Privacy Compliance Review
of the
NOC Publicly Available Social Media Monitoring and Situational Awareness Initiative

May 21, 2015

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 and social media sources 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 in reports, the NOC can provide a more comprehensive picture of breaking or evolving events, which are summarized in an Item of Interest report and shared with appropriate federal, state, local, and tribal governments.

Beginning in January 2010, the NOC launched Media Monitoring Capability (MMC) pilots using social media monitoring related to specific mission-related incidents and international events. These pilots were conducted to help fulfill the NOC's statutory responsibility to provide situational awareness and to access potentially valuable public information within the social media realm. 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. These are reflected in published Privacy Impact Assessments[2] (PIA) and a System of Records Act Notice[3] (SORN) that describe appropriate 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.

Currently, 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 Report or facilitates coordination with interagency or international 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;

---

[1] Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).
[2] DHS/OPS/PIA-004 updated May 2015 http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning
[3] DHS/OPS-004 *Publicly Available Social Media Monitoring and Situational Awareness Initiative* Updated May 2015 http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning

5. 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. Public officials, current and former, who are victims or potential victims of a transportation accident or attack; and
7. Known terrorists, drug cartel leaders or other persons known to have been involved in major crimes or terror of Homeland Security interest, who are killed or found dead.

Privacy Compliance Reviews (PCRs) are a key aspect of the layered privacy protections built into the MMC initiative. The PCR is designed to be a proactive and collaborative mechanism to improve a program's ability to effectuate a culture of privacy within the Department and to comply with assurances made in existing privacy compliance documentation and other documents. MMC PCRs and self-assessments have been conducted regularly since August 2010. OPS/NOC has a history of strong compliance in previous PCRs and self-assessments.[4]

In September 2014, OPS/NOC completed its self-assessment of MMC privacy protections covering January – September 2014. In February 2015, the DHS Privacy Office initiated its seventh full PCR, covering the assessment period of January 2014 – February 2015. The DHS Privacy Office developed a questionnaire that included questions on implementing recommendations from previous PCRs and compliance with the SORN and PIAs, interviewed OPS/NOC officials and analysts on their operations and responses to the questionnaire, analyzed guidance/oversight materials, and reviewed selected MMC Reports for compliance.

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 and the February 2011 SORN and has actively implemented recommendations from previous PCRs. 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 or interact with individuals through social media, and to ensure that any PII collected falls within the seven permitted categories of individuals.

  From January 1, 2014 to January 31, 2015, the NOC distributed 20,521 discreet MMC Reports of which 907 (4.4 percent) contained PII within the seven permitted categories of individuals identified in the February 2011 SORN. OPS/NOC continued to reduce the number of MMC Reports containing authorized PII (from five percent in 2013), demonstrating the judicious use of authorized PII and increased experience in providing operationally relevant MMC Reports that do not contain PII.

[4] Find published PCRs here: http://www.dhs.gov/investigations-reviews.

- *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.[5] Our review of 12 randomly-selected days' worth of MMC Reports (643 Reports) found that they reflect a variety of topics within the 13 event categories and any PII included in those reports is within one of the seven permissible categories of individuals.

- *Use of Information* – OPS/NOC MMC uses geographic filters during crises or major events to limit social media search results to only those that are from a specific geographic location. Using geographic fencing (geofencing)[6] reduces the amount of data that must be analyzed and enhances the reliability of the information. Confirming that information is coming from the scene of an incident provides additional corroboration that an event is occurring, and in some instances, lends a higher degree of credibility to the information itself. NOC MMC's use of geo-location searches from various social media sources is associated with the scene of an incident or a disaster, not the individual user. Search results using a geo-location filter only contain social media postings that are submitted within the defined location. As a result of a recommendation made in the 6th PCR (April 16, 2014), the PIA[7] was updated to discuss the privacy risks and mitigation strategy associated with geo-location searches.

- *Technical Access and Security* – The OPS/NOC continues to audit all outbound http(s) traffic to ensure appropriate use of the Internet by MMC analysts. Our review of 26 audits (two per month) that cover all MMC analysts, documented the results in self-audit compliance reports where there were no instances of inappropriate uses of the Internet by MMC analysts.

- *Privacy Training* – The NOC MMC has a robust privacy training regimen and has taken significant steps to create a culture of privacy among its analysts. New and existing analysts are required to take annual privacy training, read current privacy compliance documentation, and participate in discussions on relevant privacy topics. Frequently issued supplemental guidance includes reminders that MMC priorities remain "operational relevance and privacy."

- *Privacy Compliance Documentation* – As recommended in previous PCRs, privacy compliance documentation has been updated to accurately reflect the data retention schedule, to clarify the categories of individuals whose PII MMC analysts may include in Reports, and reflect geo-location searches. The updated PIA and SORN can be found here: http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning.

---

[5] The thirteen categories are: 1) Terrorism, 2) Weather/Natural Disasters/Emergency Management, 3) Fire, 4) Trafficking /Border Control/Border Violence, 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.
[6] Geofencing is a technology that defines a virtual boundary around a real-world geographical area.
[7] DHS/OPS/PIA-004(f)

III. SCOPE AND METHODOLOGY

The DHS Privacy Office conducted its seventh PCR of the OPS/NOC MMC in coordination with OPS/NOC leadership for the period of January 2014 through February 2015. The DHS Privacy Office carried out the following activities:

- Reviewed the OPS/NOC self-assessment submitted in September 2014 covering January – September 2014;
- Developed and administered a questionnaire to OPS/NOC that included questions on reporting statistics for the review period;
- Reviewed 12 randomly-selected days' worth of MMC Reports distributed during the review period (643 Reports);
- 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;
- Reviewed the results of 26 monthly self-audit compliance reports conducted by OPS/NOC to ensure appropriate use of the Internet by MMC analysts;
- Reviewed the results of 26 bi-monthly PII Review Reports on the appropriate use and disclosure of PII and reviewed sample MMC Reports for each category used during this time period that demonstrate how inclusion of PII lends credibility to the Report;
- Reviewed 643 random MMC Reports looking for the seven categories of individuals releasable;
- Reviewed customer distribution list to assess target audience;
- Confirmed that the over 370 Twitter accounts followed by NOC MMC are not linked to individuals but only to local, state and federal government agencies and local, state, regional, national and international media outlets;
- Reviewed supplemental guidance and training curriculum;
- 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 April 2014 PCR; and
- Reviewed previous PCRs and existing privacy compliance documentation (PIAs and SORN).

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.

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

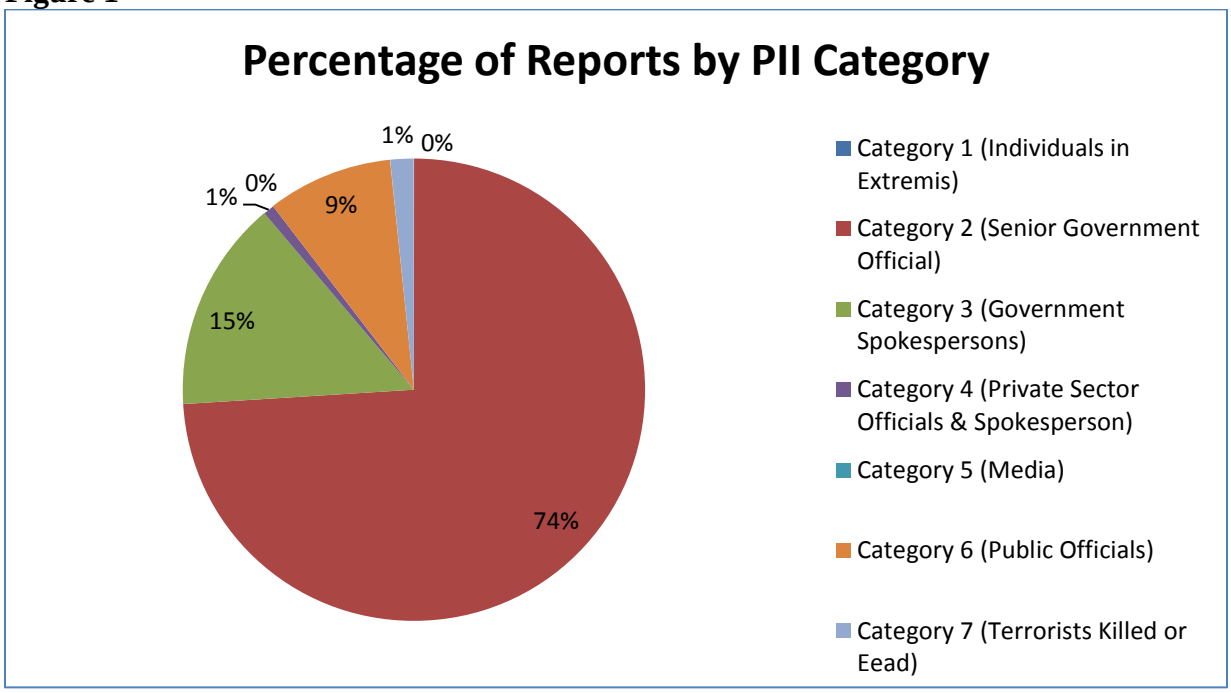
OPS/NOC is permitted to collect PII for the seven specific categories of individuals listed in the Background Section above when doing so adds value and lends credibility to a MMC Report or facilitates coordination with interagency or international partners. PII on these individuals may include full 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. If PII is inadvertently included in a NOC MMC distribution, a multi-step notification and redaction process is implemented to ensure that reports are corrected. An email deletion advisory is sent to the NOC MMC team and the full distribution list notifying them that the PII must be deleted from the errant Report. Explicit instructions are provided on how to amend a Report including how to replace the offending PII with "[Removed Due To PII]" in any saved or redistributed reports.

Review: We reviewed NOC/MMC reporting data from January 2014 to February 2015, including the number of MMC Reports produced overall and those containing PII about the seven permissible categories of individuals. While the overall percentage was very small (4.4 percent), the Privacy Office reviewed samples of MMC Reports that included PII to confirm how its inclusion added credibility to these Reports. For example, when a Report includes "The President on Thursday signed a disaster declaration for … " or "the Chief Executive Officer of Lindt Australia has spoken to the media regarding…," including information on the speaker lends credibility to that Report.

Findings: OPS/NOC continues to comply with the requirements not to actively seek PII in its reporting and takes great care to only include PII that falls within one of the seven permissible categories and provides operational value. A multi-step quality control process is used to ensure PII is not inadvertently included or retained in Reports. If allowable PII is included in a Report, the MMC analyst utilizes a drop down menu in the NOC MMC Report Application to select one of the seven permitted categories of individuals. This drop down menu tags the report in the MMC's database as including PII, allowing the system to be audited for appropriate use.

From January 2014 to February 2015, the NOC distributed 20,521 discreet MMC Reports of which 907 (4.4 percent) contained PII within the seven permitted categories of individuals identified in the February 2011 SORN. The vast majority of Reports that contained PII (74 percent) fell into Category 2 (Senior Government Official) with a distant second from Category 3 (Government Spokespersons) at 15 percent (see Figure 1).

Figure 1



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 continued to reduce the number of MMC Reports containing authorized PII – 4.4 percent during the reporting period (compared to five percent for the last PCR) – demonstrating thoughtful use of authorized PII and increased experience in providing operationally relevant MMC Reports that do not contain PII. During the current reporting period, out of the 20,521 total reports, the OPS/NOC inadvertently distributed one report containing unauthorized PII. A private individual's Twitter handle was superimposed onto a photograph that was included in a published Report. The NOC MMC Quality Control process uncovered the inadvertent distribution that same day and the analyst and Watch Lead notified NOC MMC leadership to implement the mitigation process. An email deletion advisory was sent to the NOC MMC team and the full distribution list informing them of the process on how to delete the PII. Additionally, the IT administrator accessed and removed the PII permanently from the NOC MMC database.

Bi-Monthly PII Review Process

The NOC MMC continued its bi-monthly PII review process to closely monitor the use of authorized PII and identify trends. The NOC MMC can 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.

The NOC MMC requires every distributed Report to be reviewed by two analysts to identify any instances of PII inclusion. Under this procedure, each analyst reviews the same set of MMC

Reports for a given period to identify both authorized PII and any PII that was distributed inadvertently. This helps guarantee that all instances of PII are rapidly identified. Each Report is then approved by the shift's Watch Lead prior to distribution. Additional reviews and oversight include a daily check by the NOC MMC Senior Reviewer, a weekly check by NOC MMC's Quality Control leads, and a bi-monthly review of all distributed Reports to check for authorized or unauthorized PII.

Minimizing the Use of Authorized PII When Possible
NOC MMC Analysts are continually provided instruction on identifying PII and what information can be included under the seven categories of permissible PII. Before distributing Reports, analysts first identify and carefully consider any PII information in media sources before making a decision on whether such information adds value or lends credibility to the 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, using the term "Vermont Governor" as opposed to the name of the governor when reporting on ice storm damage in January 2014. Emphasis continues to be on "operational relevance and privacy."

Use of URL Shortening Tool to Limit Distribution of PII
The NOC MMC continues to utilize 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 integration of the bit.ly URL-shortening service for citing sources has reduced the risk of inadvertent PII distributions.

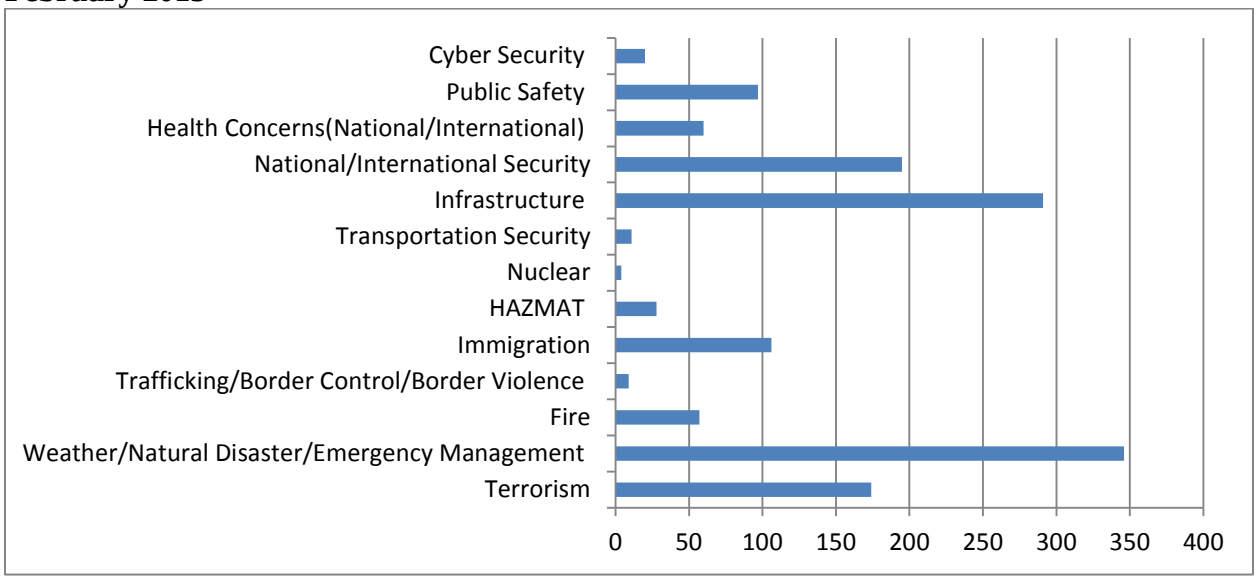
B. Use of Information
Requirement: The OPS/NOC must monitor only publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and a common operating picture.

Review: We reviewed MMC reporting data from January 2014 to February 2015 including the number of MMC Reports identified in each of the defined 13 reporting event categories. We reviewed 12 randomly-selected days' worth of MMC Reports (643 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 reviewed the social media accounts utilized by MMC analysts to confirm the accounts are not linked to individuals but to local, state, federal and international government entities or media outlets.

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 that contain authorized PII[9].

Figure 2: Reports by Event Category that contain Authorized PII from January 2014 to February 2015



Note: Out of 28,304 total Reports, including Reports that 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), 1,398 contained authorized PII.

Geo-location Information

Review: The May 2015 PIA Update describes the OPS/NOC use of geo-location services, which include the use of GPS and geo-location features offered through social media platforms to enhance their search and reporting capabilities.

Findings: A NOC MMC analyst accomplishes a geo-location search by defining three geographic parameters (latitude, longitude, and radius) of a location of interest. This location of interest is a physical location (for example, disaster location, school, airport, etc.), not the location of a specific user/individual. Geo-filtering enables the NOC MMC analyst to efficiently organize and view returned search results to significantly enhance the reliability of the information. The NOC MMC does not store geo-location data used in searches and analysts are trained on the proper use of geo-location searches.

[9] The top three reported categories of events overall in 2014 were weather/natural disaster/emergency management, infrastructure and public safety. The top three overall in 2015 were infrastructure, weather/natural disaster/emergency management and public safety.

C. Retention of Information

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

Review: The MMC has not yet operated for five years; therefore the retention schedule limitation period has not yet expired for the oldest MMC Reports. The NOC MMC will begin purging reports older than five years beginning in August 2015.

Findings: In accordance with NARA approved retention requirements, OPS/NOC maintains a database of all of the Reports distributed. An implementation plan to appropriately dispose of records in accordance with the records schedule should be finalized before August 2015, at which time privacy compliance documentation should also be updated.

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. We reviewed the process to redact Reports that inadvertently include PII and one example of a redaction. When unauthorized PII is inadvertently included in a distributed Report, a multi-step notification and redaction process is implemented.

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, including an approval requirement by NOC management. While periodic reviews of the Distribution List are conducted to ensure that no private address are included in NOC MMC reporting, we recommend that closer reviews of the Distribution List may be required to clear out email addresses of employees that have left DHS or other government agencies or who no longer have a need-to-know the information.

A demonstration during the site visit showed how the notification and redaction process works. Upon discovery, NOC MMC and OPS NOC leadership are notified. A request for authorization to send an "email deletion advisory" to the entire NOC MMC team and the full distribution list notifying them that the PII must be deleted from the Report is made. Explicit instructions on how to remove the unauthorized PII from the Report as well as how recipients delete the report are provided. NOC MMC includes the Security Operations Center on any redaction notifications as part of its Standard Operating Procedures.

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 26 monthly self-audit compliance reports covering January 2014 to February 2015.

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

F. Privacy Training

Requirement: NOC MMC Analysts are required to take annual privacy training as well as job-specific training on protecting PII.

Review: The DHS Privacy Office reviewed OPS/NOC's training materials and logs for the initiative and supplemental guidance issued since January 2014.

Finding: The OPS/NOC has implemented a robust multi-phased approach to training. The OPS/NOC PII training plan begins during a new analyst's orientation and continues with bi-annual refresher courses. The seven new analysts hired during this review period completed the requisite PII training. During their initial training seminar, analysts are 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 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 April 2014 PCR has been added to the MMC Standard Operating Procedures, Analyst's Desktop Binder, and training package. During this review period, the OPS/NOC continually reminded analysts in supplemental guidance that their priorities remain "operational relevance and privacy" and that they cannot report on First Amendment-protected activity.

G. Updated Privacy Compliance Documentation

Requirement: Current privacy compliance documents address privacy risk mitigation strategies for the NOC MMC.

Review: The May 2015 SORN and Privacy Impact Assessment updates[10] sufficiently mitigate privacy risks associated with the NOC MMC, including recent updates to address geo-location searches and to clarify the categories of individuals whose PII the OPS/NOC may include in Reports.

Finding: While updates to the PIA and SORN occurred during the course of this review, we found that NOC MMC updated its Standard Operating Procedures to reflect recommendations from previous PCRs and had operationalized these recommendations while waiting for updates to the compliance documentation.

V. CONCLUSION

The DHS Privacy Office commends the OPS/NOC for creating a culture of privacy within the MMC and for operating the NOC MMC in a privacy-sensitive manner. The DHS Privacy Office confirms that the OPS/NOC continues to demonstrate compliance with the requirements contained in the April 2013 PIA Update and February 2011 SORN.

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. Move to DHS Privacy Training – While the Privacy Office commends OPS/NOC for ensuring its MMC analysts receive appropriate privacy training, we recommend that analysts take DHS hosted privacy training to ensure that all DHS privacy policy and best practices are conveyed to the analysts in a timely fashion. This training can be accessed by outside contractors via a new external site: https://edit.dhs.gov/dhs-security-and-training-requirements-contractors (see our course at the bottom of the page: Privacy at DHS: Protecting Personal Information).

2. Fully Implement NARA Approved Records Retention Schedule – NOC MMC should complete its records retention schedule before August 2015, review this schedule annually, and update the schedule as necessary going forward. NOC MMC should update its privacy compliance documentation, as appropriate, once records retention schedule is implemented.

3. Keep Distribution List Current – While the NOC MMC Distribution List is frequently changing, we recommend that regular audits of the List occur to remove inactive emails, ensure all receivers of the Reports have an operational need-to-know, and to decrease the impact of any potential PII breaches.

[10] See all PIAs and the 2015 SORN under DHS/OPS/PIA-004 - Publicly Available Social Media Monitoring and Situational Awareness Initiative here: http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning.

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 requests the NOC MMC continue semi-annual self-assessments for the next 18 months (February - July 2015, August 2015 – January 2016, and February – July 2016) and will conduct its next full PCR of this initiative in August 2016.

VI. 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