Data Privacy & Integrity Advisory Committee

Public Meeting at the DHS Privacy Office

650 Massachusetts Ave, NW, Washington, DC

Thursday, September 12, 2013

2:00 - 5:30 PM

Homeland Security | Privacy Office

Web Conference Instructions

Please follow these instructions:

- **CONFERENCE LINE**: Dial 888-790-3560; enter passcode 1665201.
- **PHONE**: Mute your phone but don't place it on hold or we will hear music! Operator will also mute the line while the presenters are speaking.
- **QUESTIONS**: Hold questions until the end of each session when the operator will open the line. DPIAC members have priority.
- **HANDOUTS**: The presentations and handouts are available on our website: www.dhs.gov/privacy. Click on *Events*, then *DPIAC Meeting Information*.

DHS Privacy Office Update

Jonathan R. Cantor, Acting Chief Privacy Officer

- ANNUAL REPORT
- STAFFING
- TRAINING
- PCLOB

DHS Privacy Office Update

Jonathan R. Cantor, Acting Chief Privacy Officer

POLICY AND ADVOCACY

- **INTERNATIONAL**
- CANADA
- EUROPEAN UNION
- FIVE COUNTRY CONFERENCE
- INTERAGENCY COORDINATION ON INTERNATIONAL PRIVACY POLICY
- OUTREACH

DHS Privacy Office Update

Jonathan R. Cantor, Acting Chief Privacy Officer

COMPLIANCE

- PIAs and SORNs
- UNMANNED AIRCRAFT SYSTEMS
  - PRIVACY WORK STREAMS

DHS Privacy Office Update

Jonathan R. Cantor, Acting Chief Privacy Officer

FOIA

- REPORTING
- POLICY GUIDANCE
- ENGAGING THE PUBLIC

DHS Privacy Office Update

Jonathan R. Cantor, Acting Chief Privacy Officer

PRIVACY OVERSIGHT

- PRIVACY COMPLIANCE REVIEWS (PCR)
- INVESTIGATIONS
- PRIVACY INCIDENT HANDLING

Unmanned Aircraft Systems—Privacy & Departmental Use

1. *Christopher S. Lee*, Privacy Officer, Science & Technology Directorate, DHS
2. *Laurence Castelli*, Privacy Officer, U.S. Customs and Border Protection, DHS
3. *J. Scott Mathews*, Senior Advisor for Privacy & Intelligence, Privacy Office, DHS

Homeland Security | Privacy Office

Unmanned Aerial Vehicles (UAVs)

Unmanned Aircraft Systems (UAS)

UAV versus RC Airplane

UAV

- Commercial
- Government
- Private Company
- Requires FAA Certificate of Authorization (COA)

Remote Control Airplane

- Personal Use
- FAA Advisory Circular 91-57

First Published UAS Privacy Impact Assessment

Privacy Impact Assessment
for the

Robotic Aircraft for Public Safety (RAPS) Project

November 16, 2012

DHS/S&T/PIA-026

Contact Point
John Appleby
Borders and Maritime Security Division
Science and Technology Directorate
(202) 254-5620

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Beneficial Uses

- Exigent Circumstances
  - Search & Rescue Operations
  - Firefighting & HAZMAT Response
- Border Surveillance
- Disaster Response/Recovery
- Critical Infrastructure Surveillance
- Crop Dusting
- Land Surveying
- Wildlife Monitoring

FAA Modernization and Reform Act of 2012

H. R. 658

One Hundred Twelfth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Tuesday, the third day of January, two thousand and twelve

An Act

To amend title 49, United States Code, to authorize appropriations for the Federal Aviation Administration for fiscal years 2011 through 2014, to streamline programs, create efficiencies, reduce waste, and improve aviation safety and capacity, to provide stable funding for the national aviation system, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "FAA Modernization and Reform Act of 2012".

S&T's UAS Test Site

Mitigation Strategies

- Fair Information Practice Principles (FIPPs)
  - Data retention and destruction times
  - Purpose Specification
  - Notice
- Oversight
- Community Outreach

CBP Aircraft Systems PIA Overview & Context

- CBP flies three basic types of Aircraft
  - Manned rotary-wing (*e.g.*, helicopters)
  - Manned fixed-wing (*e.g.*, turboprop and jet aircraft)
  - Unmanned Aircraft Systems (UAS) (MQ-9 Predator and Guardian)
- No CBP Aircraft are armed
- CBP deploys variations of three types of information collection technology
  - Electro-Optical/Infrared (EO/IR) Ball mounted cameras
  - Radar, both Synthetic Aperture (for topographical changes) and Wide Area Surveillance Systems (for movement and broader geographic context)
  - Electronic signals intercept (for counter-terrorism and smuggling interdiction)

FIPPs Factors and Analysis 1

- Transparency: CBP achieves transparency through this PIA and on the cbp.gov website under Border Security, Office of Air and Marine
- Individual Participation: consent is not practical nor sought for collections in the Border Area or in support of law enforcement activities, however, case management SORNs do provide redress
- Purpose Specification: CBP has long standing authority to collect information in the Border Area; also, 2011 and 2012 Appropriations Acts have called out mission support for law enforcement, state and local needs
- Data Minimization: CBP relies on mission parameters (patrol or law enforcement support) to define the scope of data collected
  - Unassociated data is retained locally (on manned aircraft or ground control stations) for 30 days, distributed data, through Big Pipe, is retained on that server for 7 days, and data referred to the Office of Intelligence and Investigative Liaison for analysis of historical topographical changes and illegal immigration movement patterns may be retained for no more than 5 years
  - Associated data is retained in accordance with the retention period for the case management SORN where the data is linked to a file

FIPPs Factors and Analysis, 2

- Use Limitation: CBP/OAM controls the dissemination of live imagery and data through Big Pipe, a closed network with restricted access for video and image distribution within the DHS firewall
  - Separate requests for images, data, or analytical product incorporating collects from aircraft are subject to approval through the Assistant Commissioner, OIIL
- Data Quality & Integrity: Unassociated images that are not transferred to OIIL, and maintained for relevance relating to change analysis for a maximum of 5 years, are overwritten within 30 days
  - Associated images used for case support are subject to strict evidentiary chain of custody procedures and retain in conjunction with the retention of the case record in accordance with the case management system

FIPPs Factors and Analysis, 2

- Security: Satellite relays from ground control stations to UAS are encrypted for both command and control signals and imagery and data feeds
  - Video distributed through Big Pipe employs user access controls and password authentication
  - Video retained as evidence is stored on separate hard drives and is subject to physical security, including locked containers
- Accountability & Auditing: CBP requires all employees to receive annual privacy awareness training and to maintain logs and/or disclosure records for all disseminations

Other UAS Privacy Activities I

- In September 2012, DHS formed a Privacy Civil Rights and Civil Liberties UAS Working Group to provide a forum to discuss DHS' use of UAS, and to make recommendations to the Secretary.
- The working group is co-chaired by the DHS Privacy Office, DHS Office for Civil Rights and Civil Liberties, and the CBP Office of Air and Marine.
- Developing a guide for best practices based on the DHS FIPPs that will be publicly available when complete.
- Additional topics the Working Group may address include privacy considerations when DHS funds are used by SLTT to buy UAS, and DHS receipt of support requests from law enforcement agencies.

Other UAS Privacy Activities II

- The Privacy Office has provided support and text regarding UAS privacy issues to the FAA and other agencies over the past year.
- We are heavily engaged in several government-wide committees that are discussing UAS policy issues, including privacy.
- We have participated in 3 congressional briefings on UAS privacy issues so far this year; we have promised to keep Congress abreast of all UAS privacy developments at DHS.

Conclusion

- Questions and Answers.

- Contact emails:
  - DHS Privacy: privacy@dhs.gov
  - CBP Privacy: privacy.cbp@cbp.dhs.gov

Cybersecurity Executive Order – Integrated Task Force, Implementation and Privacy

1. *Jeannette Manfra*, Deputy Director, Enterprise Performance Management, Office of Cybersecurity and Communications, National Protection & Programs Directorate, DHS
2. *Emily Andrew*, Senior Privacy Officer, National Protection & Programs Directorate, DHS
3. *Martha Landesberg*, Senior Director, Oversight, Privacy Office, DHS

Homeland Security | Privacy Office

Enhancing Security & Resilience

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensable to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships

Taking Action

- In February 2013, the President announced two new policies:
  1. Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  2. Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience
- Together, they create an opportunity to work together to effect a comprehensive national approach to security and risk management.
- Implementation efforts will drive action toward ***system* and *network*** security and resiliency.

Integrating Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Integrated Task Force (ITF)

- Establishes and manages working groups to accomplish the major deliverables and action items
- Integrates efforts for delivering EO and PPD requirements
- Develops and manages the governance process
- Engages relevant partners and stakeholders to develop products
  - Request for Information, Federal Register Notices, social media, meetings, presentations, workshops, interviews, etc
- Regularly reports on progress made throughout the EO and PPD implementation to partners and stakeholders

Working Groups

1. Stakeholder Engagement
2. Planning and Evaluation
3. Situational Awareness and Information Exchange
4. Cyber-Dependent Infrastructure Identification
5. Voluntary Program
6. Information Sharing
7. Research and Development
8. Framework Collaboration
9. Assessments: Privacy and Civil Rights & Civil Liberties

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

Opportunities to Engage

- National Infrastructure Protection Plan process
  - Review and comment on Draft Documents
    - www.dhs.gov/eo-ppd
    - Comments on DRAFT 1 due Aug.19
    - Provide input through dialogue on IdeaScale -- http://eoppd.ideascale.com
  - Participate in Working Group meetings
- Cybersecurity Framework
  - Learn more by visiting http://www.nist.gov/itl/cyberframework.cfm
- PPD/EO Integrated Task Force Weekly Stakeholder Bulletin
  - Current status of activities
  - List of upcoming Open Forums, Webinars and other Engagement Opportunities
- *Contact EO-PPDTaskForce@hq.dhs.gov for more information*

NPPD Privacy's Role

- Engage proactively and identify EO and PPD activities at NPPD.
- Ensure the Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks are embedded in new and ongoing programs that support the EO and PPD.
- Report to SAOP on progress.

Assessments Working Group

- EO 13636 Section 5 privacy & civil liberties requirements:
  - Agencies coordinate with senior agency officials for privacy and for civil liberties to ensure privacy and civil liberties protections, based on the FIPPs and other privacy/civil liberties frameworks, are embedded in all EO activities
  - Senior agency officials for privacy and civil liberties assess privacy and civil liberties risks of those activities and recommend steps to minimize or mitigate risks
  - Make agency assessments available in a public annual report (or classified annex, as appropriate) compiled by the DHS Privacy Office and Office for Civil Rights and Civil Liberties (1st issue: February 2014)
- National Security Staff Guidance on Conducting Assessments (June 2013)
  - Assess privacy impacts against the FIPPs and other privacy and civil liberties policies, principles, and frameworks

Break: 3:45 – 4:00

Homeland Security Information Sharing Environment

1. *Tom Bush*, Deputy Assistant Commissioner, Office of Intelligence and Targeting, U.S. Customs and Border Protection, DHS
2. *Donna Roy*, Executive Director, Information Sharing Environment Office, Office of the Chief Information Officer, DHS
3. *Rebecca Richards*, Acting Deputy Chief Privacy Officer and Senior Director of Compliance, Privacy Office, DHS

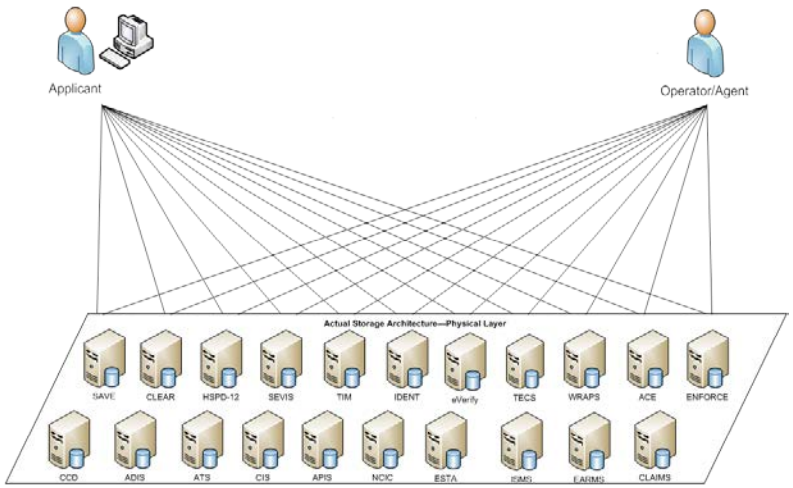
Homeland Security | Privacy Office

Agenda

- Welcome (level setting)
- Mission problems/high level approach
- Current pilot architecture
- DPIAC Report guidance
- Privacy Activities Update

Mission Problem

- Today's mission constraints
  - Stove-piped systems and ***inaccessible data***
  - ***Multiple*** log-ins
  - Different systems ***deliver different search results***
  - Difficult and ***inefficient use and sharing*** of available homeland security information



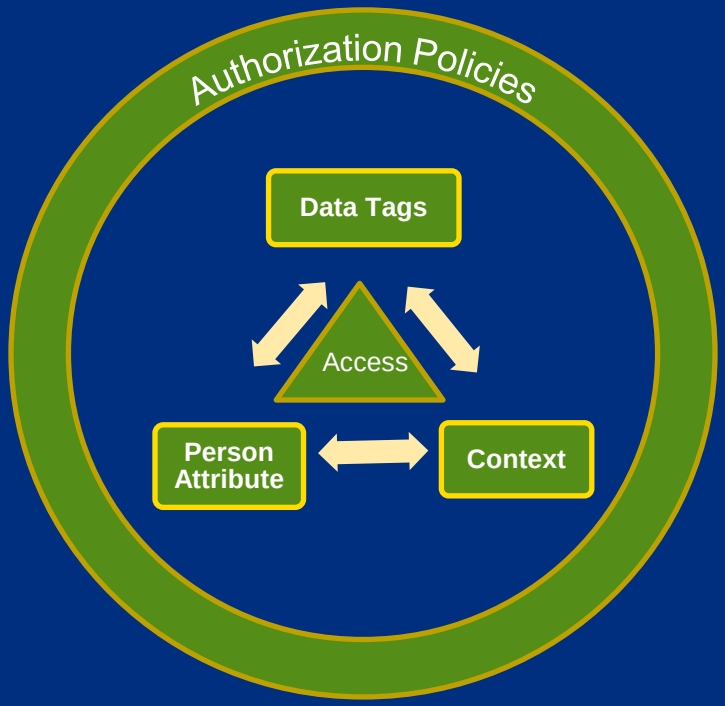
High Level Approach

- Guiding Principles:
  - ***Enable scalable and controlled*** aggregation of DHS datasets
  - ***Design built-in Safeguards*** for access and use of DHS data
  - Proven ***governance*** process
  - ***Drive new analytics*** to enhance efficiencies and mission capabilities

- This initiative will be informed by the current pilots underway demonstrating the ability to control and safeguard DHS information, while supporting our operational need for advanced analytics.

Progress Made to Date Controlling Access and Use

Access Control is the process of controlling the flow of data by making decision requests and authorization decisions based on policies.



Authorization Policies are the rules by which persons are granted or denied access to data or resources based on the alignment of their *personal attributes*, the *context* of their request, and the *type of data* they are requesting.

Person Attributes (User, Requestor) are characteristics of an entity requesting an operation on an object.

Context or Use is the purpose for which the data will be used (e.g. Law Enforcement) and/or the type of search/query conducted (e.g. Person search by name).

A data tag is characterizing metadata (data about data) associated with a data object. A data tag is both the tag name and the value, e.g., system name "ESTA".

Major Pilot Activities

1. ***Neptune Pilot:*** Data will be tagged and ingested in a "big data" platform on the SBU domain. Data in the Neptune Pilot will be shared with the CEI Prototype and the Cerberus Pilot but will ***not*** be accessible for other purposes.

2. ***CEI Prototype:*** The CEI Prototype, residing on the SBU domain, will receive a subset of the tagged data from the Neptune Pilot and correlate data across component data sets.

3. ***Cerberus Pilot:*** The Cerberus Pilot, residing in the TS/SCI domain, will receive all of the tagged data from the Neptune Pilot and test the ability to ensure that only users with certain attributes are able to access data based on defined purposes using the rules engine.

Pilots and Relevance to Access Concepts

Concepts highlighted in green are being explicitly tested by the pilot.

Person Attributes

Person Attributes will be provided by the DHS Attribute Hub under a separate effort.

Data Tagging

- **Purpose**: Allow for data consolidation
- **Approach**: Provide platform and methodology for data tagging
- **Lead:** OCIO/ISEO
- **Pilot 1**: Neptune

Develop
- Policies
- Data Tags

CEI (Person Correlation)

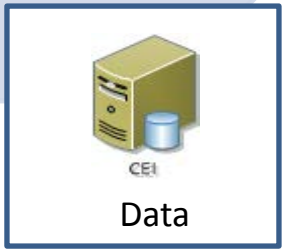
Purpose: Better identify individuals across data sources

Approach: Test correlation and access control to data from multiple sources

Lead: OCIO/ISEO

Pilot 2: Common Entity Index

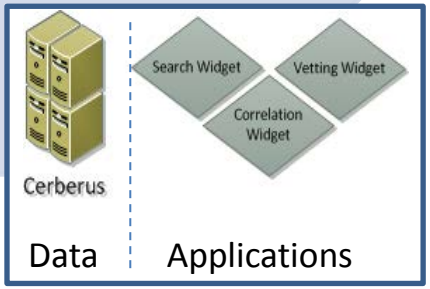
Access w/ Policies Data Tags Context



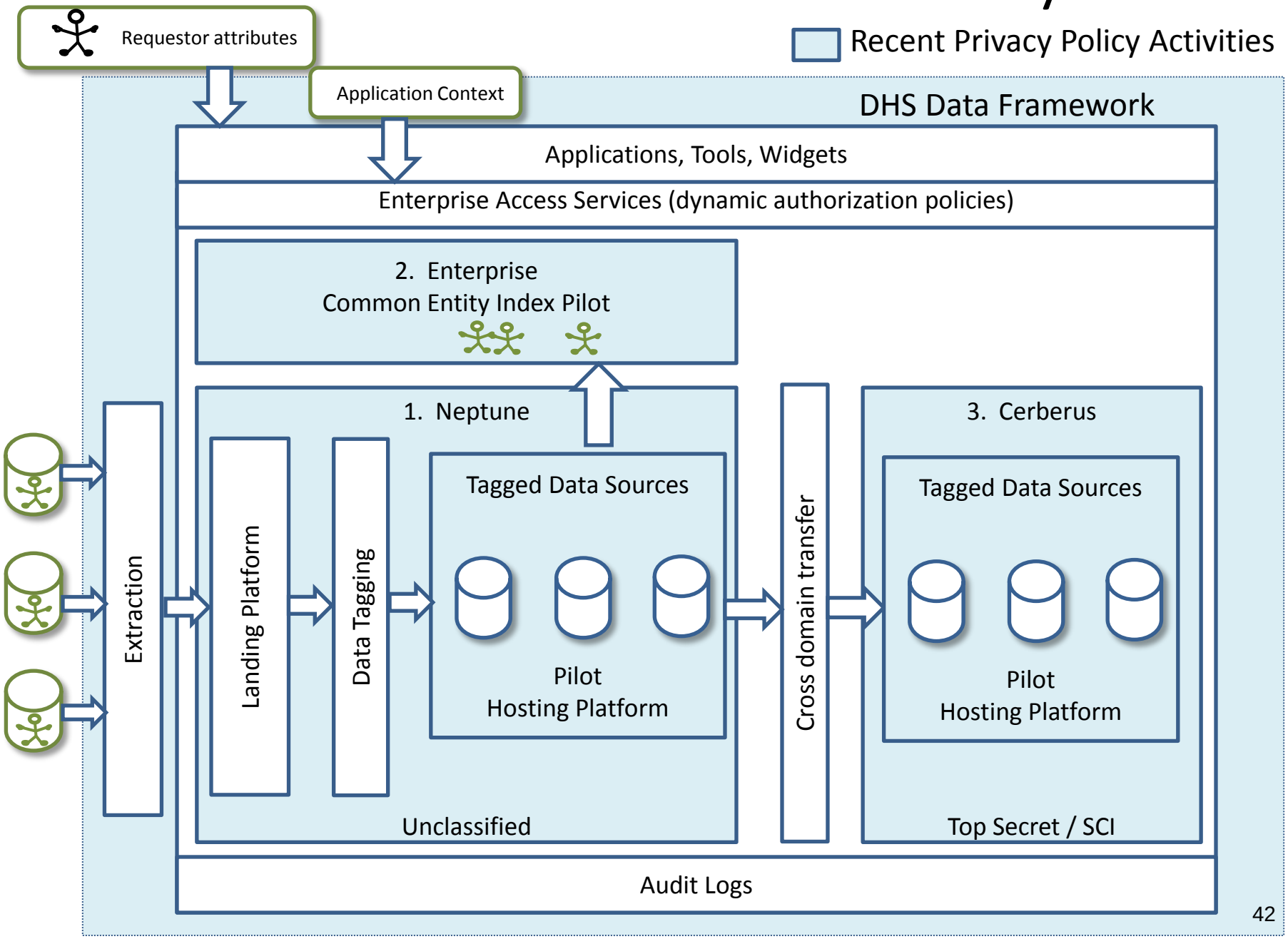
Cerberus (High Side Data Store)

- **Purpose**: Build a consolidated data store on the high side for screening and analysis; Align to ICite
- **Approach**: Test architecture, big data storage and data tagging techniques
- **Lead:** I&A
- **Pilot 3**: Cerberus

Access w/ Policies Data Tags Context



2013 Pilot Current Architecture & Privacy Activities



DPIAC Report Guidance

- **Controlling Access and Use**
- **Applicable Privacy Policies**
- Data Integrity and Quality Assurance
- Accountability and Audit
- Data Security and Data Retention
- Redress

Privacy Compliance Documentation

- System of Records Notice
  - Common Entity Index Prototype published 8/23/2013
- Privacy Impact Assessments
  - Overall Project PIA – in progress
  - CEI Prototype – in progress
  - Neptune – In progress
  - Cerberus – In progress

Questions?

Policy Subcommittee Report

Presentation of research findings regarding privacy considerations in the Department's use of live data for training purposes, for testing new or updated systems, or for research.

Joanne McNabb, Chair, Technology Subcommittee, DPIAC

Homeland Security | Privacy Office

Public Comments: 5:15 – 5:30

Homeland Security