Data Privacy & Integrity Advisory Committee

Public Meeting

Monday, December 5, 2016

9:00 AM - 12:30 PM

Homeland Security | Privacy Office

Web Conference Instructions

Please follow these instructions:

CONFERENCE LINE

- Dial 1-877-461-0584 and enter passcode 1697821.
- Please mute your phone but don't place it on hold.

QUESTIONS

- Hold questions until the end of each session when the operator will open the line. DPIAC members have priority.

HANDOUTS

- This presentation is also available on our website: www.dhs.gov/privacy. Click on *Privacy Events*.

Remarks

Paul M. Rosen
Chief of Staff

Department of Homeland Security

Privacy Office Update

Jonathan Cantor

Chief Privacy Officer (Acting)

Biometric Framework Update

Laurence (Larry) Castelli
Senior Advisor to the Chief Privacy Officer
DHS Privacy Office
Telephone: (202) 343-1717
E-mail: Laurence.Castelli@hq.dhs.gov

Biometric Framework Update

Objective: Apply Unity of Effort Vision

- Support creation of a DHS enterprise approach to biometrics maintenance, retention, and sharing
- Continue to allow for sharing of Component-collected data consistent with the purpose for which it was collected
- Provide transparency to interagency shared missions by creating a System of Records that expressly allows for storage of biometrics collected from external entities
- Establish a stakeholder governance process for internal and external use of DHS biometric holdings

Biometric Framework Update

Current IDENT/HART SORN Framework, Challenge

- **Broad, DHS-wide purpose**
  "Enable DHS to carry out its DHS national security, law enforcement, immigration, intelligence, and other mission-related functions, and to provide associated testing, training, management reporting, planning and analysis, and other administrative uses, by allowing DHS to positively identify an individual whether the name information is the same or different based on biometrics."

- **Biometric Services Provider *and* System of Record for all DHS Biometrics**
- Leads to a confusing interpretation of the Privacy Act, since the most biometrics collected by IDENT were collected pursuant to component source system SORNs.
- Therefore, should be *shared* with IDENT (SORN) under (b)(1) intra-agency sharing.

Biometric Framework Update

Enterprise Framework, Opportunity -Align with Current Policy

- A privacy legal framework that supports the goals and objectives of the IBSV to advance an integrated biometrics strategy across all Components

- Facilitate the vision of the ISSGB's approved International Information Sharing Architecture: "a unified DHS approach to improve bi-directional data exchange capabilities between the US and our international partners, while protecting privacy and preserving civil rights and civil liberties."

- Maintain IDENT/HART as a shared service under Privacy Policy Guidance Memorandum 2011-02 (now, Policy Directive 262-09 Roles and Responsibilities for Shared IT Services) and as the biometric repository, consistent with the May 2007 Identity Management and Screening Memo

Biometric Framework Update

Reinforce Compliance Structure

Closely align IDENT/HART with a proper Privacy Act Analysis:

- Biometrics are collected by the Components, pursuant to their statutorily authorized missions (which vary by Component).
- Collection of information by Component aligns with the Privacy Act requirements for data minimization and is relevant and necessary to the Component authorized purpose.
- Components send the biometrics to IDENT (the IT system) as the Biometric Repository and Service Provider.

Biometric Framework Update

New Biometric SORN Framework, Purpose:

- Biometrics are shared from Component SORNs under the intra-agency condition for disclosure provision (b)(1), into IDENT/HART (the IT system) for the several purposes stated in those Component SORNs:

- Screening to allow multiple factors to inform determinations of positive identity at the border, upon entry to controlled facilities, or apprehension

- Vetting to enhance and ensure positive identity determination to support inclusion in privileged groups (Trusted Traveler, Trusted Worker, FEMA Volunteers, etc.)

- Benefits Distribution

DHS receives information from external sources in support of its border security and other missions, and shares that information, which resides in IDENT/HART (the IT system), within DHS under (b)(1).

Biometric Framework Update

IDENT SORN Proposed Future State

One IT System –IDENT/HART will maintain biometric data **consistent with the original, source Component purpose for collection/ingestion**

A Tiered SORN Framework with Two New DHS-wide SORNs:

- The Foundation Tier for the Biometric SORN Framework – this identifies the several DHS Component SORNs that cover the direct collection of biometrics

- The Transaction Tier for the Framework – this identifies a new DHS-Wide SORN that covers how IDENT/HART assigns FINs and EINs, manages the associations of subsequent record matches, and generates Reporting covered by the current TRAC SORN (DHS/NPPD-003)

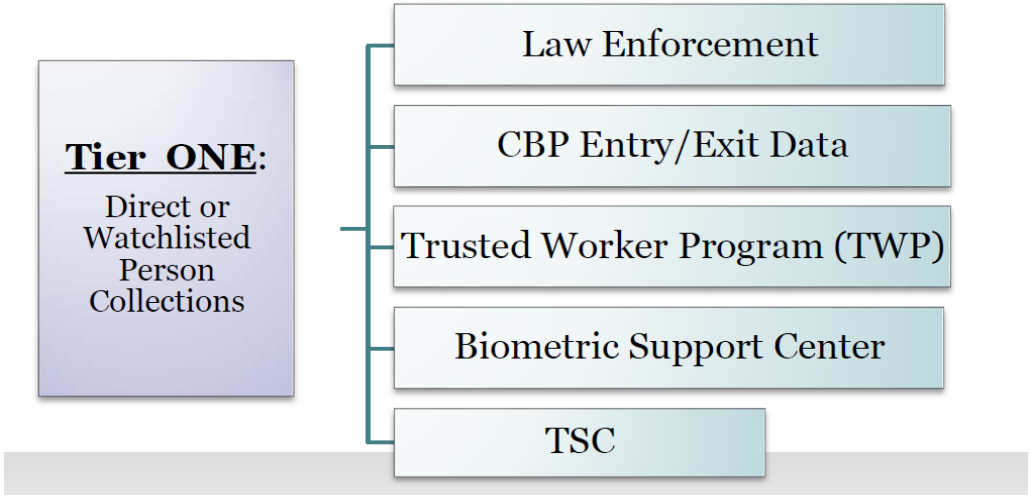
- The Third Tier for the Framework – this identifies a new DHS-Wide SORN, DHS/ALL-xxx, External Biometric Records SORN, for those ingested biometrics provided by foreign or domestic partners, under whose authority collection occurred, and that support the DHS Border Security or other related Missions of DHS

Biometric Framework Update

Tier 1: DHS Component Biometric Collections

- The several DHS Component SORNs covering biometrics collected from U.S. citizens and non-U.S. citizens by DHS Components for the various missions of DHS and its components

- Specific SORN covering the DHS ingest of the TSDB Watchlisting Biometrics

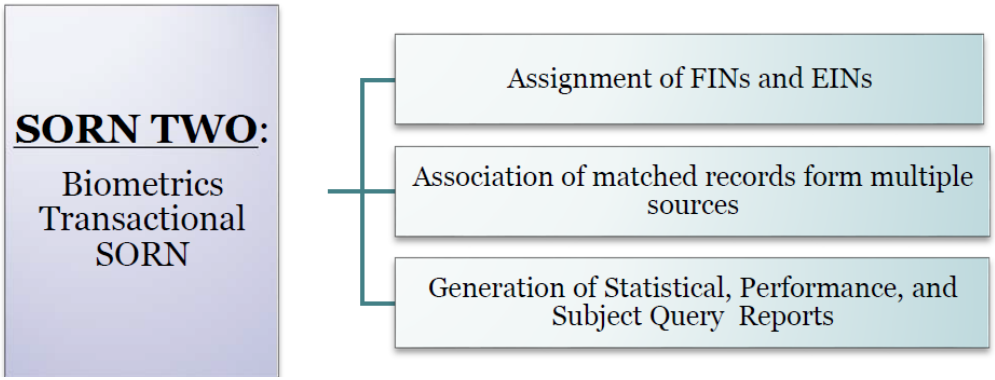


Biometric Framework Update

Tier 2: DHS-wide Biometrics Transactional SORN

Tailored to provide coverage for internal administrative, "housekeeping," reporting, and transactional functions performed by IDENT/HART to maintain the DHS biometric repository

- New SORN will state a purpose directed at serving as an information management tool to assist DHS/OBIM in maintaining its enterprise biometric repository and contain Routine Uses restricted by the scope of its purpose
- These Uses are proposed to be consistent with its internal to DHS purpose

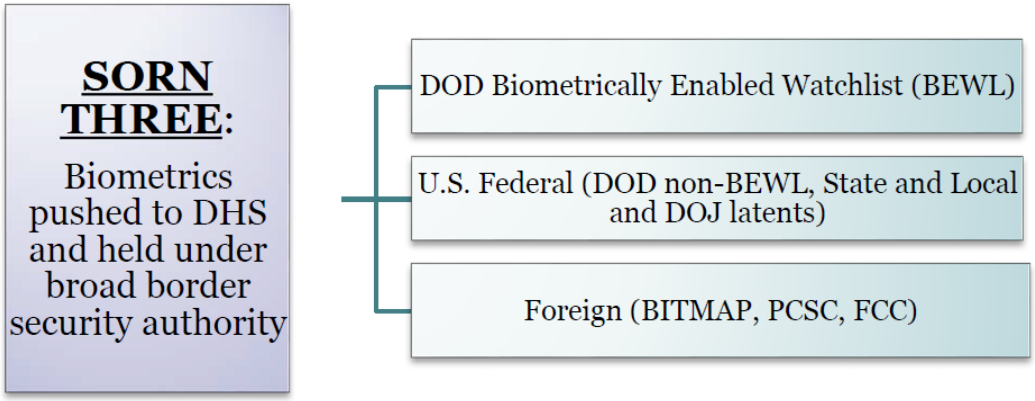


Biometric Framework Update

Tier 3: DHS-wide SORN, External Biometrics

Biometrics stored in IDENT/HART, but not collected by DHS

- External Biometric Records SORN (EBR) will contain biometrics obtained from non-DHS partners –including other federal agencies, state/local governments, and foreign partners where the full provenance or attribution of the prints is unknown to DHS or restricted by specific agreement.



Biometric Framework Update

Sharing Information from External Tier 3

Internal sharing

- Sharing biometrics covered under EBR within DHS is permissible under 5 U.S.C. §552a(b)(1) ("need to know" within agency)
- "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."

- Biometrics covered by Tier 1 SORNs can be vetted against EBR
- *In the event of a match against a Tier 1 SORN, the biometrics and encounter context from EBR become associated with the biographic record for the respective Tier 1 SORN*

External sharing

- Biometrics that have a *match against a Tier 1 SORN* would be shared external to DHS, as part of those records.
- EBR SORN **will have tailored Routine Uses: redress, IC, DOJ for litigation, law enforcement defined by agreement or sharing arrangement**

Biometric Framework Update

Sharing Information from EBR

- **Step 1**

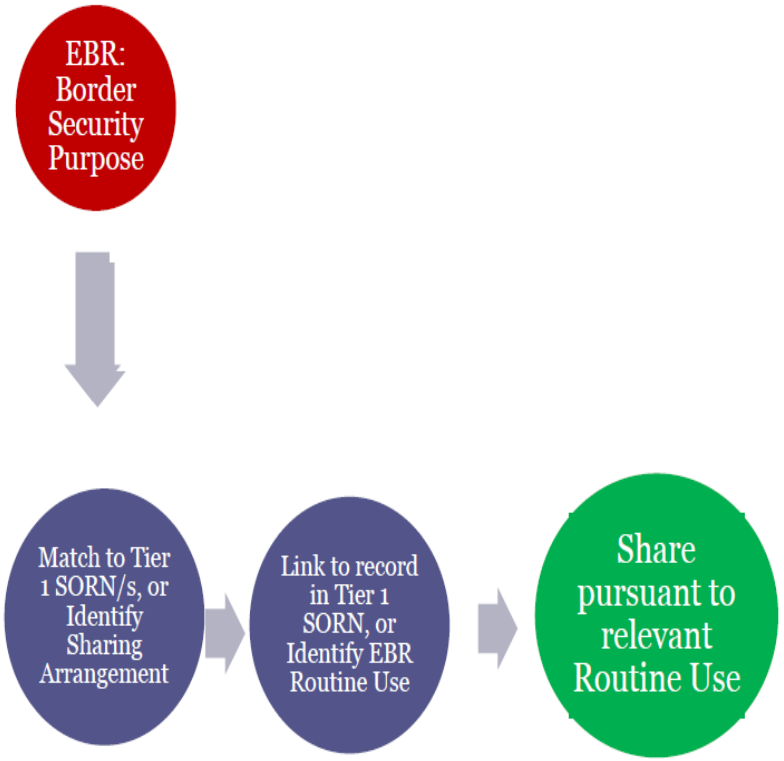
Is there a match within EBS to information covered by a Tier 1 SORN?

- **Step 2**

If yes, then the record from EBS is associated with the respective Tier 1 SORN/s.

- **Step 3**

Newly associated records may be shared consistent with the appropriate Tier 1 SORN/s routine uses for external sharing.



Biometric Framework Update

Information Sharing Use and Policy Governance

Governance (Proposal for Consideration)

- DHS will establish or identify an IDENT/HART Governance Board to guide OBIM on Information Sharing Policy and coordinate Data Steward (Stakeholder) concurrence regarding access and use, including future SORN coverage for any new data sets added to IDENT/HART repository.
- All Data Stewards, OBIM (as service provider), DHS/Policy, DHS/I&A, DHS/CRCL, and DHS/PRIV will be represented on the "Governance Board."
- DHS Policy will serve as a permanent Co-Chair of this IDENT Governance Board.
- Each DHS operational component with one or more Data Stewards will rotate on a yearly basis through the position of operational Co-Chair of the IDENT Governance Board.

Privacy Compliance Review Update

Shannon Ballard
Director, Privacy Oversight
DHS Privacy Office
Phone: 202-343-1717
E-mail: Shannon.Ballard@hq.dhs.gov

Privacy Compliance Review Update

The DHS Privacy Compliance Review (PCR) Process

- The DHS Privacy Office's mission is to protect individuals by embedding and enforcing privacy protections and transparency in all DHS activities
- One way to assure that technologies sustain and do not erode privacy protections is through PCRs
  - DHS Chief Privacy Officer authorities under *Section 222 of the Homeland Security Act*
- PCRs are a **collaborative effort** to help improve a program's ability to comply with privacy compliance documentation

Privacy Compliance Review Update

Privacy Compliance Reviews at DHS: Constructive

PCRs are a constructive mechanism to:

- Assess implementation of protections described in privacy compliance documentation
- Ensure that a program is operating consistent with privacy law and policy
- Identify areas for improvement
- Correct course if necessary

Privacy Compliance Review Update

Privacy Compliance Review at DHS: Collaborative

- PCRS are collaborative rather than adversarial
- Independent internal review leads to:
  - improved accountability
  - increased ethical and professional practices
  - effective risk management
  - Improved quality of output

Privacy Compliance Review Update

PCR Benefits

Constructive. Collaborative. Transparent.

- Assure that technologies sustain and do not erode privacy protections
- Corroborate assurances made in PIA, SORN and/or Agreement
- Identify areas for improvement and correct course if necessary
- Your privacy documents are promises that you need to demonstrate your program is living up to!
- Improve program & increase transparency

Privacy Compliance Review Update

How do you determine which programs get a PCR?

- Planned as part of the development of a new program or system for those that present unique privacy concerns
- Controversial issues that may heighten public scrutiny
- Fallout from an incident or breach

✓ Consider staffing resources

Privacy Compliance Review Update

Collaboration in Action

- Step 1: Collect & Review Available Background Info
- Step 2: Formulate Review Objectives
- Step 3: Notify Program of Review
- Step 4: Formulate Review Questions & Document Requests

Privacy Compliance Review Update

Collaboration in Action (cont.)

- Step 5: Conduct Interviews & Obtain Supporting Docs
- Step 6: Analyze Documentation & Interviews and Draft Preliminary Findings
- Step 7: Review and Confirm Findings
- Step 8: Prepare and Issue Product

Privacy Compliance Review Update

Potential Outcomes and Benefits

- Recommendations to the program result in improvements
- Privacy documentation updates
- Lessons learned
- Heightened awareness by all participants about privacy
- Early issue identification and remediation
  - ✓ Accountability and sustainability

Privacy Compliance Review Update

DHS PCRs Online

Privacy
- Compliance
- Cybersecurity
- Events
- FOIA
- **Reviews & Investigations**
- Policy
- Reports
- Other Correspondence Logs
- Proactive Disclosure of Information

Privacy Reviews & Investigations

Privacy Compliance Reviews

The DHS Privacy Office serves as both an advisor and oversight body for the Department's privacy-sensitive programs and systems. The Privacy Compliance Review (PCR) was designed as a collaborative effort to help improve a program's ability to comply with existing privacy compliance documentation, including Privacy Impact Assessments (PIA), System of Records Notices (SORN) and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements. A PCR may result in a public report or internal recommendations, depending upon the sensitivity of the program under review.

Listed in alphabetical order:

- Analytical Framework for Intelligence
- DHS Use of Social Media for Communications and Outreach
- EINSTEIN
  - Privacy Compliance Review Follow-Up Letter for the EINSTEIN Program
- Enhanced Cybersecurity Services (ECS) Program
- ICE Pattern Analysis and Information Collection Law Enforcement Information Sharing Service
- Media Monitoring Initiative
- Office of the Chief Human Capital Officer
- Passenger Name Records Reviews
  - also see DHS/CBP/PIA-006
  - Passenger Name Records Agreements
  - Answers to Frequently Asked Questions
  - Privacy Policy for Passenger Name Records

https://www.dhs.gov/investigations-reviews

BREAK: 11:00 – 11:15 am

DHS Social Media Update

David Linder

Senior Privacy Analyst
DHS Privacy Office

Phone: (202) 343-1717

E-mail: David.Lindner@hq.dhs.gov

DHS Social Media Update

- DHS uses social media for four purposes:
- Public Affairs –push out information; no PII collected
- Situational awareness –passive observation; minimal PII collected
- Operational Use –varies based on authorities
- Intelligence –Executive O 12333

- Majority of DHS social media collections are for **operational use**
- Authorities to collect do not change based on the media/platform/method of collection

DHS Social Media Update

Examples of Operational Uses

- Multiple components, programs and HQ elements leverage social media for operational use:
- Screening/Vetting: an agency or office screens individuals in advance of an action (border crossing, flight, etc.) against social media to determine a risk score/threshold of their post or to augment the benefit adjudication process (CBP, TSA, USCG, USCIS)
- Investigations: an agency or office leverages social media during an investigation on a case by case basis (CBP, USCG, ICE)
- Personnel Security: an agency or office monitors it's workforce for professional responsibility, insider threat or security violations (TSA, OCSO, USCG, CBP, USSS, ICE, CIS, NPPD)

DHS Social Media Update

Legal Authorities

- No explicitly worded authorities regarding social media.
- Use of social media by components is natural follow-on to components authorities to carry out specific missions.
- Authorized Purpose: Specific use of social media has to be tied to the component's mission and its authority to carry out that mission.
- Statutes such as the E-Government Act of 2002 and Privacy Act of 1974 create privacy protection for individuals whose information is being used and stored by the government.

DHS Social Media Update

DHS Privacy Policy Framework

DHS Management Directive 110-01-001, "Privacy Policy for Operational Use of Social Media" provides DHS-wide guidance regarding…operational use of social media (2012). Certain SM uses are exempt:

- Comms/outreach
- Situational awareness
- Intelligence activities in accordance with Executive Order 12333

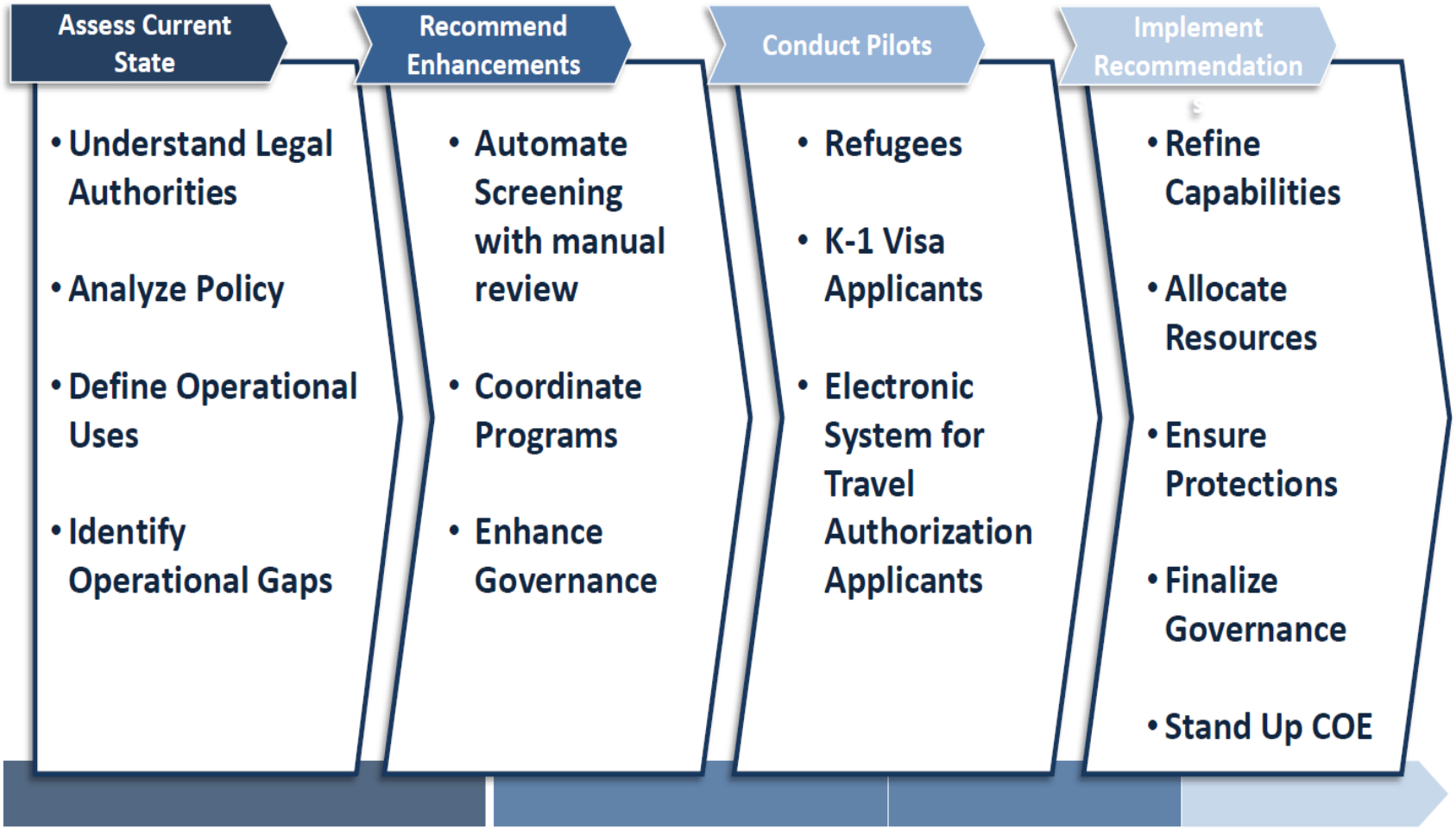
- Oversight process for using social media is centralized to ensure adherence to privacy and legal authorities but federated across components.

- To date, over 30 social media usage policies are active, spanning all components and many HQ elements with operational missions.

DHS Social Media Update

DHS Social Media Task Force

DHS established a social media task force composed of members from operational components and oversight to evaluate our social media posture.



DHS Social Media Update

Technical Challenges

- DHS is working to develop a suite of tools and capabilities to enable an automated process with a manual review for screening and vetting publically available social media information in bulk and at a scale.

- This is a novel, complex, and fluid challenge to address as a Department.

- We believe a number of capabilities currently on the market and within the USG could be adapted to meet the DHS use case but we will need to commit resources to test and shape currently available technical capabilities to our mission needs.

DHS Social Media Update

Potential Privacy Risks

- Over-collection of Information
- Use Limitation
- External sharing
- Notice
- Retention

Data Breach Tasking Update

Joanne McNabb
Chair, Policy Subcommittee
Data Privacy and Integrity Advisory Committee


QUESTIONS?
COMMENTS?
CONCERNS?