

POLICY AUTOMATION

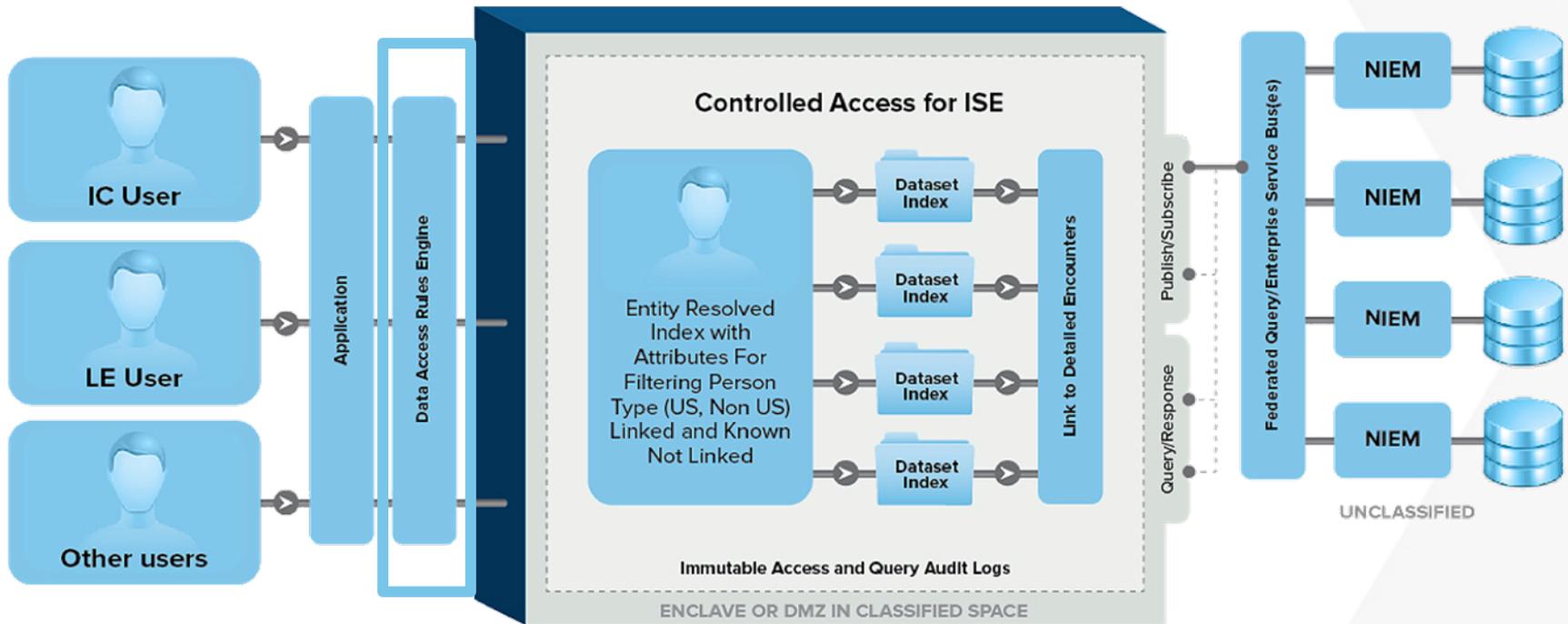
WIS3 | December 5, 2011

OUTLINE

- **Background**
 - CHISE (Controlled Homeland Security ISE)
 - DHS Framework Overview
- **Privacy Activities**
 - Dictionary
 - Flags for Model
 - Tags for IEPDs
 - Process coordination
- **The Contribution of Standards**

CHISE

CONCEPTUAL ARCHITECTURE INDEX



CHISE Goal: Provide a sustainable method to share information, in an architecture supportive of our privacy and legal requirements, under DHS control, accessible by the IC enclaves on classified networks.

CHISE BENEFITS

- *Minimize inefficient and costly duplication* of datasets
- Enable *efficient, federated searches* across DHS datasets
- Enable *controlled information sharing* across classified and unclassified domains in a way that protects search parameters and the underlying data
- Enable *efficient development of data analysis tools and services* tailored for multiple datasets
- Ensure *scalability of access to data* as appropriate for mission and task

FRAMEWORK COMPONENTS & PROCESS

- **Person Model**
 - Who is asking for access to data
- **Information Sharing Taxonomy**
 - Why are they asking for data - organizations, roles, and purposes of the request
- **Data Access Rules**
 - What are the restrictions and rules for access to the data
 - Based on SORN, PIA, and interviews with Top 10
- **Audit Log**
 - Immutable log to provide record of the request: who, when, what, why, and the result

PLAIN LANGUAGE RULES INTO XACML

AUTHORIZED PURPOSE

- National Security
- Law Enforcement
 - Investigations
 - Inspection
 - Assets seizure
- Intelligence

ACCESS REQUIREMENTS

- Need-to-know based on job mission/function
- Full background investigation
- TECS Security and Privacy awareness

ACCESS RESTRICTIONS

- Role-based
- Location of Duty Station
- Job Position

AUDIT REQUIREMENTS

- Transactional level logging
- Session level logging

INTERNAL USERS / INTERNAL PARTNERS

- All DHS components*
- ICE
- USCIS

OPERATIONS

- Read
- Search / Query
- Create
 - Supervisory review required
- Update / Modify
 - Supervisory review required
 - Int

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schemas:os" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schemas:os http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schemas-os.xsd" PolicyId="urn:isapf:names:tc:sp:policy:needtoknow" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
  <Description>
    This policy addresses some of the access requirements outlined in the PIA and SORN for the TECS platform (dataset). Specifically this policy addresses the following requirements for users access to TECS: 1. Has need-to-know Need-to-know: Need-to-know is determined by the mission/function/purpose that access to TECS will support.
  </Description>
  <Target>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">TECS</AttributeValue>
          <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DefsType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
  <!-- Rules -->
  <Rule RuleId="urn:isapf:names:tc:rs:rule:needtoknowlawenforcement" Effect="Permit">
    <Target>
      <Actions>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Law Enforcement</AttributeValue>
            <ActionAttributeDesignator AttributeId="urn:isapf:names:tc:sp:actions:authorizedpurpose" DefsType="http://www.w3.org/2001/XMLSchema#string"/>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  </Rule>
  <Rule RuleId="urn:isapf:names:tc:rs:rule:needtoknowintelligence" Effect="Permit">
    <Target>
      <Actions>
        <Action>

```

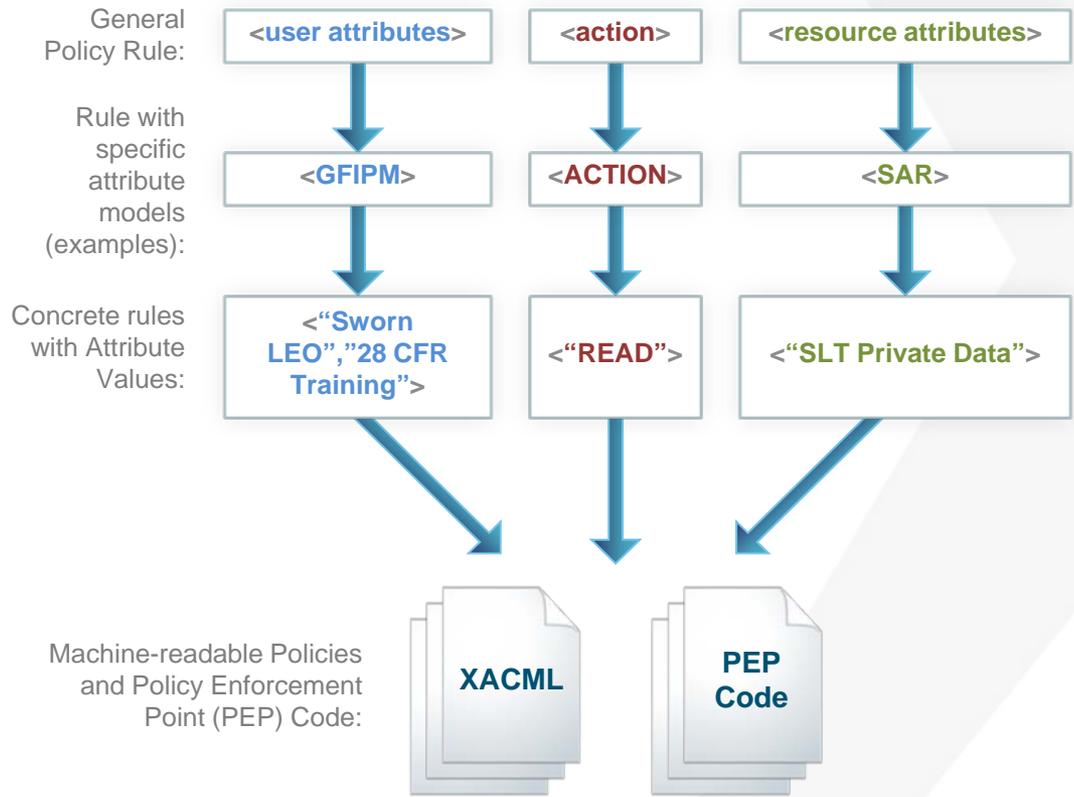

IDENTIFICATION AND MAPPING

Detailed legal analysis of privacy-related statutes, regulations, and policies:

Privacy Act of 1974, as amended, Electronic Communications Privacy Act (ECPA), E-Government Act of 2002, DHS Policy for Internal Information Exchange and Sharing, EO 12333, EO 13355, DHS ISE Privacy Protection Policy, OMB 7-17, PIAs, SORNs

- *Subject attributes define characteristics of the user*
- *Resource attributes define characteristics of the resource*
- *Action attributes define the actions that a subject may invoke on a resource based on the attributes of the user and the attributes of the resource.*

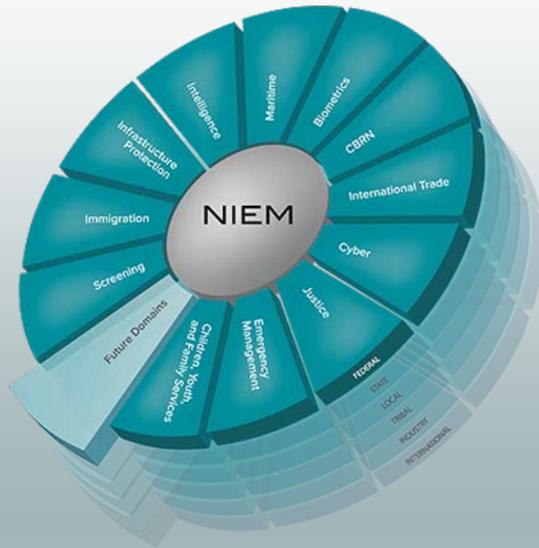
Laws, Statutes, and Policies



NIEM AND DATA TAGGING

Common Language

(Data Model Lifecycle)



- NIEM is a comprehensive data model that provides consistent semantics and structure

Repeatable, Reusable Process

(Exchange Specification Lifecycle)



- Model Layer
- IEPD Layer

PRIVACY ACTIVITIES

Federal Privacy Dictionary

Business Process Analysis

NIEM Data Tagging Analysis

Privacy Enabling Technologies Roadmap

QUESTIONS TO BE CONSIDERED DURING THE PRIVACY ANALYSIS PROCESS

- Do we all agree?
 - What information is sensitive
 - What is linked to terrorism
 - What is Mandatory and Voluntary disclosure
 - What “Promptly” make corrections means
 - How we define “Activity for which record sought”
 - Define “Timely” and “Accurate”
- Does “purpose for which it is collected” travel with the data?
- Do retention periods travel with data?
- Can we develop standard and reusable Routine Uses?
- What level of fidelity do we need in Activity?
- How and when we maintain accounting of disclosure?
- How an individual exercises First Amendment rights?

EXAMPLES

Policy Statement

Florida Constitution Sec. 24 Access To Public Records And Meetings.—

- (a) Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution.

Attributes

- Subject Attributes Organization: [Government: Legislative] Organization: [Government: Executive] Organization: [Government: State] Organization: [Government: Local]
- Resource Attributes Record Type: [Public Record] Record Use: [Official Business] Record Role: [Non Exempted]
- Actions [Transmit], [Access], [Share]
- Conditions Resource **Conditions:** Official business (True) Non Exempted Records (True)
- Rule Rule Target = Resource: Public Record

Policy Rule Statement

- Fla. Const. art. I, Sec. 24 (a)A [**Subject: All**] in [**Organization: Government: State, Local, executive, Legislative**] must perform [**Action: Transmit, Access: Share**] on [**Resource: Public Record**] for [**Purpose(s): All**] if [**Data: Conditions: Official business[Yes] (True) Non Exempted Records [yes](True)**], if [**Condition: Rule Target: Public Record**] and with [**Obligations: None**]. Effect = PERMIT.

THE PIECES TO SUPPORT PRIVACY

Issues	Stakeholder Community	Current Project	Other Projects
Definitions	Privacy	Data dictionary	
Problem Set Focus	Privacy	Business Process	
Identity Attributes	Privacy, Standards	Data Dictionary	GFIPM
Resource Attributes	Privacy, Standards	Data Tagging	
Obligations	Privacy, Standards	Business Process	GFIPM
Automated/Manual Obligations	Privacy, Standards	Business Process	
Environment	Privacy, Standards	Business Process	GFIPM
Allowed Assertions	Privacy	Business Process	
Level of attribute assurance needed	Privacy	Business Process	
Level of attribute timeliness needed	Privacy	Business Process	

REQUEST FOR THE STANDARDS COMMUNITY

- Define the reusable form for building privacy elements
- Define the requirements for Privacy Standards
- Help us define the issues at the highest level possible
- Develop a means for incremental implementation
 - Partial network compliance
 - Increasing complexity of Attributes
 - Increasing need to obtain attributes dynamically

WHY?

- Reusable policies that can implement elements of a privacy regime
- Understanding of the Privacy community in what can be automated and how well?

QUESTIONS?

Anthony Hoang

anthony.hoang@hq.dhs.gov

Patricia Hammar

patricia.hammar@associates.hq.dhs.gov