Biometrics in US Army
Accessions Command

LTC Joe Baird
Mr. Rob Height
Mr. Charles Dossett
Title: Biometrics in US Army Accessions Command

Performing Organization: Defense Research and Engineering, Biometrics Identity Management Agency (BIMA), Washington, DC, 20301

DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

Supplementary Notes:

Security Classification of:
- Report: Unclassified
- Abstract: Unclassified
- This Page: Unclassified

Limitation of Abstract: Same as Report (SAR)
Number of Pages: 8
Army Accessions Command (AAC) recruits the Active and Reserve enlisted force and recruits and trains officers for the Active component, Reserve, and National Guard.

**FY 11 Enlisted Mission**
United States Army Recruiting Command (USAREC) – 93,000

**FY 11 Officer Mission**
Cadet Command (ROTC) – 5,350

Source: USAAC G3, as of 20101025
Problems and Challenges

• Approximately 10% of the 17-24 Youth Market is not qualified to serve in the military due to **criminal history**.¹

• Currently we don’t get comprehensive resolution on an applicant’s criminal background until after he or she goes to the Military Entrance Processing Station (MEPS) to enlist and gets fingerprinted.

• The information we do have is based on applicant disclosure and what can be discovered from local, no-fee, police checks.

• There are substantial resources wasted in terms of recruiter time, MEPS processing workload, and logistical costs when an applicant is found unfit to serve at the point of enlistment.

¹ Source: Lewin Group 2007 Study; Developed by US Army Accessions Command G2/9, Center for Accessions Research (CAR)
Biometrics-enabled Solution

- What we are doing:
  
  - Capturing fingerprints electronically
    - Hardware is in place, or postured for fielding this year, across the command
    - 271 locations in Cadet Command, over 1500 in USAREC
  
  - Moving timeline for FBI checks to the left
    - Formal fingerprint check with FBI is typically done at point of enlistment at the MEPS.
    - Currently running FBI checks on a limited scale (Tampa Recruiting Battalion and other selected companies) during the interview stage of the process.
Biometrics-enabled Solution

• The LiveScan implementation in the Tampa Recruiting Battalion has yielded significant improvements to efficiency, effectiveness and accuracy:

  – Fraudulent enlistment (from law violations) rates have gone from approx 50-70 per year to zero.

  – All charges are identified up front, including juvenile charges, without doing manual police checks (time intensive) or forfeiting information available in fee-based checks (incomplete).

  – Eliminates MEPS floor count losses and jobs unnecessarily pulled from the system due to fraudulent enlistments (from law violations).
Metrics

- How we are measuring success:
  - Hours spent by recruiter running police checks per applicant
  - Number of fraudulent enlistments from law violations
  - Cost per applicant of providing background checks (future)
Challenges/Opportunities

• Our implementation challenges:
  – Software acquisition and configuration
  – Moving from thick client to thin client
  – Integration into the Integrated Accessions Architecture (IAA)
  – Policy that regulates which nodes can transmit and accept fingerprints and results

• The way ahead:
  – FBI checks conducted at the interview stage across the entire Accessions Command
  – Single repository for all biometric data in the command
  – Use captured fingerprints for positive identification in VIPS
  – Single channeling agent for all fingerprints going to the FBI
  – Collect fingerprints for geographically separated civilian hires
  – SF86 data paired with fingerprint results for each applicant/cadet security investigation prior to submission to the Office of Personnel Management (OPM)