



THE CENTER FOR ADVANCED STUDIES  
IN SCIENCE AND TECHNOLOGY POLICY



## IMPLEMENTING EO 13356: STANDARDIZING TERROR DATA

**K. A. TAIPALE**

EXECUTIVE DIRECTOR

CENTER FOR ADVANCED STUDIES

PRESENTED AT:

THE POTOMAC INSTITUTE FOR POLICY STUDIES ROUNDTABLE:

“HOW SHOULD THE U.S. IMPLEMENT INFORMATION SHARING? A DISCUSSION ON THE  
EXECUTIVE ORDER STRENGTHENING THE SHARING OF TERRORISM INFORMATION”

ARLINGTON, VA • NOVEMBER 09, 2004

# Presentation Overview

- Technology, Security, and Privacy
  - Policy framework
    - emphasizes CT, sharing and operational security
  - Technical structure
    - rules based processing and authorization
    - data labeling (metadata) (XML)
  - Missing piece (privacy language)
    - but the technology supports both

# Call for Info Sharing

- “Executive Order 13356”
  - 1981, 1995 EOs (need to know/classification) (~priv)
  - Homeland Security Act of 2002 §892 (HSIS)
  - Executive Order 13311 - §892 delegated to SecDHS
  - HSPD-6 (09/03)
    - TTIC
    - “Terrorism information”
  - EO 13354 - NCTC (08/04)
  - EO 13356 - policy/system, sharing, preparation, domestic collection, “terrorism information” (need to share/write to share) (~priv)

# “Information sharing”

- “Everybody is for it, few understand it”
- Operational security (sources and methods) (and policy affects)
- Data/info security (~ one-way, cash) (and policy affects)
- Information use (~ Grey Davis) (and policy affects)
- Data veracity/reliability (IA) (counter-program) (contextual) WMD
- From “practical obscurity” to “volume obscurity” (overload)
- Share vs. “alert” (“I told you ...”)
- Barriers are largely legal and cultural, not technical
- Federation = LCD (trust/risk moves to edge of network) (~)
- Need appropriate business process for security

# Enterprise architecture

- Business process (policy)
  - security? (~ CT-centric)
  - sharing? (~ info to the right place)
  - privacy? (needs to be built in)
- Logic (support policy)
  - information flow management
  - rule-based processing
- Technical (support logic)
  - distributed architecture
  - policy appliances (control/mediate flows)

# Executive Order 13356

- Overview (need to share)
  - §1 Policy/Systems
  - §2 Duty to share
  - §3 Preparation
  - §4 Domestic collection
  - §5 Information Systems Council
  - §6 Definitions (“terrorism information”)

# EO 13356 Section 1

- §1 Systems/Policy
  - Policy: IT systems primarily to support CT (cf. intel reorg) and sharing (“interchange”)
  - “in the design and use of information systems and in the dissemination of information among agencies give:
    - (a) highest priority to sharing between agencies, Fed/state/local, protect sources and methods) and
    - (b) “protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsec. (a)”

# EO 13356 Section 2

- §2 Duty to Share
  - Affirmative duty to share “terrorism information” with other agencies with “counterterrorism functions”
  - Specific mandate to “write to share”
  - Implementation
  - Cf. EO 13353 Civil Liberties board  
(privacy not built in to technical infrastructure)

# EO 13356 Section 3

- §3 Preparation
  - metadata for operational and data security (“protect sources and methods”)
  - tearline (multiple versions at varying levels of classification)
  - shared free of originator control (cf., JTTF?)
  - minimize compartmentalization (eliminate physical network separation?) (~ secure “virtual machines”)
  - incentives/accountability (~ cya)

# EO 13356 Section 4

- §4 Domestic collection
  - AG, SDHS, DCI to develop “collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States,” I.e., rules for domestic CT intelligence gathering.) (90 days)
  - “including, but not limited to, from publicly available sources, including nongovernmental databases” (commercial databases)
  - “Other” - (USP abroad?)
  - Executive action to eliminate FI/DI, USP/non-USP line?
    - see Markle report re HSPD-6

# EO 13356 Section 5

- §5 Information Systems Council
  - Information Systems Council (ICS) (to plan and establish “interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies”) (120 days)
  - Cf. IC SIS (Intelligence Community System for Information Sharing)
    - ICON (charter 1999) (Intelligence Collaborative Operations Network) “To develop an IC information technology architecture that provides users secure access to information across the Community comparable to that currently provided within individual agencies”
    - Key requirement “Ability to share applications and information securely”

# EO 13356 Section 6

- §6 Definitions

- (d) the term “terrorism information” means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other United States Government activities, relating to (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) information relating to groups or individuals reasonably believed to be assisting or associated with such groups or individuals.
- How does this interact with other law? (~ PATRIOT, FISA)

# IC System for Information Sharing (ICSIS)

- Intelligence Collaborative Operations Network (ICON) (charter 1999)
  - “community space” concept (move from agency space, to shared space, to community space)
  - “approved” early 2001 by Intelligence Community Deputies Committee (ICDC)
  - develop uniform interpretation of DCID 6/4, 1/19, 1/2 & 6/3

## IC SIS cont.

- “Where we want to be” (2001-2003) (c.2000)
  - data access from anywhere at any time
  - fully interoperable data stores
  - streamlined flow from collector to producer to customer aided by intelligent applications
  - secure push and pull between spaces
  - analytic tools and digital production support
    - To develop an IC information technology architecture that meets the customer’s expectations for sharing information and assets across the Community

## IC SIS cont. 2

- What is Phase One? (c. early 2001)
  - infrastructure that issues and maintains certificates for all ICSIS users (PKI infrastructure)
  - full Service directories that include and can be used by all ICSIS users
  - secure email systems for exchange of information up through B level (cf. FBI - no email in secure areas)
  - controlled TSABI approved interface(s) to collateral space

## IC SIS cont. 3

- What is Phase One? (c. 2001)
  - an agreed set of databases and applications hosted in either Community or Organization Shared space
    - Collaboration tool kit
    - Web-enabled applications and databases
  - meta data and markup standards defined and implementation started
    - With agreed level of content and security markings
  - a “community space” infrastructure to support Phase One
  - a communications infrastructure with bandwidth adequate to support Phase One capabilities

## IC SIS cont. 4

- What is Phase One? (c. 2001)
  - system engineering and integrations support organization for defining interfaces and maintaining standards
  - a governance mechanism for overseeing day-to-day operations as well as future enhancements

## IC SIS cont. 5

- Welcome to Phase 2, four years later (2004)
  - June 2004 DCI issues a “management imperative emphasizing data sharing”
  - “officials [then] began developing an enterprise architecture plan for data sharing, IT services, and information assurance”
  - Phase 1 (2000-2004) recast as “developing policies, procedures and standards for sharing ”
  - Phase 2 is “more about data and tools and applications to process data” and includes tagging, collaboration and acquisition initiatives ...

# Anyway ...

- Shifting security and privacy paradigms

# (Cyber)Security + INFOSEC + NATSEC

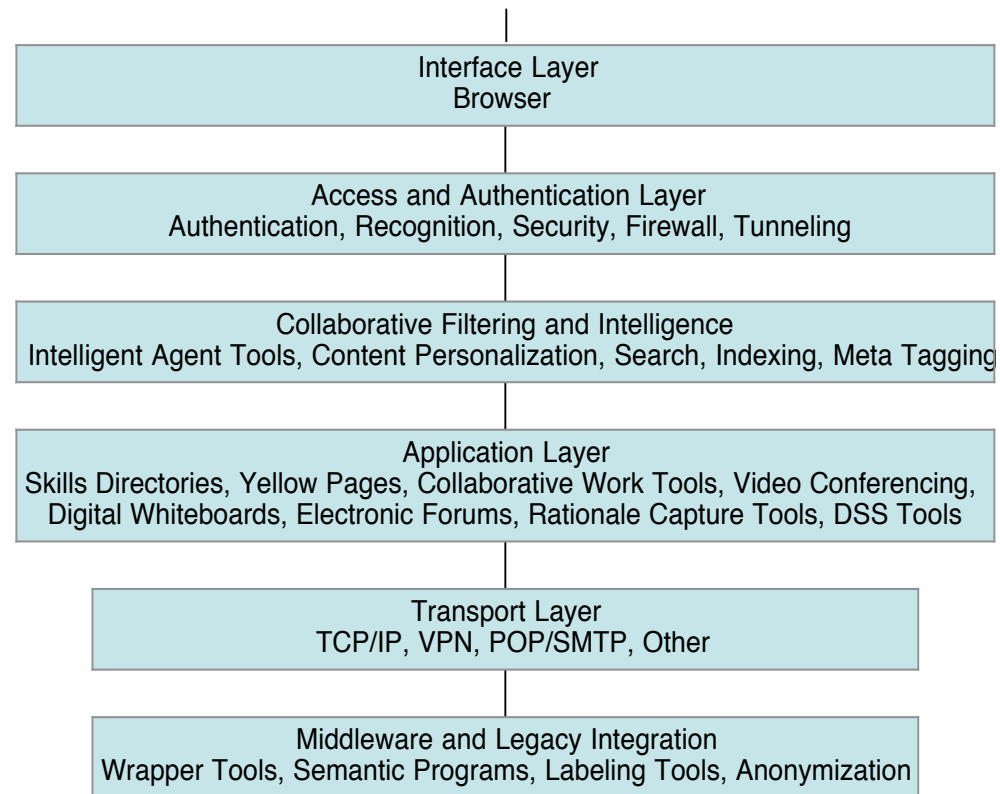
- Historical migration of security locus
  - Security in WAN (“access control”)  
 (“smart” closed network vs. open end-to-end IP architecture)  
 (~VPN) (~ totalitarian vs. free systems)
  - Security in LAN (firewall) (“access/accountability” control)  
 (~borders)
  - Security in application (current) (“accountability” control)  
 (~TSA)
  - Security in data (predicted) (“resilience/recovery” control)  
 (~data and identity surveillance)

# Privacy

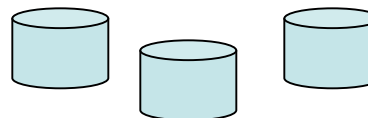
- Privacy (protected through technical inefficiency)
  - control in network (collection)
  - control in database (stovepipe)
  - control in data (data labeling)
- Privacy  $\equiv$  DRM
  - control in network, control in device, control in data
- “Smart” data
  - develop technologies to make data “responsible” for its own processing

# Overall architecture

USERS



Legacy Data, Distributed Data,  
Data Warehouse, Forums,  
Document Bases, Other



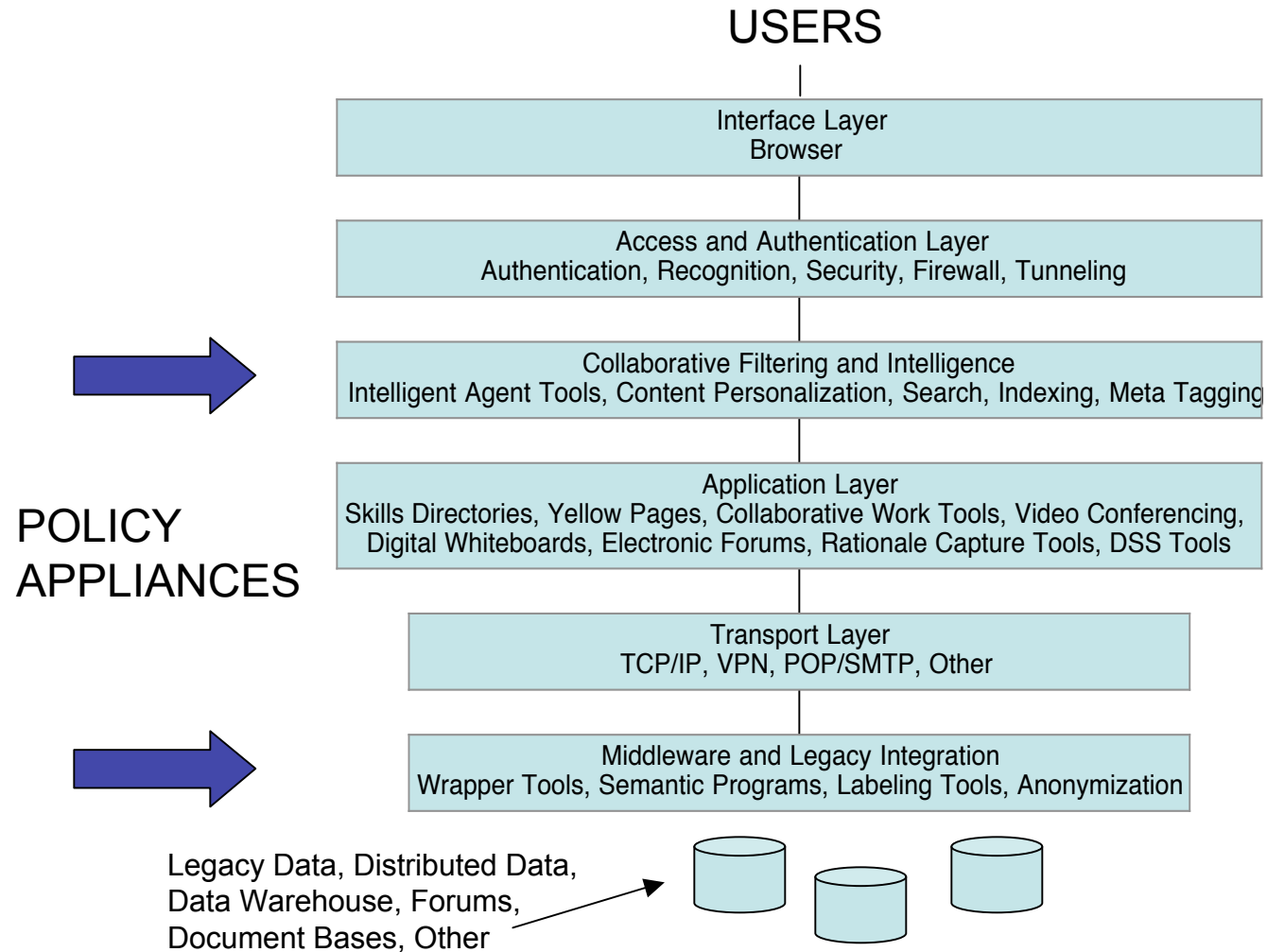
# Smart data systems

- Common language (DTD, XML schemas, protocols)
- Analytic filtering
  - to DB (agent)
  - from DB (tuple)
  - Note on collection (“cost” of data availability)
    - ~ Carnivore (cf. Echelon) (select/delete vs search/store)
- Program semantics
  - legacy data, derivative data
  - contextualize use “on the fly” to categorize data to correspond to query

# Smart data technologies

- Labeling (meta-data) (XML)
- Wrappers (encrypted) (~ hashing)
- Proof carrying code (~ credentialed query)
- Self reporting data (~ DB reporting)
- ???

# Policy Appliances to Enforce Rules



# Technical issues

- Arbitrary nature of designation
  - policy attribute vs. data attribute
  - relationship of attribute to collection/transaction/query
- Commingling
  - collection policy doesn't match use categories
- Derivative and legacy data
- What is “intake” in a distributed architecture
  - pre-processing?
  - collection problem with identity systems (see PR)
- Policy problem -- re-purposing

# Technologies req. to Implement EO 13356

- Rules-based processing
  - build policy rules into processing
    - security (§2)
    - privacy (?)
- Technologies the same for security and privacy
  - selective revelation or selective attribution
  - credential/authorization
  - audit (control of logs)

## IC SIS cont. 6

- IC Metadata Working Group (IC Dep. Comm.)
  - IC MWG (2004)
    - IC Metadata Compliance Plan (SAIC)
    - IC XML Registry
    - Tearline XML
    - Taxonomy/Thesaurus
    - Terrorist Watchlist Person Data Exchange Format
    - Geospatial Metadata (NGA)
    - HUMINT namespace
    - SATURN, StoneGhost, 5-Eyes
  - DOD XML (DOD GIG)
  - Global Justice XML v.3.0

# Potential “privacy” taxonomies

- Who the data relates to
  - subject-based
  - US person (USSID-18 exception vs. rule problem)
- Where/how it was collected
  - foreign/domestic, public/private, commercial
  - collection vs. use for existing data (re-purpose problem)
  - by owner (FI, CFI, LE, Gov, Com, Priv)
  - by legal structure
- What kind of information it is
  - identification (identifier/identity)
  - communications -- BSD (account info), traffic (who you called), content (what you said)
  - transactional -- traffic (you where there), content (you bought X)
  - “sensitive” - (Markle - identifiable/available) (statutory - Bork)

# Conclusion

- Next step is to develop a common policy language so that technical requirements can be specified in the IC XML framework