



Homeland
Security

Privacy Office

Protecting privacy while promoting transparency



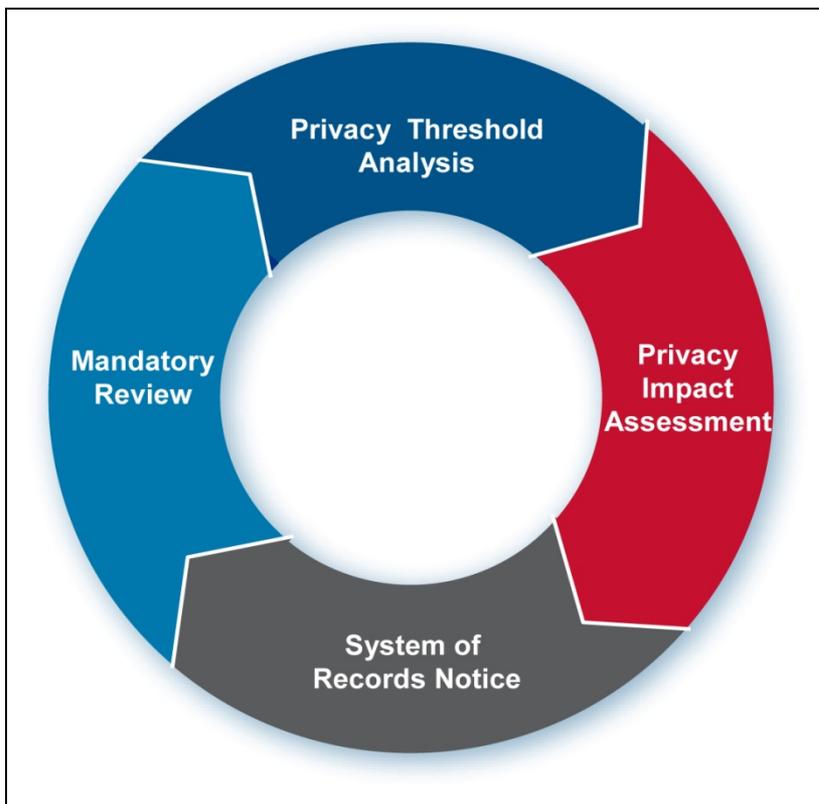
Social Media Monitoring & Privacy Compliance Reviews

Jamie Danker, Associate Director for Privacy Compliance,
DHS Privacy Office

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



Privacy Compliance Lifecycle



Privacy Compliance Artifacts

- Privacy Threshold Analysis (PTA)
- Privacy Impact Assessment (PIA)
- System of Records Notice (SORN)
- Privacy Compliance Review (PCR)



Initial interaction with Privacy Office

- **Series of pilots in 2010**
 - DHS/OPS/PIA-004 Haiti Social Media Disaster Monitoring Initiative January 21, 2010
 - DHS/OPS/PIA-004(a) 2010 Winter Olympics Social Media Event Monitoring Initiative February 10, 2010
 - DHS/OPS/PIA-004(b) April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative April 29, 2010



FIPPs based analysis of the program

- Transparency: Publication of Pilot PIAs
- Data Minimization: Very limited PII collected
- Use Limitation: Only situational awareness/establish common operating picture
- Data Quality/Integrity: Redacting any PII outside of discreet categories; retention period
- Auditing/Accountability: PCR process



January 2011 PIA Update & Feb. 2011 SORN Publication

- Permits limited PII on 7 narrow categories of individuals when doing so lends credibility to the report or facilitates coordination with interagency or international partners.
- PII may include: full name, affiliation, position or title, and publicly-available user ID.

DHS National Operations Center Media Monitoring Capability (MMC)



NOC Media Monitoring and Privacy
Mission Effectiveness and Privacy Compliance
Can Thrive Together

DHS National Operations Center



Mission: To serve as the primary National-level hub for domestic situational awareness, a common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management.

Engage with Privacy Office early

- ❑ Protect Privacy and avoid misperceptions
- ❑ Start off on the right foot
- ❑ Facilitate compliance engagement
 - Specify mission requirements (full disclosure)
 - Tell Privacy what's required... ask how best to do it



Privacy Impact Assessment
for the
Office of Operations Coordination
and Planning

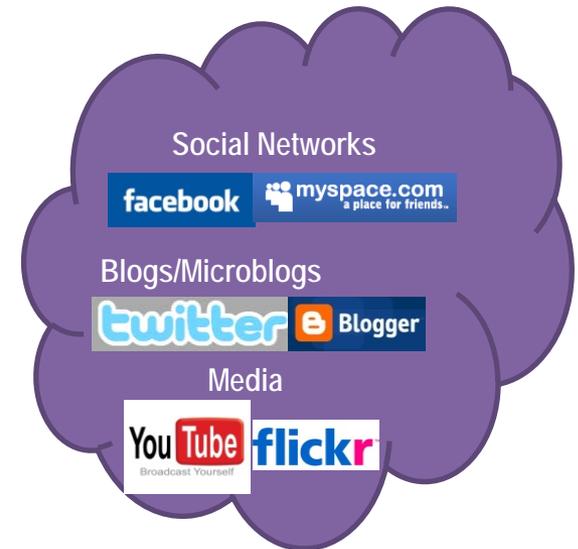
Publicly Available Social Media
Monitoring and Situational
Awareness Initiative Update

January 6, 2011

Cooperation – mutually acceptable solutions

NOC MMC Overview

- ❑ Enhances situational awareness
 - International, national, and local traditional news sites, broadcasts, and online print media
 - Social networking/media sites
- ❑ Search tools & data all publicly available
- ❑ NOC approved distribution list - DHS HQ, DHS Components, Interagency, SLTT
- ❑ Produces 40 - 65 reports plus daily OPSUM



NOC MMC Limits...

MMC IS NOT:

- an intelligence desk
- a law enforcement (LE) desk

PIA and SORN address limitations on collecting, reporting, and storing PII

Does **NOT** report or store PII*

*Limited exceptions: - *In extremis* situations, MMC will report names/positions of officials, spokespersons, reporters, officials as victims, dead “bad guys”

Public Redress:

- No internal procedures for correcting information
- Redress occurs through the public media site
(source: *MMC PIA*)



Training & Compliance

- Training is paramount
- Classroom, self study, and job aids



**Privacy Compliance Review
of the**

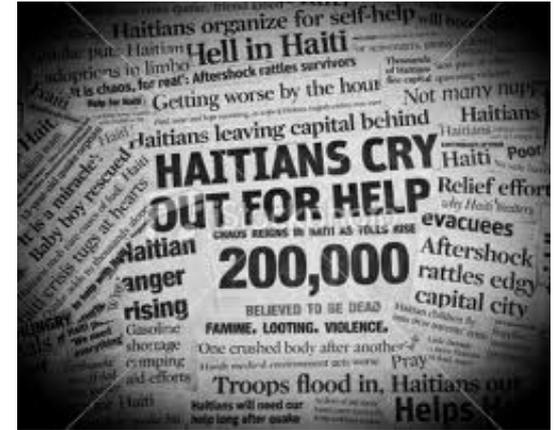
**NOC Publicly Available Social
Media Monitoring and
Situational Awareness Initiative**

May 3, 2012

- Identify inadvertent release
- Compliance reviews
- 17 of 21,000 reports contained PII

Data Accuracy and Quality

- ❑ **Accuracy:** limited to what is posted
 - News and citizen input
 - Social media tends to self correct as events unfold



- ❑ **Corroboration:** tiered system for media sources
 - Higher confidence in major news organizations
 - Social media requires corroboration

- ❑ **Quality:** robust QC program
 - 100% reviewed weekly
 - Timely feedback from readers

Enhance situational awareness for incidents & crises

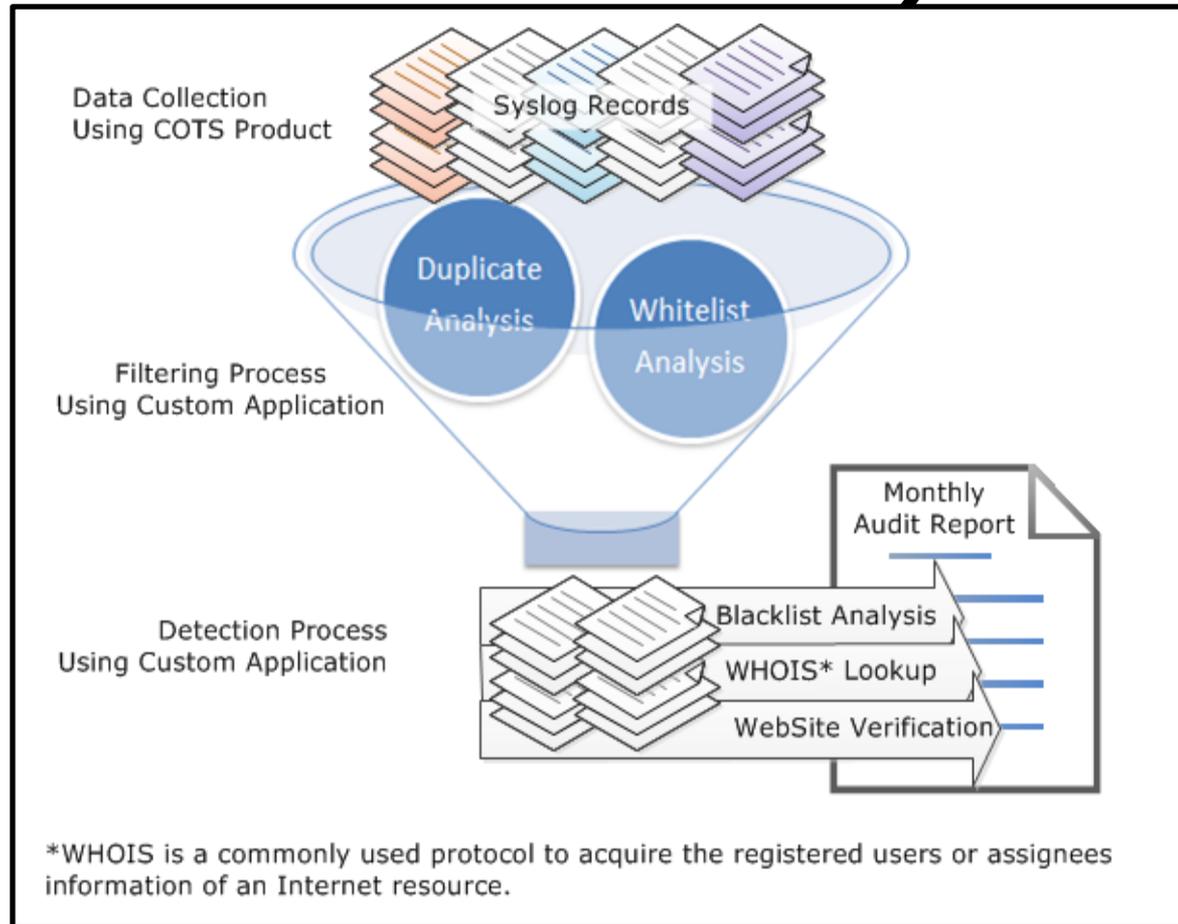
Auditing MMC Internet Activity

MMC Internet Access

- ❑ Unfettered access restricted to mission activities
- ❑ Small intra-network for monitoring use of Internet

Audit

- ❑ System monitoring:
 - 50,000 messages/hr
 - Advanced filters for select monitoring
- ❑ Scheduled and unannounced



Real-time Logging/Monitoring/Advanced Message Filtering



NOC Publicly Available Media Monitoring and Situational Awareness Initiative PCRs

- Early 2010 Initiative began as a series of Pilots
- PCR conducted on pilots (positive assessment)
- June 2010 PIA published (expanded scope no PII collection permitted)
- Second PCR conducted (positive assessment)
- February 2011 PIA Update and January 2011 SORN Publication (to enable limited PII collection on 7 narrow categories of individuals)
- Bi-annual PCRs conducted (most recent March 2012)





What are Privacy Compliance Reviews?

- Consistent with the Privacy Office's unique position as both an advisor and an oversight body for the Department's privacy sensitive programs and systems, the Privacy Compliance Review (PCR) is designed to improve a program's ability to comply with assurances made in PIAs, SORNs and/or other formal information sharing agreements.
- PCRs are a *constructive* mechanism to assess implementation of protections described in documentation, to identify areas for improvement, and to correct course if necessary.



What are the outcomes and benefits of a PCR?

- Recommendations to the program resulting in improvements
- Updates to privacy documentation
- Informal discussions about lessons learned
- Formal report either internal or publicly available
- Heightened awareness by all participants about privacy
- Early issue identification and remediation



What are the basic steps of a PCR?

- Step 1: Collect and Review Available Background Information
- Step 2: Formulate Review Objectives
- Step 3: Notify Program of Review (*buy-in from program and leadership is critical!*)
- Step 4: Formulate Review Questions and Document Requests

****Reminder that the PCR is a constructive process (“gotcha” is not the intent of the review – always maintain open communication with the program under review).****



PCR Steps *continued*

- Step 5: Conduct Interviews and Obtain Supporting Documents
- Step 6: Analyze Documentation and Interviews and Document Preliminary Conclusions
- Step 7: Review and Confirm Findings
- Step 8: Prepare and Issue Product (may be public report or internal recommendations)



March 2012 Bi-Annual PCR 2012

Objectives

- 1) assess compliance with the January 2011 PIA Update and February 2011 SORN; and
- 2) review and update, as appropriate, the 2011 Guidance and Standard Operating Procedures (SOPs) to ensure they accurately reflect the scope of the initiative.



March 2012 Summary of PCR Findings

Overall - DHS Privacy found OPS/NOC in compliance with the January 2011 PIA Update and the February 2011 SORN.

- *Collection of Information* – NOC not actively seeking PII in its reporting. 20 percent of reports contained PII within 7 permitted categories
- *Use of Information* – established reporting categories of events consistent with their statutory mandate.



March 2012 PCR Findings *continued*

- *Retention of Information* - maintains a database of Reports distributed consistent with 5-year retention.
- *Internal and External Sharing and Disclosure* - a process is in place to determine the need-to-know for Report distribution.
- *Technical Access and Security* – conducted 14 random audits.
- *Privacy Training* - All MMC Analysts successfully passed an annual PII Certification exam.



PCR Recommendations

- Identified three recommendations to improve the Initiative's ability to demonstrate compliance with privacy requirements
 1. Updates to guidance and SOPs to more accurately reflect the scope and purpose of the Initiative (*implemented*)
 2. Incorporation of guidance into SOPs about use of a social media account profile (*implemented*)
 3. Development and implementation of a logging mechanism for searches conducted in the database that maintains MMC Reports (*in progress*)



Questions

- Next PCR scheduled to commence in September 2012
- The March 2012 PCR Report on the Initiative as well as other PCR Reports including other DHS Programs can be found at www.dhs.gov/privacy under “Investigations and Compliance Reviews”
- Questions about PCRs at DHS or building a similar process at your agency? Contact Jamie Danker (Jamie.Danker@hq.dhs.gov)