Privacy Compliance Review

of the

NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative

April 16, 2014

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

Reviewing Official
Karen Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

I. BACKGROUND

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has statutory responsibility to (1) provide situational awareness and establish a common operating picture for the 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 (2) ensure that critical terrorism and disaster-related information reaches government decision-makers.[1] Traditional media sources and, more recently, social media sources such as Twitter, Facebook, and a vast number of blogs provide public reports on breaking events with a potential nexus to homeland security. By examining both open source traditional and social media information, comparing it with many other sources of information, and including it where appropriate into reports, the NOC can provide a more comprehensive picture of breaking or evolving events.

In January 2010, to help fulfill its statutory responsibility to provide situational awareness and to access the potential value of public information within the social media realm, the NOC launched the first of three Media Monitoring Capability (MMC) pilots using social media monitoring related to specific incidents and international events. The NOC pilots occurred during the 2010 Haiti earthquake response, the 2010 Winter Olympics in Vancouver, British Columbia, and the response to the 2010 Deepwater Horizon BP oil spill. Prior to implementation of each social media pilot, the DHS Privacy Office and OPS developed detailed standards and procedures for reviewing information on social media web sites. A series of pilot-specific Privacy Impact Assessments (PIA) document these standards and procedures. In June 2010, the Department released its Publicly Available Social Media Monitoring and Situational Awareness Initiative PIA, which incorporated these protections.[2] OPS/NOC and PRIV subsequently updated the PIA in January 2011,[3] and published a Privacy Act System of Records Act Notice (SORN) on February 1, 2011,[4] to allow for the collection and dissemination of personally identifiable information (PII) in a very limited number of situations in order to respond to the evolving operational needs of OPS/NOC.

As of January 2011, the NOC may include PII on seven categories of individuals in an Item of Interest (hereinafter MMC Report or Report) when doing so lends credibility to the

[1] Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).
[2] PIAs for the MMC Initiative can be found at http://www.dhs.gov/privacy.
[3] DHS/OPS/PIA-004(d) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update (January 6, 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf)
[4] DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records Notice (February 1, 2011) 76 FR 5603, *available at* http://edocket.access.gpo.gov/2011/2011-2198.htm

report or facilitates coordination with interagency or international partners. The seven categories as identified in the SORN are: "(1) U.S. and foreign individuals in extremis, *i.e.*, in 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 posts or articles, or who use traditional and/or social media in real time to provide their audience situational awareness and information; (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, who are killed or found dead."

As documented in the January 2011 PIA Update, the NOC does not: (1) actively seek PII; (2) post any information on social media sites; (3) actively seek to connect with individuals, whether internal or external to DHS; (4) accept invitations to connect from individual social media users whether internal or external to DHS; or (5) interact with individuals on social media sites. The PIA was updated in April 2013[5] to reflect changes from the fourth Privacy Compliance Review (PCR) conducted in November 2012.[6] These include improvements in tracking of searches conducted to identify relevant reports, incorporation of additional guidance into standard operating procedures (SOPs) 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.

PCRs are a key aspect of the layered privacy protections built into this initiative to ensure the protections described in the PIAs are followed. Since the June 2010 PIA publication, PCRs have been conducted bi-annually. Based on the positive results of the November 2012 PCR and OPS/NOC's history of strong performance in the previous four PCRs, the DHS Privacy Office moved from a bi-annual to an annual PCR schedule for this initiative. The annual schedule includes self-assessments by OPS/NOC every six months, using question sets prepared by the DHS Privacy Office.

---

[5] DHS/OPS/PIA-004(e) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update (April 1, 2013), *available at* http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning.
[6] Privacy Compliance Review of the NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative (November 8, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy/PCRs/PCR%20NOC%20Situational%20Awareness%20Initiative%20%28FINAL%29%2020121108.pdf.

In March 2013, OPS/NOC conducted the initial self-assessment of MMC privacy protections, covering September 2012 – March 2013. The DHS Privacy Office conducted a sixth full PCR in February 2014, covering the assessment period of March 2013 – December 2013. The DHS Privacy Office developed a questionnaire, interviewed OPS/NOC officials and analysts on issues raised by the NOC's responses to the questionnaire, analyzed OPS/NOC guidance and SOP, and reviewed selected MMC Reports for compliance with the 2011 PIA Update.

II. SUMMARY

The DHS Privacy Office finds that OPS/NOC continues to be in compliance with the privacy requirements identified in the April 2013 PIA Update and the February 2011 SORN; however, a technical update of the February 2011 SORN is needed to clarify the categories of individuals whose PII NOC/OPS may include in Reports. The requirements are discussed in detail below. Our specific findings are as follows:

- *Collection of Information* - OPS/NOC continues to comply with requirements not to actively seek PII in its reporting, not to engage and interact with individuals through social media as required by the June 2011 PIA, and ensure that the PII collected falls within the seven permitted categories of individuals.

  From March 1, 2013 to December 31, 2013, the NOC distributed 15,902 MMC Reports of which 818 (five percent) contained PII within the seven permitted categories of individuals identified in the February 2011 SORN. Of particular note, OPS/NOC reduced the number of MMC Reports containing authorized PII by 8 percent over the self-assessment period of September 2012 – February 2013. This significant reduction demonstrates judicious use of authorized PII and increased experience in providing operationally relevant MMC Reports that do not contain PII.

- *Use of Information* - The OPS/NOC has established 13 reporting event categories that are consistent with its statutory mandate to provide situational awareness, a more complete common operating picture, and more timely information for decision-makers.[7] Our review of ten randomly-selected days' worth of MMC Reports (538 Reports) found that they reflect a variety of topics within the 13 event categories and any PII included is within one of the seven permissible categories of individuals.

[7] The thirteen categories are: 1) Terrorism, 2) Weather/Natural Disasters/Emergency Management, 3) Fire, 4) Trafficking /Border Control Issues, 5) Immigration, 6) HAZMAT, 7) Nuclear, 8) Transportation Security, 9) Infrastructure, 10) National/International Security, 11) Health Concerns, National/International, 12) Public Safety and 13) Cyber Security.

The NOC MMC is now using geo-location data from various social media sources. Due to the sensitive nature of geo-location data, there are new privacy risks associated with the use of this information by the NOC.

- *Technical Access and Security* - The OPS/NOC audit capability for all outbound http(s) traffic, designed to ensure appropriate use of the Internet by MMC analysts, became fully operational in May 2011. Since March 2013, OPS/NOC has conducted 20 random audits (two per month) that cover all MMC analysts and documented the results in self-audit compliance reports. These audits have not identified any inappropriate uses of the Internet by MMC analysts.

- *Privacy Training* - The NOC MMC has hired five new analysts since March 2013 and all have completed PII training and passed the PII examination. Supplemental guidance issued to the analysts since March 2013 continues to direct them to focus on events, incidents, and crises that have operational relevance and impact.

- *Privacy Compliance Documentation* - A review of the May 3, 2012 PCR determined that a requirement to update the February 2011 SORN has not been completed. A technical update of the February 2011 SORN is needed to clarify the categories of individuals whose PII NOC/OPS may include in Reports.

III. SCOPE AND METHODOLOGY

The DHS Privacy Office conducted its sixth PCR of the OPS/NOC MMC in coordination with OPS/NOC leadership for the period of March 2013 through December 2013. The DHS Privacy Office carried out the following activities:

- Reviewed the OPS/NOC self-assessment submitted in March 2013 covering September 2012 – February 2013;
- Developed and administered a questionnaire to OPS/NOC that included questions on reporting statistics for the review period;
- Reviewed ten randomly-selected days' worth of MMC Reports distributed during the review period (536 Reports) for compliance with the April 2013 PIA Update and February 2011 SORN;

- Conducted a site visit to observe the MMC analysts on the watch desks[8] as they monitored public websites, social networks, and blogs. The MMC analysts provided an overview and demonstration of their media monitoring responsibilities;
- Conducted a site visit to the NOC and observed how the MMC reports are uploaded into the NOC Common Operating Picture and subsequently archived;
- Observed a demonstration of the newly-implemented logging mechanism designed to capture information about MMC Analyst's searches of the MMC database; (established in response to the previous PCR recommendation) and reviewed the search log;
- Reviewed the results of 20 monthly self-audit compliance reports conducted by OPS/NOC to ensure appropriate use of the Internet by MMC analysts;
- Reviewed and discussed questionnaire responses with OPS/NOC officials;
- Reviewed current SOPs and the Analyst's Desktop Binder to ascertain the status of OPS/NOC's implementation of recommendations from the May 2012 PCR;
- Reviewed previous PCRs and existing privacy compliance documentation (PIAs and SORN); and
- Reviewed supporting documentation from previous PCRs.

IV. FINDINGS

A. Collection of Information

Requirement: Under this initiative OPS cannot: (1) actively seek PII; (2) post any information on social media sites; (3) actively seek to connect with individual social media users, whether internal or external to DHS; (4) accept invitations to connect from individual social media users whether internal or external to DHS; or (5) interact with individuals on social media sites.

OPS/NOC is permitted to collect PII for the seven specific categories of individuals listed in Table 1 when doing so lends credibility to a MMC Report or facilitates coordination with interagency or international partners. PII on these individuals may include full name, affiliation, position or title, and publicly-available user ID. PII inadvertently or incidentally collected outside the scope of this discrete set of categories of individuals must be redacted immediately before further use and sharing.

[8] The MMC analyst watch is composed of two analysts, one assigned to monitor social media and the other to monitor traditional media activity.

Table 1: Seven Categories of Individuals Whose PII can be included in MMC Reports

Category #	Description
1	U.S. and foreign individuals in extremis, *i.e.*, in 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 posts or articles, or who use traditional and/or social media in real time to provide their audience situational awareness and information;
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, who are killed or found dead.

Review: We reviewed NOC/MMC reporting data from March 1, 2013, to December 31, 2013, including the number of MMC Reports produced overall and those containing PII about the seven permissible categories of individuals. We viewed demonstrations on how the inclusion of PII added credibility to these MMC Reports.

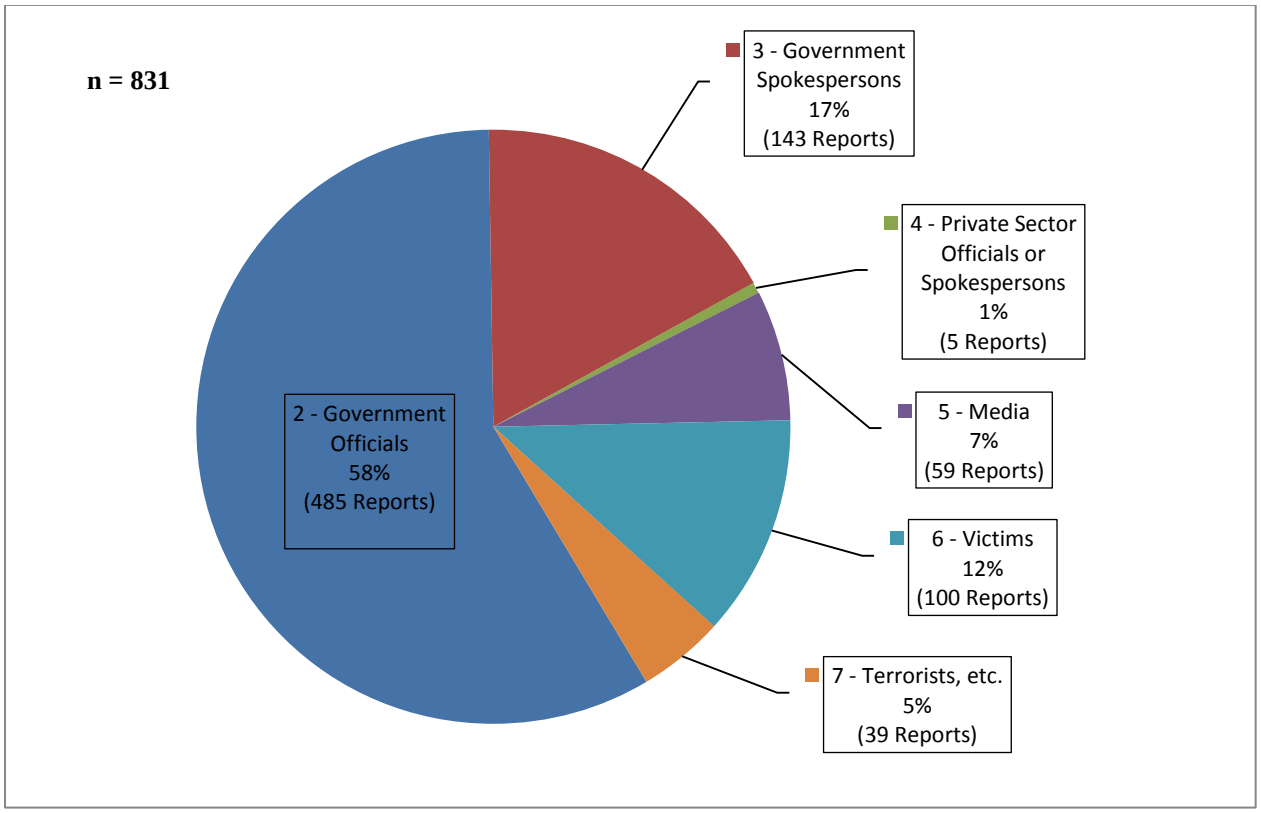
Findings: OPS/NOC continues to comply with the requirements not to actively seek PII in its reporting. From March 1, 2013 to December 31, 2013, the NOC distributed 15,902 MMC Reports of which 818 (five percent)[9] contained PII within the seven permitted categories of individuals identified in the February 2011 SORN. Ninety-five percent of Reports during this

[9] Note: The number of Reports depicted in the figure below (831) is greater than the number of Reports (818) distributed because an MMC Report may include more than one instance of the seven permissible categories of individuals.

period did not contain PII and the majority of Reports that did contain PII (88 percent) fell into Categories 2, 3, and 6 listed above. Figure 1 depicts the distribution of MMC Reports by category of permissible information.

Figure 1: Reports Containing PII by Category of Individual

March 2013 to December 2013



Note: None of the MMC Reports distributed during the review period included PII for individuals in Category 1 (U.S. and foreign individuals *in extremis*).

Use of Authorized PII

The distribution of MMC Reports across categories of permissible PII was largely consistent with our findings in the last PCR. OPS/NOC reduced the number of MMC Reports containing authorized PII by 8 percent over the self-assessment period of September 2012 – February 2013, demonstrating judicious use of authorized PII and increased experience in

providing operationally relevant MMC Reports that do not contain PII. [10] During the current reporting period, the OPS/NOC inadvertently distributed only one report containing unauthorized PII out of the 15,902 total reports.

The reduction in the use of authorized PII can be attributed to a number of processes implemented by OPS/NOC during this PCR period and discussed more fully below, including:

1. closely monitoring the authorized PII usage through a Bi-Monthly PII Review;
2. renewed emphasis on minimizing use of all authorized PII in reports; and
3. use of a URL shortening service

Bi-Monthly PII Review Process

To more closely monitor the use of authorized PII and identify trends, the NOC MMC updated its bi-monthly PII review process. The NOC MMC is now able to easily compare current authorized PII usage against the previous months and PCRs. This provides the NOC MMC leadership with the ability to closely monitor and guide the use of authorized PII.

To enhance the PII review process, the NOC MMC added a step requiring every distributed Report to be reviewed by two analysts (previously the reports were reviewed by one analyst) specifically searching to identify instances of PII. Under this procedure, each analyst reviews the same set of MMC Reports for a given period to identify both authorized PII as well as those that were distributed inadvertently. This helps guarantee that all instances of PII are rapidly identified. Under this approach, PII is identified within two weeks of distribution, allowing the NOC MMC to classify it under an authorized PII category, or issue a redaction if necessary.

Minimizing the Use of Authorized PII When Possible

During the March 2013 self-assessment, the OPS/NOC identified a need to closely monitor the bi-monthly authorized PII usage trends to ensure PII minimization. The previous format of the bi-monthly PII report did not provide a running total or any benchmarks; therefore, it was difficult for OPS/NOC leadership to easily track the overall trends of authorized PII usage. The OPS/NOC has enhanced the bi-monthly report with metrics on the current PCR period and the percentage change from the previous PCR period.

[10] Thirteen (13) percent of MMC Reports for the self-assessment period PCR contained authorized PII; five (5) percent of the MMC Reports issued during the reporting period for this PCR included authorized PII.

The goal of the bi-monthly PII reviews is to verify that authorized PII is used only when it significantly adds credibility or overall value to the MMC Report. To avoid overuse of the authorized PII, the OPS/NOC uses generic terms that are specific enough to identify the source of the information rather than documenting individuals' names or titles. For example, rather than listing a journalist's name, analysts identify him or her as "a reporter" representing a particular network.

Use of URL Shortening Tool to Limit Distribution of PII

In May 2013, the NOC MMC incorporated a URL shortening service to help ensure that PII is not inadvertently included in links used as the source for MMC Reports. The service converts a website address from its normal format to a shortened version comprised of random characters. This service provides a hyperlink to the original source article, while ensuring that PII within links is not accidentally distributed. The process does not change the current procedures that the NOC MMC has in place to ensure that PII is not included in the source links. This procedural change serves only as an additional measure to further support OPS/NOC current efforts. This function does not require any additional effort by the on-watch analysts, because the link is automatically converted when added to the MMC Report Application. This additional safeguard has significantly reduced the potential for inadvertent distribution of PII.

Expansion of Approved PII Category #6

During this PCR period, OPS/NOC was instrumental in reporting social media news and information related to the Boston Marathon bombings. The DHS Privacy Office commends the OPS/NOC on its very limited reporting of PII during the Boston Marathon bombings and subsequent manhunt. As the story unfolded in real-time on social media, the NOC MMC analysts followed their guidance and did not include PII unless operationally relevant.

The OPS/NOC continues to meet its operational obligations while collecting limited PII. Within the small sample reviewed by the DHS Privacy Office, however, we found one MMC Report example during this PCR period that did not fit into any of the seven approved PII categories. This MMC Report described a college shooting in California, and noted that President Obama was also in the area. While this information is obviously relevant to the OPS/NOC's mission to provide situational awareness, the mention of President Obama does not fit into any of the existing PII categories. An expansion of Approved PII Category #6, "Current and former public officials who are victims of incidents or activities related to Homeland Security" to include *potential* victims would remedy this inconsistency.

B. Use of Information

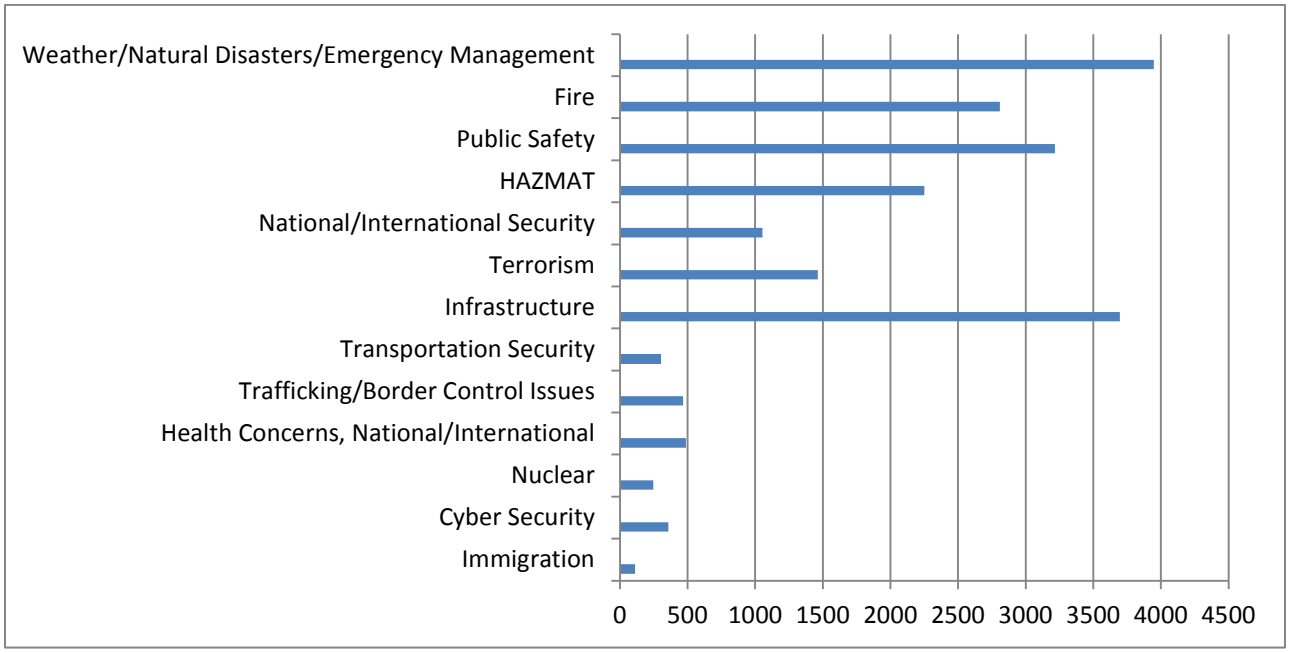
Requirement: The OPS/NOC must monitor only publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and a common operating picture.

Review: We reviewed MMC reporting data from March 1, 2013, to December 31, 2013, including the number of MMC Reports identified in each of the defined 13 reporting event categories. We reviewed ten randomly-selected days' worth of MMC Reports (538 Reports) to identify adherence to the 13 event categories and to determine whether PII contained in the MMC Reports was within one of the seven permissible categories of individuals. We also viewed a demonstration of a newly-implemented logging mechanism, implemented in response to a recommendation from our previous PCR, designed to capture search terms of MMC analysts' searches of the MMC database.

To provide further perspective on the content and scope of Reports produced by the NOC MMC, Appendix A includes randomly-selected Reports reviewed by the DHS Privacy Office dated March 20, 2013; April 15, 2013; May 31, 2013; June 7, 2013; July 28, 2013; August 20, 2013; September 17, 2013; October 29, 2013; November 10, 2013; and December 27, 2013. The Reports reviewed reflect a variety of topics within the 13 categories and any inclusion of PII was found to be within one of the seven permissible categories of PII.

Findings: OPS/NOC has 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. Requiring analysts to identify the particular mission-related category also helps ensure that reporting remains within scope. Figure 2 depicts the distribution of MMC Reports issued during the period by category of event.

Figure 2: Reports by Event Category March 2013 to December 2013



Note: The number of Reports depicted in this figure is greater than the number of Reports (15,902) distributed because an MMC Report may fall into more than one event category (e.g., both the Weather/Natural Disasters/Emergency and Infrastructure categories could be assigned to a Report of a tornado that led to the closing of a stretch of interstate highway).

Geo-location Information

During the PCR site visit, the DHS Privacy Office found that the OPS/NOC is now using GPS and geo-location features offered through social media platforms to enhance their search and reporting capabilities. There are new privacy risks associated with the use of this information by the NOC. The April 2013 PIA Update does not describe the OPS/NOC use of geo-location services.

C. Retention of Information

Requirement: In accordance with the retention schedule and disposal policy established and approved by the OPS/NOC records officer and National Archives and Records Administration (NARA) (NARA #: N1-563-08-23), the NOC retains information for no more than five years.

Review: We discussed MMC retention practices, including the redaction and deletion procedures to be followed when PII outside the seven permissible categories of individuals is included in an MMC Report. As the MMC has not yet operated for five years, the retention schedule limitation period has not yet expired for the oldest MMC Reports.

Findings: In accordance with retention requirements, OPS/NOC maintains a database of all of the Reports distributed. There were no instances of unauthorized collection or dissemination of PII during the review period. Nonetheless, we verified that OPS/NOC has a process in place to redact unauthorized PII from Reports within the MMC.

D. Internal and External Sharing and Disclosure

Requirement: OPS/NOC will share MMC Reports with Departmental and component leadership, and other federal government, state, local, tribal, and territorial agencies as appropriate, to ensure that critical information reaches government decision-makers. Information may also be shared with private sector and international partners where necessary, appropriate, and authorized by law.

Review: OPS/NOC disseminates its MMC Reports via email. We reviewed the MMC Report e-mail distribution list and discussed OPS/NOC practices for keeping this list current. We also conducted a site visit to the OPS/NOC to review how MMC reports are disseminated and archived by the OPS/NOC.

Finding: OPS/NOC continues to comply with its information sharing requirements. A process is in place to determine the need-to-know for MMC Reports, and the distribution list is updated internally as the MMC Initiative receives approval from OPS/NOC leadership to add or remove specific recipients. The distribution list is submitted weekly to NOC senior staff for review and approval.

E. Technical Access and Security

Requirement: OPS/NOC must maintain a log of social media monitoring Internet-based platforms and information technology infrastructure that MMC analysts visit under this initiative. OPS/NOC must also implement auditing at the router level for all outbound http(s) traffic and generate audit reports that will be available to the DHS Privacy Office for each PCR.

Review: We reviewed the results of twenty monthly self-audit compliance reports covering March 2013 through December 2013.

Findings: The OPS/NOC audit capability for all outbound http(s) traffic designed to ensure appropriate use of the Internet by MMC analysts became fully operational in May 2011. The current Self-Audit capability dynamically collects and logs all OPS/NOC MMC traffic, and audits of this traffic are conducted randomly. Since March 2013, OPS/NOC has conducted twenty random audits (two per month) that covered all NOC MMC analysts and documented the results in audit reports. The reports did not identify any inappropriate uses of the Internet by MMC analysts.

F. Privacy Training

Requirement: NOC MMC Analysts are required to take the annual privacy training required of all DHS employees and contractors, as well as job-specific training on protecting PII.

Review: The DHS Privacy Office reviewed OPS/NOC's training log for the initiative and supplemental guidance issued since March 2013.

Finding: The OPS/NOC remains in compliance with training requirements. The OPS/NOC PII training plan is a multi-phase process that begins during a new analyst's orientation and continues with bi-annual refresher courses. All five new analysts hired during this period completed the requisite PII training. During their initial training seminar, analysts were required to read the Privacy Impact Assessment (PIA) and then were provided with MMC report examples to demonstrate how the OPS/NOC minimizes its collection of PII. Once the instruction period was complete, analysts were required to complete a PII examination. Approximately every six months, analysts are required to review the most current PIA and are then engage in a discussion regarding new and existing PII guidance. At the conclusion of this discussion, they are again given the PII examination.

All supplemental guidance issued since the September 2012 PCR has been added to the MMC Standard Operating Procedures and training package. During this period, the OPS/NOC continually reminded analysts in supplemental guidance they cannot report on First Amendment-protected activity. The NOC MMC also provided new supplemental guidance on the use of permissible PII Category 5.[11] Following their bi-monthly privacy reviews, the OPS/NOC leadership determined that analysts required additional guidance and training to reduce the amount of PII collected from members of the media. Since the training and supplemental guidance, the collection of inadvertent PII continues to decrease, with only one instance of inadvertent PII collected this reporting period.

[11] "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."

G. Existing Privacy Compliance Documentation

Requirement: The 2012 PCR for the OPS/NOC MMC states that "[t]he DHS Privacy Office plans to republish the February 2011 SORN to clarify certain language."[12]

Review: A review of the 2012 PCR determined that a requirement to update the February 2011 SORN has not been completed. The Privacy Office reviewed all supporting documentation from the PCR and notes pertaining to the February 2011 SORN. Emails between DHS Privacy Office and the DHS Office of the General Counsel note that the February 2011 SORN requires a technical update to clarify the categories of individuals whose PII the OPS/NOC may include in Reports.

Finding: Permissible PII Category 5 is grammatically incorrect and reads more like a SORN Category of Records than a Category of Individuals. We recommend that Category 5 be redrafted as follows: "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."

III. CONCLUSION

The DHS Privacy Office continues to work collaboratively with the OPS/NOC to ensure implementation of the NOC MMC in a privacy-sensitive manner. At the front end, the DHS Privacy Office established protections to build in privacy through the conduct of PIAs, and we have confirmed compliance through the conduct of several oversight PCRs. OPS/NOC has demonstrated continued compliance with the requirements contained in the January 2011 PIA Update and February 2011 SORN. Since the September 2012 PCR, the DHS Privacy Office updated the January 2011 PIA Appendices to identify representative lists of sites searched and search terms used as part of the MMC. The new PIA was published on April 1, 2013.[13]

The DHS Privacy Office recommends that OPS/NOC take the following steps to continue to improve its ability to demonstrate compliance with privacy requirements:

1. Require the use of the URL shortening service. The OPS/NOC began using a URL shortening service as a pilot in May 2013. The URL shortening service removed all PII contained in links and reduced the overall amount of PII collected. In addition,

[12] See Privacy Compliance Review of the NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative, May 3, 2012 (page 13), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_ops_monitoringinitiative_05082012.pdf.
[13] DHS/OPS/PIA-004(e) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update, April 1, 2013, available at http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning.

since most inadvertent PII is contained in the source links, the use of the URL shortening service will reduce the amount of inadvertent PII collected.

2. Tag all MMC Reports that contain PII. For audit purposes, the NOC MMC should add a field to the MMC Reports database to enable analysts to click whether the MMC Reports contains PII. This will assist the bi-monthly privacy reviews and the PCRs in identifying which MMC Reports contain PII.

3. Update the April 2013 PIA to describe the use of GPS and geo-location tags, specific geo-location data points collected by the NOC, the operational value added by the use of these tools, and how privacy risks are mitigated.

4. Continue to reinforce the operational relevance standard for the use of PII in MMC Reports. Public officials do not need to be included in MMC Report unless doing so provides operational relevance and lends credibility to a Report. For example, consider whether the fact that a Governor toured a disaster area (as opposed to taking an action by issuing a State of Emergency) enhances the MMC Report and is necessary.

5. Report all inadvertent disclosures of PII to the DHS Security Operations Center (SOC), as required by the Privacy Incident Handling Guidance.[14] Include reporting procedures as Supplemental Guidance for MMC Analysts.

In addition, DHS Privacy Office Oversight Team finds the following inconsistencies with existing privacy compliance documentation:

1. Update the February 2011 SORN. Permissible PII Category 5 is grammatically incorrect and reads more like a SORN Category of Records than a Category of Individuals. We recommend that Category 5 be redrafted as follows: "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."

2. Expand permissible PII Category 6, "Current and former public officials who are victims of incidents or activities related to Homeland Security" to include "potential victims."

[14] See DHS Privacy Office Privacy Incident Handling Guidance (PIHG), January 2012, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf. Designed to inform all Department personnel of their obligation to protect PII, it also establishes procedures delineating how they must respond to the potential loss or compromise of PII.

3. Update the February 2011 SORN to include the newly approved records retention schedule, National Archives and Records Administration (NARA) (NARA #: N1-563-08-23).

We discussed these recommendations with OPS/NOC officials and the DHS Privacy Office Compliance Team, who are taking steps to implement them. The DHS Privacy Office has requested a self-assessment for the period of January – June 2014 and will conduct its next full PCR of this initiative in March 2015.

IV. PRIVACY COMPLIANCE REVIEW APPROVAL

Responsible Official

Carl Gramlick
Director, Operations Coordination Division
Office of Operations Coordination and Planning

Approval Signature

Original signed copy on file with DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A – RANDOMLY-SELECTED MEDIA MONITORING REPORTS DISSEMINATED BY THE MMC.

For a copy of the Appendix, please contact the DHS Privacy Office at privacy@dhs.gov.