Biometric Uses for Mobile Devices: NCIS’s Portable Biometrics Equipment Pilot

Dr. Mike Missler, Booz Allen Hamilton

supporting the

NCIS Biometrics Program Office

CTST 2009, New Orleans, LA

7 May 2009
Overview of NCIS
- NCIS’s need for mobile biometrics equipment
- Conducting a pre-deployment pilot
- Conclusion
NCIS is a team of law enforcement professionals dedicated to protecting the people, families, and assets of the U.S. Navy and Marine Corps worldwide

- In support of its mission -- to prevent and solve crimes that threaten the warfighting capability of the U.S. Navy and Marine Corps – NCIS pursues three strategic priorities:
  - Combating Terrorism (CT) -- detecting, deterring, and disrupting terrorism against Department of the Navy (DoN) personnel and assets
  - Counterintelligence (CI) -- safeguarding DoN classified information
  - Law Enforcement (LE) -- investigating all major criminal offenses (felonies) -- those crimes punishable under the Code of Military Justice by confinement of more than one year -- within the DoN

- NCIS works closely with other local, state, federal, and foreign agencies to counter and investigate terrorism, espionage, computer intrusion, homicide, rape, child abuse, arson, procurement fraud, and more

- Composition:
  - 2320 personnel including 1293 special agents
  - 90% Civilian
  - NCIS special agents (97%) have statutory arrest authority

NCIS Special Agent Afloat takes notes during USS Wasp transit through Suez Canal
NCIS Major Offices

Puget Sound, WA
Camp Pendleton, CA
San Diego, CA
Washington, DC (FO and HQ)
Norfolk, VA
Camp Lejeune, NC
Mayport, FL
Pensacola, FL
Contingency Response FO
Singapore
Naples, Italy
Bahrain
Honolulu, HI
Yokosuka, Japan
Newport, RI

140+ locations worldwide
17 Major Offices: NCIS HQ; 14 Regional Field Offices (FOs), 2 Functional FOs
All Carrier Strike Groups
All Expeditionary Strike Groups

Naval Criminal Investigative Service
Overview of NCIS
- NCIS’s need for mobile biometrics equipment
- Conducting a pre-deployment pilot
- Conclusion
NCIS leaders want to leverage biometrics to better support investigations and improve agent safety

- Currently, Special Agents (SAs) take fingerprints to support NCIS’s LE strategic priority, where fingerprints are submitted
  - To the Federal Bureau of Investigation’s (FBI’s) Integrated Automated Fingerprint Identification System (IAFIS) via fingerprint cards and large, immobile LiveScan units
  - Late in the investigative process after a suspect has been charged with a felony
  - Without requesting/receiving prior criminal record information from IAFIS

- Recent mobile biometric technology advancements potentially support all (LE, CI and CT) strategic priorities, enhancing SA investigations in the field by
  - Identifying suspects/informants with records on file – e.g., in IAFIS, the Department of Defense’s (DoD’s) Automated Biometric Information System (ABIS), and other government biometric databases/watchlists -- thus thwarting attempts to hide identity with missing/false driver’s license, social security number, etc.
  - Guiding more effective interrogations of suspects/informants
  - Handling suspects/informants safely, consistent with their potential for violence
NCIS Director Betro was inspired by a briefing on the FBI’s mobile biometrics equipment – his guidance is to get this capability to NCIS SAs in the field

- The FBI has had success with its Quick Capture Platform (QCP) in Iraq, Afghanistan, Somalia and Ethiopia by doing rapid acquisition and search of known and suspected terrorists through IAFIS and ABIS
  - The QCP provides electronic collection followed by wireless communications (submission to and response from) IAFIS/ABIS in as little as two minutes
  - The QCP can be loaded into a backpack that weighs 22 lbs

- An SA carries in excess of 50 lbs of equipment when working in the field; any new equipment must be light and provide a real benefit for the SA to want to take it to the field and use it
The FBI’s Criminal Justice Information Services (CJIS) Division developed the QCP to support enrollments and searches of FBI and DoD biometric databases from remote locations.
Agenda

- Overview of NCIS
- NCIS’s need for mobile biometrics equipment
  - Conducting a pre-deployment pilot
- Conclusion
The problem is to determine how to effectively acquire, integrate, and deploy mobile biometrics equipment when faced with numerous challenges, such as

- Lack of infrastructure: new tools, process and people infrastructure is needed to provide, e.g., equipment, training, maintenance support, rapid two-way communications between the biometrics equipment in the field and IAFIS, etc.

- Cost of procurement and sustainment: massive deployment of new technology (and its associated infrastructure) requires significant funds that may not be currently available

- Disuse of equipment: SAs may cease to use equipment that is too heavy, unreliable, or of minimal utility – SAs have to see the value of the technology
The first step to resolving the problem is to conduct a pilot of available mobile fingerprint technologies at pre-selected NCIS sites

- If the pilot identifies a solid portable solution then challenges will be addressed as follows:
  - Lack of infrastructure: the pilot will verify the new tools, process and people infrastructure needed; it will facilitate planning to shore up the infrastructure
  - Cost of procurement and sustainment: since NCIS will better understand the portable infrastructure it needs, it can strongly justify a request for funds to build it
  - Disuse of equipment: the solution will demonstrate benefit to SAs and uncover requirements for improvement that will provide greater benefit

- Else the pilot will determine requirements for a solution that needs to be developed
Additional issues for consideration

- **Policy**: Establish policies for the collection and use of biometrics in support of LE, CI and CT strategic priorities
  - Identify appropriate government biometric databases/watchlists for each strategic priority
  - Handle citizenship and privacy concerns properly

- **Business Process**: Improve biometric business processes
  - Train NCIS personnel in how to quickly submit biometric data and use immediate feedback information
  - Establish a biometrics analytic capability to support intelligence efforts

- **Technology**: Address security of biometrics data and equipment
  - Use encryption throughout enrollment, transmission and storage
  - Certify and accredit mobile devices for high-speed Internet connectivity
  - Protect data on mobile devices that are lost or stolen
Several questions surface when planning the pilot

- What are the goals of the pilot?
- What mobile fingerprint devices should be used during the pilot?
- How will two-way connectivity between mobile fingerprint devices and IAFIS be established?
- How can DoD watchlists be obtained and loaded on the mobile devices?
- What training and exercises are needed for SAs participating in the pilot?
Q: What are the goals of the pilot?
A: The goals are to:

- Engage NCIS SAs into the usefulness of automated fingerprint technologies
- Identify the right portable solution(s) for NCIS SAs – find out what works
- Determine desired/non-desired functionalities of the solution(s)
- Determine tools, processes, and people infrastructure needed
- Develop a plan to fill the infrastructure gaps
- Estimate infrastructure procurement and sustainment costs
Q: What mobile fingerprint devices should be used during the pilot?
A: Pilot devices should:

- Collect and transmit fingerprints of acceptable quality for IAFIS enrollments and queries
- Receive IAFIS hit / no hit feedback within 30 minutes, where hit feedback includes criminal history information
- Store DoD watchlists to a watchlist that resides on the device
- Add fingerprint records collected by the device to its watchlist
- Search the device’s watchlist against a fingerprint record taken by the device and return hit / no hit feedback within two minutes
- Meet the following mobility constraints
  - Weigh less than five pounds
  - Fit into a large trouser pocket
  - Rugged -- consistent with a Panasonic Toughbook
Investigation of devices that meet NCIS requirements reveals incomplete solutions

- L1 Handheld Interagency Identity Detection Equipment (HIIDE) being used widely in Iraq and Afghanistan is mobile, but can only take a single flat fingerprint that is unacceptable for IAFIS enrollments and queries.

- System for Intelligence and Identity Management Operations (SIIMON) promises to meet NCIS requirements, but is under development and not available.

- QCP components (Cross Match Guardian and Panasonic Toughbook computer) provide IAFIS enrollment and query capabilities, but do not meet NCIS mobility constraints.

- Cross Match Secure Electronic Enrollment Kit (SEEK) provides IAFIS query capabilities and mobility, but does not meet IAFIS enrollment capabilities.
The decision was made to evaluate three different configurations of the following equipment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Equipment Lineup</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><strong>Toughbook Guardian R2 Combo</strong>&lt;br&gt;Panasonic Toughbook + Guardian R2 + BGAN*</td>
<td>▶ Easy to view laptop screen&lt;br▶ Easy to use laptop keyboard&lt;br▶ Full enrollment and query capability&lt;br▶ Large watchlist (&gt; 40k on SEEK)</td>
<td>▶ Least portable alternative&lt;br▶ Lacks SEEK iris and facial image capabilities</td>
</tr>
<tr>
<td>B</td>
<td><strong>SEEK ID Guardian R2 Combo</strong>&lt;br&gt;Seek ID + Guardian R2 + BGAN</td>
<td>▶ Full enrollment and query capability&lt;br▶ SEEK capability (fingerprints, iris and facial images)&lt;br▶ More portable than A</td>
<td>▶ Small screen&lt;br▶ Need external keyboard when doing enrollments&lt;br▶ 40k person watchlist</td>
</tr>
<tr>
<td>C</td>
<td><strong>Seek ID Standalone</strong>&lt;br&gt;Seek ID + BGAN</td>
<td>▶ Query capability&lt;br▶ SEEK capability (fingerprints, iris and facial images)&lt;br▶ More portable than A or B</td>
<td>▶ Cannot do enrollments&lt;br▶ Small screen&lt;br▶ 40k person watchlist</td>
</tr>
</tbody>
</table>

* Broadband Global Area Network, a **global satellite Internet network with telephony using portable devices**
SAs will need to determine which equipment configuration best matches their mission needs and field conditions.
The tradeoff between the capabilities of a configuration and mission conditions will be evaluated.
For fingerprint enrollments and queries, the Cross Match Guardian R-2 will be evaluated

- Captures fingerprints; approved by FBI for fingerprint enrollment
- Approximately 6” X 6” X 5”
- Weighs 5 lbs.
- USB connection to computer (Toughbook or SEEK)
For fingerprint queries only, the Cross Match Secure Electronic Enrollment Kit (SEEK) will be evaluated

- Captures fingerprints, iris, mug shots
  - Two finger fingerprint slaps
  - Not approved by FBI for fingerprint enrollment

- Size: Approx 8” X 5” X 4”

- Weighs 3 lbs

- On board computer; small touch screen approx. 4” X 3.5”

- USB connections to Guardian R2 and modem
Q: How will two-way connectivity between mobile fingerprint devices and IAFIS be established?
A: The following architecture will support the pilot:
Q: How can DoD watchlists be obtained and loaded on the mobile devices?
A: The Biometrics Task Force in West Virginia assists here by

- Receiving current DoD watchlists
- Running a software application that transforms the DoD watchlists into a format that can be loaded on mobile biometric devices
- Sending processed watchlists to NCIS via CD or FTP
Q: What training is needed for SAs participating in the pilot?  
A: The training plan is:

<table>
<thead>
<tr>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to the NCIS biometrics program and equipment (SEEK,</td>
<td>Configuration exercises (2 hrs)</td>
<td>‘Train an Agent’ evaluative (3 hrs)</td>
</tr>
<tr>
<td>Guardian R2, Toughbook, and BGAN) (2 hrs)</td>
<td>Scenario exercises (2 hrs)</td>
<td>Review and feedback on equipment and biometrics program (1 hr)</td>
</tr>
<tr>
<td>Managing MOBS (Mission Oriented Biometrics Software) (2 hrs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Developing and using a watchlist (0.5 hrs)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Introduction to the NCIS biometrics program and equipment (SEEK, Guardian R2, Toughbook, and BGAN) (2 hrs)
- Managing MOBS (Mission Oriented Biometrics Software) (2 hrs)
- Developing and using a watchlist (0.5 hrs)
- Configuration exercises (2 hrs)
- Scenario exercises (2 hrs)
- ‘Train an Agent’ evaluative (3 hrs)
- Review and feedback on equipment and biometrics program (1 hr)
**Q: What exercises are needed for SAs participating in the pilot?**

**A: The exercise scenarios are:**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Activity Breakdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct full enrollment &amp; transmit</td>
<td>Identify suspect ▶ Enroll rolled ten prints and slaps into MOBS* (SEEK ID or Toughbook with Guardian R2) ▶ fill out suspect’s information ▶ capture mug shots and other photos ▶ when charges are referred transmit prints to IAFIS via telephone line or BGAN ▶ fetch IAFIS response</td>
</tr>
<tr>
<td>Query IAFIS</td>
<td>Identify suspect or informant ▶ take fingerprint slaps using MOBS (SEEK or Toughbook with Guardian R2) ▶ transmit fingerprints to IAFIS via telephone line or BGAN ▶ fetch IAFIS response</td>
</tr>
<tr>
<td>Match against a watchlist</td>
<td>Identify suspect or informant ▶ take fingerprint slaps using MOBS (SEEK ID or Toughbook with Guardian R2) ▶ MOBS will inform whether individual is on the device’s watchlist</td>
</tr>
<tr>
<td>Transfer enrollment to LiveScan device</td>
<td>Find EFT file in MOBS ▶ copy files onto thumb drive ▶ download files into LiveScan machines ▶ downloaded files may be stored and transmitted to IAFIS when conditions for transmission are met</td>
</tr>
</tbody>
</table>
| Add records into watchlist      | 1. Capture full enrollment ▶ confirm record is automatically enrolled into device watchlist  
2. Download watchlist into MOBS using download EFT files, download EFT folders, or download watchlist (record templates rather than EFT files) |

* Mission Oriented Biometrics Software, Cross Match’s biometrics processing software application
Observations from the pilot to date identified some strengths and weaknesses of the equipment

- **SEEK**
  - Well received by agents for its size and ease of use
  - Encountered problems in direct sunlight
    - Sun glare off of monitor
    - Direct light into fingerprinting prism causes problems with capturing fingerprints

- **Guardian R2**
  - Less liked compared to SEEK due to size and lack of convenient carrying case for device and Toughbook computer

- **MOBS & Watchlist**
  - Software easy to use
  - Would like the ability to save a transaction and come back to it and edit
  - Like the idea of the watchlist, but critical information (like arrest history) was missing

- **BGAN**
  - Difficult to use
  - Surrounding buildings, ships, and trees impede signal
Agenda

- Overview of NCIS
- NCIS’s need for mobile biometrics equipment
- Conducting a pre-deployment pilot
- Conclusion
NCIS’s mobile biometrics pilot provides insights into deploying an effective solution by

- Getting stakeholder buy-in on the usefulness of mobile biometric devices
- Identifying the right mobile device solution(s) for deployment
- Providing a basis for
  - Determining tools, processes, and people infrastructure needed
  - Estimating infrastructure procurement and sustainment costs
- Pushing for improvements to the biometric system architecture
In the future, NCIS is plans to leverage a more robust biometrics architecture being developed by the Biometrics Task Force in West Virginia (BTF West)
Questions