates audit reports that are available for each compliance review and upon request to the Privacy Office. Also, information on sources used to generate all reports can be provided for review by Privacy officials. The MMC application server resides on a secure, firewalled, isolated private network that does not allow inbound access or connection.

NOC MMC has implemented an automated logging mechanism to account for searches conducted to identify relevant reports. The log captures the date and time of the search, the analyst user ID, and the character search term (the purpose of the searches is also documented in their SOPs and Analyst's Desktop Binder). The logging mechanism also captures numeric search terms (e.g., NOC Number). NOC MMC continues to leverage the technology to ensure ongoing compliance with its policy.

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?

Media feed aggregation tools/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 MMC, mitigates any privacy risk.

The PII collected is secure, and the information is comprised of a very limited scope within the discrete set of categories discussed above. NOC MMC does not retain any raw information reviewed during the collection phase. All data entered into the MMC application is carefully reviewed to ensure compliance with the guidelines provided in this PIA. The MMC application is not designed to share information by any means other than sending reports to a pre-approved, predetermined, distribution list. The only way to access data in the application is for an authorized user physically connected to a contained system to pull out data, create a separate file, and then share that file. Privacy-compromising risks are low because the system cannot be accessed remotely and the collected PII is very limited.

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 used 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, Operations Coordination Division
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Jonathan R. Cantor
Acting 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 MMC 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 MMC 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
AccuWeather	http://accuweather.com	
Al Jazeera Blog	http://blogs.aljazeera.net	
al Sahwa	http://al-sahwa.blogspot.com/	No
AllAfrica	http://allafrica.com/	No
Avian Flu Diary	http://afludiary.blogspot.com/	No
Barf Blog	http://barfblog.foodsafety.ksu.edu/barfblog	
BNOnews	http://www.bnonews.com/	No
Border Violence Analysis	http://borderviolenceanalysis.typepad.com/mexicos_drug_war	
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
Emergency Management Magazine	http://www.emergencymgmt.com	No
Fierce Homeland Security	http://fiercehomelandsecuritynewswire.com	
Food Poison Journal	http://foodpoisonjournal.com	
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
Homeland Security News Wire	http://homelandsecuritynewswire.com	
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
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
M3 Report	http://m3report.wordpress.com	
Malware Intelligence Blog	http://malwareint.blogspot.com/	No
MEMRI	http://www.memri.org/	No
MexiData.info	http://mexidata.info/	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
New Mexico Fire Information	http://fireinfo.wordpress.com	
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
Somalia Report	http://somaliareport.com	
STRATFOR	http://www.stratfor.com/	No
Technorati	http://technorati.com/	No
Terror Finance Blog	http://www.terrorfinance.org/the_terror_finance_blog/	No
The Jawa Report	http://mypetjawa.mu.nu	
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
War on Terrorism	http://terrorism-online.blogspot.com/	No
WireUpdate	http://wireupdate.com/	No

APPENDIX B

Terms Used by the NOC MMC When Monitoring Social Media Sites

This is a representative list of terms that the NOC MMC will use 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
Breach
Hacked
Hacktivist
Zombie
Breach
Vulnerability
Exploit
CERT (Computer Emergency Response Team)
Zero day
Spearphishing
Network
Grid
Obfuscation
SQL (Structure Query Language)
Injection
Man in the middle
Hijack
Logger
DOS (denial of service)

Other
Breaking News