Use of Rapid Biometric Devices by Florida Law Enforcement
Introduction

• A Quick History
  ○ Rapid ID Pilot – October 2006
    - Jessica Lunsford Act –
      - Re-registration of sex offenders
      - Identification of probationers
    - Roadside stops
    - Jail/Prison intake/release
    - Court – First Appearance
    - Domestic Security
  ○ Rapid ID Full Operational Capability – October 2009
    - FBI RISC (Repository of Individuals of Special Concern)
    - DNA Verification
    - Warrant Service
Devices/Transactions

- **Number of devices** – 5,632 active devices
  - Mobile – 4,406
  - Fixed or tethered – 1,226

- **Average transactions**
  - 47,221 per month
  - 65% Hit rate (not accuracy, criminal encounters)
General Characteristics (1)

- Desired matching / enrollment capabilities:
  - Enrollment: controlled facility – not mobile (at booking)
  - Search & Match capability
    - Two Modes:
      - Two finger search against 5.5M subjects
      - One finger (1:1) verification of subject with identifier (i.e. SID)
    - Response time target <1m
    - Wants/Warrants & Rapsheet returned on hits
  - Types of responses
    - Hit, No-Hit, Ambiguous for Florida CMF
    - Red, Yellow, Green for RISC
General Characteristics (2)

- Database verification:
  - **Enrollment**
    - **Submission**: Tenprint by local Sheriff/Jail/Corrections
      - fingerprints / face (if available) for criminal history
    - **Response time**: Ten minutes or less
    - **Connectivity**: Criminal Justice Network (CJNet) –
      - Dedicated T1/MPLS at every criminal justice agency
  - **Search/Verification**
    - **Mobile devices**: Florida Highway Patrol Troopers and several thousand Police Officers and Sheriff Deputies.
    - **Connectivity**: Bluetooth from device to Mobile Data Terminal, air-card VPN to CJNet point of presence.
    - **Response requirements**: 24 seconds average response
Mobile Unit Description

- **Mobile Unit Data Captured:**
  - Fingerprints (index and middle finger -- 2,3,7,8 any combination is allowed)

- **Form Factor / User Interface**
  - **Cogent:**
    - CSD301 and CSD330 – FAP 10 tethered devices (mobile)
    - CSD450 – FAP 30 tethered (jails and courthouses – not really mobile)
    - MI3 – FAP 30 wireless
    - Blue Check FAP 10 wireless
    - Blue Check 2 (optical scanner) FAP 10 wireless
    - Blue Check 2U FAP level 10 wireless
  - **Motorola:**
    - MC75 – FAP 10 wireless
  - **MorphoTrak:**
    - MorphoIdent – FAP 20 wireless
  - **L1:**
    - IBIS Extreme – FAP 30 wireless
  - **CrossMatch:**
    - Verifier 300 or 310 - FAP 30 tethered
    - Verifier MW – FAP 30 wireless
Data Exchange Requirements (Details)

- Fingerprints sent to State Identification Bureau for searching against Florida Criminal Master File
  - Unique identifier for the transaction, individual and device
  - Interface Control Document available
    - [www.fdle.state.fl.us/Content/FALCON/Menu/System-Requirements/Current-FALCON-ICD.aspx](http://www.fdle.state.fl.us/Content/FALCON/Menu/System-Requirements/Current-FALCON-ICD.aspx)
- Fingerprint images must meet quality standards of ANSI/NIST-ITL in order to be usable and have enough associated metadata to ensure traceability to the officer and device.
Lessons Learned

- Lessons learned –
  - Areas of most concern are user training and documentation of success stories.
    - For both of these it has been imperative to develop and sustain relationships with the local agencies.
  - Continuous spot checking of transactions has helped to identify issues that can quickly be addressed usually through additional training.
Future Plans

• Searching additional repositories – NDR flag
  ○ Recent approval to pilot connectivity to US-Visit via FBI CJIS for Florida Domestic Security Task Forces.

• Interoperability with other agencies
  ○ Regional States
  ○ Federal Partners – Currently discussing with FBI Flyaway Teams and use of Quick Capture Devices by Florida FBI Field Offices.

• Livescan integration to perform Notice to Appear/Cite and Release arrests on scene.