National Counterterrorism Center

Office of Mission Systems

NDIA Biometrics Interoperability Panel

Dirk Rankin
28 Jan 2009

Overview

- Definitions
- Challenges: Collection, Storage, Use & Analysis, Sharing
- Considerations: Policy, Technology, Community
- Summary

Definitions*

- **Biometrics**: the measureable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition

- **Interoperability**: the ability of two or more systems or components to exchange information and to use the information that has been exchanged

* NSPD – 59 and HSPD –24, 5 Jun 2008

Challenge: Collection

- Cooperative Users
  - Rapid & quality collection of unique biometric data
    - Fingerprints, Iris Scans, Facial Features, DNA, etc.
  - Need standardized collection methodologies
    - Streamline data format translation and archiving for better matching
    - Facilitate efficient updating of changes to biometric features
      - Cosmetic Surgery, Facial Hair, etc.

- Non-Cooperative / Uncooperative Users
  - Rapid & quality collection of unique biometric data *at distance*
  - Growing need for ruggedized sensors worldwide
    - Housings/profile, power, weight, computation, communications
    - Complex collection environments; automation
    - Narrow collection windows

Challenge: Storage

- Biometric data will drive storage solutions geometrically vs. biographic-only based designs
  - PetaByte level depending on collection resolution, number of samples, number of entities
  - Data format compatibility with current production systems to enable efficient operational use within O&M budgets

- Solid Certification & Accreditation criteria and process is crucial
  - Accreditation officials from all stakeholders share equities
  - Must protect U.S. Person’s data from unauthorized access
  - Must provide assured access control for authorized users within IC and LE communities respectively
  - Must provide assured access control for those entities authorized for both IC and LE datasets

- Robust backup storage is mission essential
  - Many biometric data collections will be one-time events
  - Crucial component of Continuity of Operations / Disaster Recovery

Challenge: Use & Analysis

- NCTC phased implementation approach to biometric enabled intelligence (BEI) for counterterrorism:
  - Phase 1:
    - Receive, ingest and forward to the TSC nominations of KSTs to include biographic data, facial images and biometric reference numbers
  - Phase 2:
    - Receive and store nominations of KSTs to include biographic data, facial photos, raw fingerprint image files, raw iris image files and biometric reference numbers
    - Introduce CT Data Integration Layer (CTDIL) capability
    - Coordinate and implement standardized electronic nomination format (including associated biometrics) to enable automated ingest into TIDE
  - Phase 3:
    - Search / match raw biometric files against existing TIDE holdings using CTDIL as data service capability (SOA based)
    - Distribute to TSC a comprehensive terrorist identity record

Challenge: Sharing

- Provide assured access across security domains
  - Biometric information, once stored within TS/SCI domain (even if unclassified), generally stays in that domain
  - Maximizing biometric information sharing requires:
    - storing data at lowest permissible security domain, then enabling secure access mechanisms for users operating within higher domains
    - storing data at highest security domain, then enabling secure access from lower domains
  - Multilevel security platform-based solutions; verified mandatory access control model

- Data standardization ownership and adoption
  - NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards
  - IC Information Sharing Data Standards Coordination Activity
    - Terrorist Watchlist Personal Data Exchange Standard (TWPDES)
    - National Information Exchange Model (NIEM)
    - DoD – DNI Universal Core (UCORE)

Policy Considerations

- …AG and DNI shall ensure that policies and procedures for the consolidated terrorist watchlist maximize the use of all biometric identifiers
- …DNI shall maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols and interfaces
- …DNI shall ensure compliance with laws, policies, and procedures respecting information privacy, other legal rights, and information security
- …DNI shall ensure that biometric and associated biographic and contextual information on KSTs is provided to NCTC and TSC
- …DNI shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners

- **Data Exploitation Way Ahead: Which Model ??**
  - Bring Data to the Processor (replication model – high cost)
  - Bring Processor to the Data (services model – high integrity)

Technology Considerations

- Database
  - Relational (Oracle, “pair-at-a-time”)
  - Hierarchal (XML, “many-at-once”)
- Web 2.0 technologies
  - Cloud Computing (shared processing, storage, etc.)
  - Service-oriented Architecture (SOA) constructs
- Modernized, fast moving code base
  - Open Source, Commercial, Government
- Access and dissemination across security domains
  - User authentication (LDAP, etc.)
  - Approved, accepted, adopted Protection Level (PL) capabilities for implementation of sharing paradigm

Community Considerations

- Must converge on methodologies, standards, formats, security, schedule, cost, performance, risk, maintenance, refresh…
  - Implementation synchronization hard to do

- Unified CONOP required to minimize number of variables, lower cost, increase potential for success
  - Policy authorization, support, resourcing essential
  - Long-range mindset

- How to integrate Vertical and Horizontal paradigms
  - Vertical: top-down policy, budget…
  - Horizontal: peer-level stakeholder implementation…

Summary Points

- NCTC recognizes the value of biometrics in identity discovery
- Current state: working to incorporate biometrics into the USG’s central repository for KSTs
  - Means a more comprehensive repository for analysts and better watchlisting support to screeners
- Effective biometric enabled intelligence (BEI) implementation requires new thinking and strong commitment across stakeholders

BACK-UP

Watchlisting: Legal and Policy Framework

- IRTPA: December 2004
  - NCTC to serve as the central and shared knowledge bank on known and suspected terrorists (KSTs)
- HSPD-6/TSC MOU: September 2003
  - Development of a comprehensive database of international terrorist identities at the NCTC
  - Creation of TSC to consolidate the governments approach to terrorist screening
  - NCTC as single source of international terrorist data for the TSC's consolidated watchlist database
- Addendum A and B to TSC MOU: August 2004 and January 2007
  - DOD and Treasury added to database sharing community of interest
  - Expands FOUO data identifiers from ~ 7 to 40
- NSPD 59/HSPD 24: June 08
  - Focus on biometrics to further identify KSTs
  - Category of National Security Threats (NSTs)
  - Calls for Interagency Action Plan