



Privacy Compliance Review
of the
NOC Media Monitoring Initiative

November 15, 2011

Contact Point

Donald Triner

**Director, Operations Coordination Division
Office of Operations Coordination and Planning
202-282-8611**

Reviewing Official

**Mary Ellen Callahan
Chief Privacy Officer**

**Department of Homeland Security
(703) 235-0780**



I. SUMMARY

The Department of Homeland Security (DHS) Office of Operations Coordination and Planning (OPS), including the National Operations Center (NOC), launched the Social Networking/Media Capability (SNMC) to assist DHS and its components involved in the response, recovery, and rebuilding effort resulting from the earthquake and after-effects in Haiti¹ as well as the security, safety, and border control associated with the 2010 Winter Olympics.² These limited purposes were expanded in June 2010³ to meet the operational needs of the Department. Since then, and to meet its statutory requirements,⁴ OPS, through SNMC analysts, monitored publicly available online forums, blogs, public websites, and message boards to collect information used in providing situational awareness and establishing a common operating picture.

The DHS Privacy Office (PRIV) and OPS/NOC decided to further broaden the program's capability to collect additional information, including limited instances of personally identifiable information (PII). As such, a Publicly Available Social Media Monitoring and Situational Awareness Initiative Privacy Impact Assessment (PIA) Update⁵ and new DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records Notice (SORN)⁶ were issued on January 6, 2011 and February 1, 2011 respectively and are the basis for this Privacy Compliance Review (PCR).

PRIV found OPS/NOC to be in compliance with the privacy parameters set forth in the January 6, 2011 PIA update and February 1, 2011 SORN.

II. SCOPE

On August 22, 2011, PRIV conducted a PCR to review OPS/NOC SNMC analyst activities as they related to the January 6, 2011 PIA update and February 1, 2011 SORN. The PCR was attended by OPS and NOC leadership including: Donald Triner (Director, Operations Coordination Division), Carl Gramlick (NOC Director), Raymond Cole (Senior OPS Advisor), Brad Duty (MMC Program Manager), and Jae in Yoon (Associate Director, IT). The PCR was led by Rebecca Richards (Director of Privacy Compliance), Eric Leckey (Associate Director for Privacy Compliance), and Catherine Bauer (Privacy Analyst). PRIV carried out the following activities for this PCR:

- i. In advance of the PCR, PRIV sent a questionnaire to OPS/NOC which included questions regarding the initiative and the focus of the PCR.

¹ http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_haiti.pdf

² http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_2010winterolympics.pdf

³ http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf

⁴ Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)).

⁵ http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf

⁶ <http://edocket.access.gpo.gov/2011/2011-2198.htm>



- ii. PRIV conducted a site visit of the SNMC analyst and watch desks⁷ to observe the SNMC analysts monitoring public websites, social networks, and blogs. The SNMC analysts provided an overview and demonstration of their responsibilities with regards to monitoring media.
- iii. PRIV observed a demonstration of the Automated Syslog Audit System⁸ and discussed with OPS/NOC leadership the approach to locating, analyzing, and documenting data from unique destinations.
- iv. PRIV discussed with OPS/NOC leadership the development and implementation of the Standard Operating Procedure (SOP) for the Media Monitoring Capability (MMC) Self-Audit Compliance.
- v. OPS/NOC leadership provided PRIV with the *PCR Official's Binder* which houses a snapshot of PCR activities, including the presentation for the Automated Syslog Audit System, written responses to the questionnaire, SNMC analyst training materials, and audit logs.

III. FINDINGS

The following outlines the requirements based on these compliance documents, as well as PRIV's reviews and findings.

Collection of Information

Requirement: OPS/NOC is permitted to collect PII on the following categories of individuals when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners: 1) U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances; 2) senior U.S. and foreign government officials who make public statements or provide public updates; 3) U.S. and foreign government spokespersons who make public statements or provide public updates; 4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; 5) names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed; 6) current and former public officials who are victims of incidents or activities related to Homeland Security; and 7) terrorists, drug cartel leaders, or other persons known to have been involved in major crimes of Homeland Security interest. PII inadvertently or incidentally collected outside the scope of these discrete set of categories of individuals shall be redacted immediately before further use and sharing.

Review: During a PCR preparatory self-inspection, MMC discovered that, between December 1, 2010 and August 22, 2011, twelve email reports (IOIs) inadvertently

⁷ The SNMC analyst watch is composed of two watch analysts, one assigned to monitor social networking and the other to monitor media activity.

⁸ The Automated Syslog Audit System is a tool that was developed by OPS/NOC to apply industry standard blacklists and analysis of SNMC analyst entries under established SOP processes.



included unnecessary PII or potential PII. Redaction notices for these IOIs were sent to the recipients and all PII was deleted from the MMC Analyst computers and application database. Also during the PCR preparatory self-inspection, MMC found no incidental receipts of PII. PRIV reviewed hard copies of twelve IOIs and five redaction notices. Additionally, the Director and Associate Director of Privacy Compliance conduct spot checks on a routine basis and have found no issues. Based on the preparation for the review and the finding of IOIs that needed redaction, MMC changed the SOP so that MMC supervisors will conduct more timely reviews and analysis.

Finding: The new SOP will help ensure timely identification of issues, investigations (e.g. employee monitoring and interviews), and any need for additional training. Accordingly, PRIV finds that OPS/NOC meets privacy standards with respect to the redaction of PII outside the scope of the discrete set of categories of individuals.

Use of Information

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

Review: PRIV reviewed Appendix A of the PIA update (Social Media Web Sites Monitored by the NOC) and found that the websites listed were all publicly available and that all use of data published via social media sites was solely to provide more accurate situational awareness, a more complete common operating picture, and more timely information for decision makers in compliance with their statutory mandate.

Finding: PRIV finds that OPS/NOC use of SNMC data is consistent with the stated purpose for the collection.

Retention of Information

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

Review: The OPS MMC capability has not been operating for five years and the retention schedule limitation of no more than five years on the discrete set of categories of individuals listed above has not had any effect.

Finding: PRIV will monitor that this retention schedule is followed and that only information on the discrete set of categories of individuals listed above is retained for the allotted time.

Internal and External Sharing and Disclosure

Requirement: OPS/NOC will share Media Monitoring Reports (MMRs) with Departmental and component leadership, private sector, and international partners where necessary, appropriate, and authorized by law to ensure that critical disaster-related information reaches government decision makers.



Review: OPS/NOC continues to email MMRs to federal employees, contractors, and private sector and international partners who have requested and been approved to receive notifications based on job description and a need-to-know the information, and as such, are on the distribution list maintained and controlled by the Director of the NOC. Additionally, MMC will notify OPS and PRIV when it has determined that there has been egregious usage identified during an audit and make available self-audit compliance reports upon request.

Finding: PRIV finds that the sharing of information and reports generated is sufficiently limited to those who have a need-to-know and that privacy risks are minimal in that data is gleaned only from publicly accessible websites upon which users have voluntarily posted information.

Technical Access and Security

Requirement: OPS/NOC must maintain a log of social media monitoring Internet-based platforms and information technology infrastructure that SNMC analysts visit under this initiative. Additionally, OPS/NOC will implement auditing at the router level for all outbound http(s) traffic and generate audit reports, which will be available for each compliance review and upon request.

Review: OPS/NOC maintains a log of social media monitoring Internet-based platforms and information technology infrastructure that SNMC analysts visit under this initiative. The MMC capability to conduct syslog message collection at the router level has been in operations since March 2011, for which the requirements and processes were finalized in May 2011 and are documented in the SOP for MMC Self-Audit Compliance. Since then, monthly self-audit compliance inspections and reports have been completed. PRIV observed a live demonstration of the Automated Syslog Audit System and reviewed hard copies of MMC self-audit compliance reports generated from May through July 2011.

Finding: PRIV finds that the automated logs are in compliance with the stated PRIV recommendations. PRIV finds that auditing at the router level for outbound http(s) traffic and generating audit reports were adequately implemented. Additionally, the MMC application server resides on a secure, firewalled, isolated private network that does not allow inbound access or connection.

Privacy Training

Requirement: SNMC analysts are required to take annual privacy training and specific PII training.

Review: PRIV reviewed OPS/NOC's PIA/PII Training Package for 2011, which includes an overview of PII and the PIA update.

Finding: PRIV finds that certification exams demonstrate individual learning and a training log records guidance issued on various topics.



IV. CONCLUSION AND RECOMMENDATIONS

PRIV finds OPS/NOC to be in compliance with the January 6, 2011 PIA update and February 1, 2011 SORN under review by this PCR. OPS/NOC should continue to train its analysts and follow the detailed handbook provided to all analysts, as well as integrate on an as-needed basis any OPS, Privacy, and OGC recommendations into the SOP.

PRIV will conduct the fourth PCR of the Initiative and of OPS social media monitoring Internet-based platforms and information technology infrastructure in February 2012.

V. PRIVACY COMPLIANCE REVIEW APPROVAL

Responsible Official

Donald Triner
Director, Operations Coordination Division
Office of Operations Coordination and Planning

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security