Privacy Compliance Review of the National Operations Center Publically Available Social Media Monitoring and Situational Awareness Initiative

December 8, 2017

Contact Point

Carl Gramlick
Director, Operations Coordination Division
Office of Operations Coordination
(202) 282-8611

Andrew Akers
Supervisor, NOC-West Team
National Operations Center
Office of Operations Coordination
(703) 464-7645

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

I. Background

The Office of Operations Coordination (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 only including pre-approved personally identifiable information (PII) categories when appropriate in reports, the NOC can provide a more comprehensive picture of breaking or evolving events. These reports are summarized in an Item of Interest report and shared with appropriate federal, state, local, and tribal governments, while protecting individuals' privacy.

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 Notice[3] (SORN) that describe appropriate collection and dissemination of PII in a 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 report (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;

---

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

4. U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates;
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 (PCR) 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 ensure programs operate in compliance with federal privacy laws, departmental policies, and assurances made in existing privacy compliance documentation and other documents. MMC PCRs and self-assessments have been conducted regularly since August 2010 and OPS/NOC has demonstrated a history of strong privacy compliance over that time.[4]

The last full PCR was completed in May 2015, which resulted in three recommendations to improve privacy compliance and requested that the NOC MMC continue semi-annual self-assessments for the following 18 months.[5] OPS/NOC completed self-assessments of MMC privacy protections and submitted reports to the DHS Privacy Office in March 2016 and September 2016 that noted follow-up actions and the status of implementation of the May 2015 PCR recommendations. To launch this eighth PCR, the DHS Privacy Office reviewed OPS/NOC self-assessments, 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. Scope and Methodology

Scope

As noted in DHS Instruction 047-01-004 Chief Privacy Officer Privacy Compliance Review,[6] PCRs may result in recommendations to change program or system practices or update privacy documents, or result in informal discussions on lessons learned or formal internal or publicly

[4] Previous PCRs of the MMC *available at*: https://www.dhs.gov/publication/privacy-compliance-reviews-media-monitoring-initiative.
[5] May 21, 2015 NOC MMC PCR *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-pcr-mmc-7-20150521.pdf.
[6] Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews, January 2017, *available at*: https://www.dhs.gov/sites/default/files/publications/Instruction%20047-01-004%20Chief%20Privacy%20Officer%20Privacy%20Compliance%20Reviews.pdf.

available reports. Given seven previous PCRs and the NOC MMC's biannual self-audits, the scope of this PCR focused on the use and dissemination of social media information within the NOC MMC as defined in privacy compliance documents, as well as in the NOC's standard operating procedures (SOP).

Methodology

This was the eighth PCR conducted by the DHS Privacy Office and in coordination with NOC MMC system and program managers, subject matter experts, and the OPS Privacy Office. This review was organized according to the DHS Fair Information Practice Principles (FIPPs) framework.[7] Our review considered activities for the period of August 2016 through June 2017. The DHS Privacy Office carried out the following activities:

- Reviewed previous PCRs and existing privacy compliance documentation (PIAs and SORN);
- Reviewed the OPS/NOC self-assessments submitted in March and September 2016;
- 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 (120 reports reviewed – 10 randomly selected from each date) looking for allowable PII and the seven categories of individuals releasable;
- 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 11 monthly self-audit compliance reports conducted by OPS/NOC to ensure appropriate use of the internet by MMC analysts;
- Reviewed the results of 22 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 customer distribution list to assess target audience;
- Confirmed that 379 Twitter accounts (up from 372 as reported in PCR #7) 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 the totality of OPS/NOC responses to ascertain the implementation status recommendations from the May 2015 PCR; and
- Reviewed current SOP to randomly test internal controls.

[7] DHS Policy Directive 140-06 (Privacy Policy Guidance Memorandum 2008-01) "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security" (December 29, 2008), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[8] The MMC analyst watch is composed of two analysts, one assigned to monitor social media and the other to monitor traditional media activity.

III. Findings

A. Implementation Summary of Previous Recommendations (May 2015 PCR)

The DHS Privacy Office finds that OPS/NOC continues to be in compliance with the privacy requirements identified in the relevant PIAs and the May 2015 SORN and has actively implemented recommendations from previous PCRs.

Finding: NOC MMC implemented the three May 2015 PCR Recommendations

There were three recommendations from the seventh PCR: (1) move to DHS Privacy Training; (2) fully implement National Archives and Records Administration Approved Records Retention Schedule; and (3) keep customer distribution list current.

NOC MMC utilizes the DHS-hosted privacy training for all contractors. NOC MMC contractors (who do not have access to DHS servers) receive and are required to complete DHS-hosted privacy training annually. NOC MCC provided the DHS Privacy Office training dates and confirmed completion by all contractor staff.

According to DHS/OPS/PIA-004(f), MMC Reports are maintained for five years and then deleted. The NOC MMC Contracting Officer's Representative (COR) directed the purge of 5-year old reports beginning in the first week of November 2015 for MMC Records dating from August 2015 through October 2015. Monthly purges have occurred since. The DHS Privacy Office reviewed the NOC MMC NARA deletion notice and full log of removals (as of July 7, 2017, over 32,000 MMC Reports were deleted).

NOC MMC forwards a potential customer to the NOC MMC COR, who approves or disapproves all requests to be added to the distribution list. No addresses are added unless approved by the Director of the Operations Coordination Division, Director of the National Operations Center, or the NOC MMC COR. The distribution list is periodically reviewed to ensure that no private addresses are included on the NOC MMC distribution list. DHS Privacy Office review of the MMC customer distribution list confirmed that addresses (whether international, group distribution, or individual) are .gov, .mil, or other official federal, state, or local government address.[9]

B. Summary of Current Findings

The DHS Privacy Office commends the NOC MMC for its vigorous and continuous quality control process. As noted in the 2015 PCR, the Geofencing (i.e., the creation of a virtual geographic boundary as discussed in April 2013 PIA Update) procedures continue to respect the privacy of individuals by using a location filtering system that does not provide a special set of meta-data. The location used in Geofencing is a physical location related to the Item of Interest

[9] The exception is the American Red Cross, which is a charitable organization, not a government agency, which assists people following disasters.

being reported (e.g., disaster location, school, airport), not the location of a specific user/individual. MMC online search platforms use filtering that finds online articles for that location as well as of news organization reporting from the location of the event.

The DHS Privacy Office notes that the distribution of MMC Reports across categories of permissible PII continues to decrease. OPS/NOC continued to reduce the number of MMC Reports containing authorized PII down to 2.54 percent during the reporting period compared to 4.4 percent for the last PCR. This affirms the considered use of authorized PII and increased experience providing operationally relevant MMC Reports that do not contain PII. During the site visit, NOC MMC analysts reported that protecting and minimizing PII neither hinders the NOC MMC mission nor the efficiency and quality of their work. The DHS Privacy Office commends OPS/NOC for steps taken to reduce the use of PII while remaining operationally effective.

While the DHS Privacy Office recognizes NOC MMC robust effort towards privacy compliance, the following specific findings provide additional room for improvement:

1. NOC MMC internal policy controls for breaches do not reflect current DHS policy and best practices.
2. OPS Privacy Officer does not have an active collaboration and oversight role in the NOC MMC and OPS is not fully implementing the requirements for Component Privacy Officers.
3. Current MMC contract does not contain the two new required Homeland Security Acquisition Regulation (HSAR) Clauses.

C. Summary of Recommendations

The DHS Privacy Office notes OPS NOC MMC compliance with privacy requirements of federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by OPS in existing privacy compliance documentation. Furthermore, OPS NOC engages in privacy best practices in conducting the MMC. Based on our findings, the DHS Privacy Office makes the following recommendations:

1. OPS should fully implement DHS Instruction 047-01-008, DHS Privacy Incident Handling Guidance.[10] OPS Privacy Officer must follow up to see that there is a reasonable assurance that a NOC MMC PII spill (however rare) will ultimately be reported to DHS Enterprise Security Operations Center.

[10] DHS Instruction 047-01-008, Privacy Incident Handling Guidance, October 2017, *available at*: https://www.dhs.gov/publication/privacy-incident-handling-guidance.

2. OPS should fully implement DHS Instruction 047-01-005 for Component Privacy Officers[11] to oversee privacy compliance, policy, and oversight activities in general and to ensure the internal NOC MMC controls keep pace with existing DHS privacy policy and best practices.

3. As a best practice, OPS Privacy Officer should test the general incident reporting procedures for suspected or confirmed breaches as well as identify appropriate mitigations and lessons learned.

4. OPS Privacy Officer should coordinate with NOC MMC when conducting self-audits to ensure that current DHS-wide privacy guidance is implemented by the NOC MMC.

5. OPS Privacy Officer should work with the NOC MMC COR and the DHS Privacy Office to ensure that all contract renewals or modifications contain new HSAR clauses and are also consistent with recent FAR Clauses.

D. Analysis of Findings

Finding 1: Current MMC PII breach internal controls do not reflect current DHS policy and best practices.

DHS Instruction 047-01-008, Privacy Incident Handling Guidance, defines a privacy incident or breach as encompassing both suspected and confirmed incidents.[12] Any breach involving PII is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an unauthorized purpose. DHS personnel (including DHS contractors) should not disclose or cause to be disclosed any information to any person who does not have a need-to-know.

DHS Instruction 047-01-008 defines the Department's privacy incident management processes, which applies to all DHS employees and contractors (DHS personnel). The Instruction emphasizes that all suspected or confirmed breaches (minor and major incidents) must be reported. The DHS Component Privacy Officer and the Component Security Operations Center (SOC) are required to immediately consult and evaluate the incident upon receipt of the preliminary report. If the facts confirm that a privacy incident may have occurred, then the Component Privacy Officer or Component SOC must open a privacy incident report in the DHS Online Incident Handling Database.

---

[11] DHS Instruction 047-01-005 for Component Privacy Officers, February 2017, *available at*: https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-005-component-privacy-officers.
[12] See also Office of Management and Budget Memorandum M-17-12, "Preparing for and responding to a Breach of Personally Identifiable Information." (Jan. 3, 2017).

According to MMC Standard Operating Procedures (SOP) and responses about current practice provided during the PCR, notice of an unauthorized PII disclosure is sent to the Immigration and Customs Enforcement (ICE) SOC[13] concurrently with an email deletion advisory that is sent to the full distribution list. The emailed deletion advisory directs the recipient to permanently delete the MMC Report because it included unauthorized PII. The advisory provides a general description of how to permanently delete the MMC Report in Outlook and who to contact with questions for programs other than Outlook. The DHS Privacy Office finds there is a gap, however, between the incident reporting criteria stated in the NOC MMC SOP, and the actual MMC PII breach reporting process. Furthermore, MMC PII breaches have not been officially reported and documented in the Department's incident website.

As part of this PCR, the NOC MMC provided an example of the practice for discerning whether or not there has been an inadvertent release of PII; what the DHS Privacy Office would consider a privacy incident. The DHS Privacy Office discussed this example and the NOC MMC SOP with responsible SOCs, which included the ICE SOC (as identified in the MMC SOP to assist with MMC PII incident remediation) and the DHS Enterprise Security Operations Center (ESOC) (which is the principal SOC responsible for breach response across the Department). Neither ICE SOC nor DHS ESOC were aware of the NOC MMC breach process SOP, nor was this incident in any of their records. The practice also did not include the OPS Privacy Officer as part of the mitigation process. Although it was ultimately concluded that the PII used in the provided example fell into an approved PII category and was therefore deemed not to be an incident, any breach mitigation must include the OPS Privacy Office and appropriate SOC, revealing deficiencies in the MMC SOP.

While there have been no recent PII breaches, the NOC MMC breach process reflects a lack of adherence to official DHS policy and introduces a serious risk of mishandling an incident.

The ability to spot a potential incident and the willingness to report it appropriately complies with official guidance and helps DHS maintain public trust. Fully implementing DHS Instruction 047-01-008 and reporting to department program supervisors, Component Privacy Officers, or responsible SOCs at a minimum, spurs rapid action and mitigation. Using the Department's central repository also fosters unity of effort, promotes the ability to obtain quick advice, and leads to better communication regarding decisions and guidance, accurate record keeping, and lessons learned and best practices.

NOC MMC self-audits[14] report that the last inadvertent PII releases requiring email deletions and additional redactions occurred in 2012 (one incident) and 2013 (three incidents). However, DHS ESOC could not locate those events in the DHS online incident reporting database, Enterprise Operation Center (EOC). Although the 2015 PCR did not identify shortcomings in the NOC MMC breach response process and there have been no identified PII breaches in the current

[13] The ICE SOC is not responsible for managing incidents for OPS. DHS Headquarters Component Incident Response Team (HQ CIRT) is responsible for OPS as well as a select few other components.
[14] Provided to the DHS Privacy Office in March 2016 and September 2016.

review period, NOC MMC should review its SOPs and current practice to ensure full compliance with DHS Instruction 047-01-008. While the NOC MMC demonstrated it takes steps to mitigate inadvertent PII disclosures, the Instruction requires DHS personnel to initiate the privacy incident response process as noted above. DHS ESOC ultimately documents the evaluation, investigation, and any subsequent mitigation efforts in the EOC. When properly reported, an incident file number is assigned in the DHS Online Incident Handling Database. Together, DHS ESOC and the OPS Privacy Office can then oversee email purges, verify completion of remediation plans, and verify that all other necessary mitigations are resolved as appropriate. The DHS Privacy Office tracks all breaches and is required to report annually to Congress.

The DHS Privacy Office encourages OPS to fully implement DHS Instruction 047-01-008 and can assist with EOC training, implementation of the required reporting procedures (i.e., documentation, investigation, identifying appropriate mitigations), and testing NOC MMC general incident reporting controls, as appropriate.

Finding 2: OPS Privacy Officer (or PPOC) does not have an active collaboration and oversight role in the NOC MMC and OPS is not fully implementing the requirements for Component Privacy Officers.

DHS Instruction 047-01-005 for Component Privacy Officers requires OPS to oversee privacy compliance, policy, and oversight activities in coordination with the Chief Privacy Officer and lays out specific responsibilities of a Component Privacy Officer.[15] In the course of our review, the DHS Privacy Office observed that the OPS Privacy Office was not actively engaged with NOC MMC as envisioned by the Instruction. Specifically, item 7 requires the Component Privacy Officer to "implement and manage the privacy incident management process for suspected or confirmed incidents involving loss or unauthorized access and disclosure of PII in the possession or control of Component." To further the discussion of implementation of DHS Instruction 047-01-008, OPS Privacy Officer should test the general incident reporting procedures for suspected or confirmed breaches as well as identify appropriate mitigations and lessons learned.

While NOC MMC has demonstrated effective self-regulation of privacy compliance, better engagement with the OPS Privacy Office would ensure the Department's privacy best practices are incorporated and current policies are implemented. Additionally, the OPS Privacy Office should assume oversight responsibilities to monitor NOC MMC privacy compliance and engage more frequently with NOC MMC to also ensure internal controls keep pace with technological advances and that the NOC MMC training manual continues to refer to current DHS PII guidance.

Finding 3: Current MMC contract does not contain the two new required Department HSAR Clauses: Safeguarding of Sensitive Information and Information Technology Security and Privacy Training.

[15] See IV. C. 1-10.

According to the March 2015 Chief Procurement Officer's memo regarding Class Deviation 15-01 from the Homeland Security Acquisition Regulations (HSAR)[16], all contracts that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals require applicable Privacy Act language and sufficient OMB policy language that is enforceable on the contractor and its employees. These were dubbed "new special clauses" in the March 2015 memo in which there are also detailed requirements for the new HSAR Clauses.

NOC MMC COR explained that due to the timing of the most recent contract award and the official issue date of the two new clauses, the required clauses were not included in the existing DHS Privacy Systems Engineering and Technical Assistance contract. While NOC MMC is aware of the new special clauses, no steps have been taken to amend the existing contract. DHS Privacy Policy and Compliance Directive 047-01[17] requires Component Heads to ensure that Component contracts for activities that involve PII or otherwise impact the privacy of individuals include appropriate language requiring that Department contractors follow DHS privacy policy and this Directive. When preparing future contracts or renewals, NOC MMC should work with the OPS Privacy Officer to ensure that the new HSAR Clauses regarding incident handling and training are inserted.

Recommendations:

1. OPS should fully implement the responsibilities of DHS Instruction 047-01-008, Privacy Incident Handling Guidance. OPS Privacy Officer must follow up to see that there is a reasonable assurance that a NOC MMC PII spill (however rare) will ultimately be reported to DHS ESOC.

2. OPS should fully implement the responsibilities of DHS Instruction Number 047-01-005 to oversee privacy compliance, policy, and oversight activities in general and to ensure the internal NOC MMC controls keep pace with existing DHS privacy policy and best.

3. As a best practice, OPS Privacy should test the general incident reporting procedures for suspected or confirmed breaches as well as identify appropriate mitigations and lessons learned.

---

[16] DHS published modifications to the HSAR**.** There are three regulatory coverages to address contractor requirements for breach response: one clause for Controlled Unclassified Information (CUI), one for Privacy Training, and one for IT training. The Federal Acquisition Regulatory Council, in coordination with OMB will soon issue standard clauses that DHS will insert in future contractor Statement of Work and Performance Work Statements, *available at*: https://www.dhs.gov/sites/default/files/publications/HSAR%20Class%20Deviation%2015-01%20Safeguarding%20of%20Sensitive%20Information.pdf.

[17] Privacy Policy and Compliance Directive 047-01, July 2011, *available at*: https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01.

4. OPS Privacy Officer should coordinate with NOC MMC when conducting self-audits to ensure that supplemental DHS-wide privacy guidance is implemented by the NOC MMC.

5. OPS Privacy Officer should work with the NOC MMC COR and the DHS Privacy Office to pursue a contract modification now, and then ensure that all subsequent contract renewals contain the new HSAR clauses and are also consistent with recent FAR Clauses.

IV. Conclusion

This PCR provided the DHS Privacy Office with valuable insight into the privacy protective practices employed by the NOC MMC. The DHS Privacy Office finds that OPS NOC MMC is an outstanding example of an office with a healthy privacy culture and their commitment to protecting PII is evident.

Finding that the NOC MMC incident reporting internal control process does not comply with existing DHS policy, however, does raise concerns. Although internal audits report that there have been no recent PII breaches, the finding is still relevant because it reflects a lack of adherence to official DHS policy and introduces a serious risk of mishandling an incident. To serve and support the NOC MMC, the DHS Privacy Office recommends that the OPS Privacy Officer immediately discuss incident reporting options with the HQ Component Incident Response Team, known as HQ CIRT, and DHS ESOC. Once new internal controls are arranged, NOC MMC analysts should be informed and trained and the NOC MMC SOP can be updated.

The DHS Privacy Office requirement for future PCRs will be determined through discussions involving both operational staff and OPS Privacy Office, and will be reflected in future PIA updates, as appropriate. As such, the DHS Privacy Office requests that the OPS Privacy Office:

- monitor the implementation of the recommendations of this PCR, and
- provide a written report on the implementation status of all recommendations within six months of this PCR's publication date. For any recommendations not implemented in that timeframe, or that the OPS NOC chooses not to implement, including any best practice recommendations, we request that OPS Privacy explain why the recommendation was not implemented.

The DHS Privacy Office appreciates OPS NOC, OPS Privacy, and NOC MMC personnel and contractors for assistance and cooperation during this PCR and looks forward to working with OPS Privacy to oversee implementation of the PCR recommendations.

V. 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 the DHS Privacy Office.]

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security