Welcome

- Barbara Guttman
  - Director, Information Access Division
Looking back... some factoids:

- It was a long road to the BPR...
  - APB request announced on 08/06/2007
  - The BPR published on 08/21/2009 (746 days)
- The final comment disposition spreadsheet was 49 pages long (the BPR itself was 55 pages long).
- In 2009, there was only a handful of devices that were ready for market.
But... it's been over 5 years since publication, and much has changed.

- A mid-range desktop in 2008 could execute 10 BIPS... A smartphone last year hit 18 BIPS.
- Sensors technology has improved (1000ppi fingerprints, megapixel resolution for even the most basic cameras devices)
- Data transmission systems have radically transformed (LTE, 802.11, 802.16, Bluetooth)
We’ve come a long way... Lots of devices... FBI-NGI-RISC is in full swing... Lots of new interest...
IN CLOSING

- The time is right for an update.
- Good to see continued interest and support from everyone!
- Glad to have you here for the next evolution in Mobile ID!

Shahram Orandi
sorandi@nist.gov
NEED FOR AN UPDATE

- BPR originally published in 2009
- ANSI/NIST-ITL standard has incorporated the Acquisition Profiles, and they should be maintained in only one document
- New modalities have matured for biometric and forensic use in a mobile environment
- Referenced Standards have been updated and new ones developed
- Use cases have been further defined
- A mobile ID taxonomy has been developed
- New technology has been developed
Based on input from our member organizations, IBIA is respectfully requesting that the National Institute of Standards and Technology (NIST) consider convening a working group to discuss and review potential updates to NIST Special Publication 500-280 *Mobile ID Device Best Practice Recommendation Version 1.0* (hereafter, Mobile ID BPR), which was published in July 2009. This publication is an important reference document for implementers and suppliers of mobile devices that incorporate biometric technology and is often cited in procurement documents and is used by suppliers in developing product specifications. A number of later documents and standards, such as ANSI/NIST-ITL 1-2011 (NIST Special Publication 500-290), reference the Mobile ID BPR document extensively. However, we believe that some references in the Mobile ID BPR document may be outdated and should be refreshed.
The BPR is a NIST Special Publication, not part of the ANSI/NIST-ITL standard

We will set up working groups to develop text for the new document

Much of the document structure will be changed, since the Acquisition Profiles are now in the ANSI/NIST-ITL standard

Drafts will be circulated for comment

There will be a poll of interested parties to determine if the draft is acceptable prior to putting through the NIST publication procedure.
FORMAT OF THE MEETING

- Presentations in limited time slots
  - Questions if there is enough time left in the slot
- Group Discussion in the afternoon

Think about these questions during the day:
- What do we want to consider as ‘mobile’ in the BPR (wearable -- transportable - luggable --mixed ?)
- What modalities do we want to address?
- Should we include SOPs? Privacy issues? Etc. or just ‘technical’ aspects?
- Which areas are you willing to chair?
- Is there anything else that occurs to you as important?
USE CASE SCENARIOS
MOBILE BPR USES?

- Referencing the Mobile BPR in RFI’s, RFPs, BAAs . . .
  - Law Enforcement/Military Profiles make it easy

- We have an opportunity to tune the next version to suite our needs
  - Documentation tool for needs and requirements
  - Use cases/scenarios already spelled out
  - Mobile device characteristics in tabular form
  - Guidance on Standards and Best Practices
Forensics
- Latent finger printing on site at crime scenes
- Finger printing deceased persons

Access control
- To the mobile device itself, facility/area, obtaining services . . .
- One sentence in section 11.3.1 on Operator Authentication

BOLOs
- Ability to receive pictures and criminal history in the field on a mobile device
During a traffic stop, an unknown suspect pulled out a firearm and aimed it towards Officer Pierce.

Officer Pierce fired his duty weapon toward the suspect.

The suspect fled on foot with a weapon.

Weapon was located in a nearby back yard.

Field Technician was called out to collect and run latent prints with Fusion at the site. Seventeen prints found to be medium to high quality were submitted and resulted in AFIS hits. An arrest was made.
FORENSICS (LATENT PRINTS)

Fusion Image

Hit Right Thumb

Suspect
## Forensics (Latent Prints)

**Latent Lift #7B - From Interior Rearview Mirror**

### With Black Powder

<table>
<thead>
<tr>
<th>Fusion #187</th>
<th>Lab Auto</th>
<th>Lab Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>1290</td>
<td>1493</td>
<td>1020</td>
</tr>
<tr>
<td>1083</td>
<td>1236</td>
<td>911</td>
</tr>
<tr>
<td>860</td>
<td>919</td>
<td>883</td>
</tr>
<tr>
<td>849</td>
<td>907</td>
<td>841</td>
</tr>
<tr>
<td>842</td>
<td>902</td>
<td>840</td>
</tr>
<tr>
<td>839</td>
<td>875</td>
<td>840</td>
</tr>
<tr>
<td>826</td>
<td>865</td>
<td>804</td>
</tr>
<tr>
<td>826</td>
<td>857</td>
<td>801</td>
</tr>
<tr>
<td>822</td>
<td>854</td>
<td>794</td>
</tr>
<tr>
<td></td>
<td>846</td>
<td>786</td>
</tr>
</tbody>
</table>

**Identified:**

Workstation

**Lights Out**

- Lifted
- Not Lifted
**Acquisition planning tool for operational end users (currently Appendix B)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Law Enforcement</th>
<th>Military</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Data Collection (image sensor capabilities)</td>
<td>flat fingerprints (FAP 10) facial image (SAP 32)</td>
<td>FAP 45 or above SAP 42 or above</td>
</tr>
<tr>
<td>Durability / Ruggedness</td>
<td>Ingress Protection Rating: IP65 Must survive multiple drops at 36 inches</td>
<td></td>
</tr>
<tr>
<td>Mobility</td>
<td>Field Use and Office Use</td>
<td>Vehicle Use (mounting and charging)</td>
</tr>
<tr>
<td>Communications</td>
<td>3G cellular 802.11 (WiFi) Ethernet LAN (RJ-45 connection, for office use)</td>
<td>4G LTE cellular USB 2.0</td>
</tr>
<tr>
<td>Inputs</td>
<td>Touchscreen</td>
<td>Physical keyboard peripheral (for office use)</td>
</tr>
<tr>
<td>OS</td>
<td>Windows 7</td>
<td>Windows 8</td>
</tr>
<tr>
<td>Data Formatting Output(s)</td>
<td>DHS OBIM IXM 6.0</td>
<td>DOJ FBI EBTS 9.3</td>
</tr>
<tr>
<td>Subject Record (data) Storage</td>
<td>200 subject records (storing images, not templates)</td>
<td>DOD DFBA EBTS 3.0</td>
</tr>
<tr>
<td>Security</td>
<td>Adherence to DHS 4300A and FBI CJIS Mobile Security policies Data “at rest”, “in use” is protected and secured</td>
<td></td>
</tr>
<tr>
<td>Screen Size (inches, diagonal)</td>
<td>Greater than 6 in</td>
<td>Less than 12 in</td>
</tr>
<tr>
<td>Dimensions (inches)</td>
<td>Less than 12x10x1.25</td>
<td>Less than 12x10x0.75</td>
</tr>
<tr>
<td>Weight (pounds) (includes platform + accessory)</td>
<td>Less than 3 lbs</td>
<td>Less than 2 lbs</td>
</tr>
</tbody>
</table>

**OPTIONAL Reqs**

- Card Reader: FIPS-201-1 (e.g. PIV, PIV-I, CAC)
- Biometric Data Collection: IAP 20 or above [OPTIONAL]
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Road Stop</th>
<th>Latent Printing</th>
<th>Deceased</th>
<th>Check in/out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Data Collection (image sensor capabilities)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Durability / Ruggedness</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Mobility</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lighting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject Record (data) Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Docking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Size (inches, diagonal) (includes platform + accessory)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions (inches) (includes platform + accessory)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight (pounds) (includes platform + accessory)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIV/CAC Card Reader</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Data Collection (Iris and/or latent fingerprint image sensor capabilities)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
USE CASES AND SCENARIOS

Rick Lazarick
Chief Czar Scientist - Biometrics
DHD S&T Support Contractor
Computer Sciences Corporation

Homeland Security
Science and Technology
“Use Cases” and “Scenarios”

- Based on 2 sources:
  - NIST Mobile ID BPRS (2009)
  - DHS S&T MBHD (Mobile Biometric Handheld Device) (2011)

- Note reversal of terms
Figure 1 - Tasks Across 4 Basic Scenarios

(a) (standalone)
- Data Capture
- Signal Processing
- Matching
- Decision

(b)
- Data Capture
- Signal Processing
- Matching
- Network
- Decision

(c)
- Data Capture
- Signal Processing
- Network
- Matching
- Decision

(d)
- Data Capture
- Network
- Signal Processing
- Matching
- Decision
# MBHD "USE CASES"

<table>
<thead>
<tr>
<th>Use Case</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Document Identity Verification</td>
<td>On-board AFIS</td>
<td>Standalone Terminal with Data Query Capability</td>
<td>Remote Server (CMS) Dependent Terminal with Data Query Capability</td>
</tr>
<tr>
<td>Function(s)</td>
<td>Verification</td>
<td>Enrollment, Identification, Verification</td>
<td>Enrollment, Identification, Verification</td>
<td>Enrollment, Identification, Verification</td>
</tr>
</tbody>
</table>

### MBHD
- Document reader
- Biometric capture
- Biometric quality check
- Matcher
- Display images
- Display text response

### MBHD
- Text entry and edit
- Biometric capture
- Biometric quality check
- Display images
- Matcher
- Text response
- Local database
- Data formatting
- Disposition/decision
- Administrative
- Security

### MBHD
- Document reader
- Text edit and entry
- Biometric capture
- Biometric quality check
- Display images
- Select target data system
- Text response
- Data formatting
- Disposition/decision
- Administrative
- Security

### MBHD
- Document reader
- Text edit and entry
- Biometric capture
- Biometric quality check
- Display images
- Select target data system
- Text response
- Data formatting
- Disposition/decision
- Administrative
- Security
- Connectivity

### Bluetooth/WiFi
- Biometric quality check
- Data formatting
- Manage connectivity
- Logging

### Local Server (Patrol Car PC)
- Biometric quality check
- Data formatting
- Manage connectivity
- Logging

### Network
- Biometric Searches
- Name or Subject ID# Queries

### AFIS (ABIS)

### NCIC/CCH
## MOBILE ID BPRS “USE CASES”

Table 6 - Use cases for risks and functions

<table>
<thead>
<tr>
<th>Risk to Public Safety/Function</th>
<th>Use Case Example</th>
<th>SAP Level</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Severe/Enrollment             | Field enrollment into databases with applications where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric enrollment. Enrollment should achieve an equivalent level of quality as if conducted in a controlled environment using non-mobile devices. | 42 45+    | Recommend Capture:  
  - Iris = L&R  
  - Finger = 10  
  Enrolling all ten fingerprints, multiple views faces including full-face with three to five profiles, both irises, and multiple instances (captures) of each biometric provides additional search capabilities.  
  Note for face enrollments, attempts should be made to control, background expression and lighting where it is practical to do so. |
| Severe/Identification         | One to many search against a database to identify a subject where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric identification.                        | 42 45+    | Recommend Capture:  
  - Iris = L&R eyes  
  - Finger = 4+  
  Note for face identifications, attempts should be made to control, background expression and lighting where it is practical to do so. |
| Severe/Verification           | 1:1 match against a credential or database to verify identity where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric verification.                               | 32+ 20+  42 | Recommend Capture:  
  - Iris = Either eye  
  - Finger = 2+  
  Note for face verifications, attempts should be made to control, background expression and lighting where it is practical to do so. |
<table>
<thead>
<tr>
<th>Use Case Category</th>
<th>Description</th>
<th>Min Score</th>
<th>Min Sample Size</th>
<th>Min Enrollments</th>
<th>Recommendation for Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Moderate/Enrollment</strong></td>
<td>Mobile booking: Field cite and release when the violation is not high enough to ensure incarceration until arraignment without bail.</td>
<td>42</td>
<td>40+</td>
<td>32</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = L&amp;R eyes</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = L&amp;R eyes</td>
</tr>
<tr>
<td></td>
<td>• Finger = 6+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 6+</td>
</tr>
<tr>
<td></td>
<td>Note for face enrollments and identifications, ideal lighting conditions should be used. Otherwise, fingerprints or irises should additionally be used.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Moderate/Identification</strong></td>
<td>In field mobile identification of a subject with questionable or no identification.</td>
<td>42</td>
<td>30+</td>
<td>32</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = Either eye</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = Either eye</td>
</tr>
<tr>
<td></td>
<td>• Finger = 4+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 4+</td>
</tr>
<tr>
<td><strong>Moderate/Verification</strong></td>
<td>Personal Identity Verification (PIV) Release from custody.</td>
<td>32+</td>
<td>20+</td>
<td>32</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = Either eye</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = Either eye</td>
</tr>
<tr>
<td></td>
<td>• Finger = 2+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 2+</td>
</tr>
<tr>
<td><strong>Mild/Enrollment</strong></td>
<td>The intention is for the biometric enrolment to be of sufficient quality that it shall allow later verification (e.g. e-citations).</td>
<td>32</td>
<td>30+</td>
<td>22</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = L&amp;R eye</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = L&amp;R eye</td>
</tr>
<tr>
<td></td>
<td>• Finger = 4+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 4+</td>
</tr>
<tr>
<td><strong>Mild/Identification</strong></td>
<td>Rapid identification in custody prior to formal booking. (Typically done at the Jail Intake.)</td>
<td>32</td>
<td>10+</td>
<td>22</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = Either eye</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = Either eye</td>
</tr>
<tr>
<td></td>
<td>• Finger = 2+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 2+</td>
</tr>
<tr>
<td><strong>Mild/Verification (finger images)</strong></td>
<td>Court Appearance/Parole/Workhouse, Personal Identity Verification (PIV).</td>
<td>22+</td>
<td>10+</td>
<td>22</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Iris = Either eye</td>
<td></td>
<td></td>
<td></td>
<td>• Iris = Either eye</td>
</tr>
<tr>
<td></td>
<td>• Finger = 1+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 1+</td>
</tr>
<tr>
<td><strong>Mild/Verification (finger minutiae)</strong></td>
<td>Personal Identity Verification (PIV) (using minutiae).</td>
<td>N/A</td>
<td>5+</td>
<td>N/A</td>
<td>Recommend Capture:</td>
</tr>
<tr>
<td></td>
<td>• Finger = 2+</td>
<td></td>
<td></td>
<td></td>
<td>• Finger = 2+</td>
</tr>
<tr>
<td></td>
<td>Not recommended for use between AFIS.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Scenarios

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>Use Case 0</th>
<th>Use Case 1</th>
<th>Use Case 2</th>
<th>Use Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Law Enforcement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Patrol Activities - Variation A (fingerprint)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Law Enforcement Patrol Activities - Variation B (face/iris)</td>
<td></td>
<td>O</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Law Enforcement Public Event Disturbance</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Border Protection</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POE Identity Verification (Document Check)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>POE Identity Verification (US-VISIT) (Identity Check)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>POE Identification and Verification (US-VISIT)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Maritime</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coast Guard Interdiction</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Maritime Interdiction Operation (DSB Task Force, 2007)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>First Responders &amp; Emergency Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Site Operations</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DHS First Responders Access Control</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Applications of TWIC</td>
<td>X</td>
<td></td>
<td>O</td>
<td></td>
</tr>
<tr>
<td><strong>Immigration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citizenship Application Processing</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Scenario Based on United States Border Patrol</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospital Scenario</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Identification of Deceased</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Checkpoint Operations</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Joint Operation</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Scenario TRADOC</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hold, detain, release decisions regarding suspects</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Identification of local nationals for base access</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Scenario Stockton Police Department</strong></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Field Capture Latent Pilot</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Patrol Mobile Identifications</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>County jail house booking, transfer, and release</td>
<td></td>
<td>O</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
WAY FORWARD

- Define our terms and stick with them
- Early agreement on configurations
- Start with collection of detailed descriptions
MOBILE VOICE APPLICATIONS

- Presentation not authorized for distribution
FBI CODIS AND RAPID DNA

- RapidDNA capabilities have been developed and machines deployed around the world.
- Some have the capability to export data using ANSI/NIST-ITL 1-2011 format.
- FBI/CODIS is not now accepting ANSI/NIST_ITL format.
- DHS is testing RapidDNA units in a field environment but not linking to CODIS.
CODIS DNA Data Exchange Standards

Kevin M. Ellis
Requirements Manager, CODIS Unit
FBI Laboratory
October 31, 2014
CODIS currently uses an XML file format for adding and modifying specimens in the CODIS database.

Common Message Format (CMF 3.2) is used to add specimens with STR and Y-STR loci.

CMF 3.2 was released in July 2003.

This format is used by commercial vendors that do not use CODIS, but need to provide DNA profiles to CODIS laboratories.
An example of an Import CMF 3.2 file results follows:

```xml
<?xml version="1.0" encoding="utf-8"?>
<CODISImportFile xmlns="urn:CODISImportFile-schema">
  <HEADERVERSION>3.2</HEADERVERSION>
  <MESSAGETYPE>Import</MESSAGETYPE>
  <DESTINATIONORI>TXDPS6900</DESTINATIONORI>
  <SOURCELAB>TXDPS6900</SOURCELAB>
  <SUBMITBYUSERID>Kevin.Ellis</SUBMITBYUSERID>
  <SUBMITDATETIME>2014-09-10T00:01:00</SUBMITDATETIME>
  <BATCHID>GFE12345</BATCHID>
  <KIT>GlobalFiler Express</KIT>
  <SPECIMEN SOURCEID="N/A">
    <SPECIMENID>ARRESTEE_01</SPECIMENID>
    <SPECIMENCATEGORY>Arrestee</SPECIMENCATEGORY>
  </SPECIMEN>
  <LOCUS>
    <LOCUSNAME>CSF1PO</LOCUSNAME>
    <READINGBY>Kevin.Ellis</READINGBY>
    <READINGDATETIME>2014-08-22T19:56:00</READINGDATETIME>
    <ALLELE>
      <ALLELEVALUE>11</ALLELEVALUE>
    </ALLELE>
  </LOCUS>
</CODISImportFile>
```
A new Rapid CMF interface specification is being developed to support the possible integration of Rapid DNA instruments with CODIS.

Discussion is occurring with Local, State and Federal law enforcement agencies to determine how law enforcement agencies (not on CJIS WAN) can communicate with CODIS.

Future DNA message exchanges may use the ANSI/NIST-ITL Type-18 format.

The FBI Laboratory Division is working with the CJIS Division to create messaging standards for Rapid DNA integration.
Goals of FBI Rapid DNA Initiative

- Rapid DNA is being designed for use in the law enforcement booking process to analyze DNA in near real-time.

- Produce CODIS-compatible DNA profiles from arrestee reference samples in the booking station environment.

- Use the existing CODIS structure to search a DNA database to determine if the arrestee is linked to an unsolved crime while the individual is still in police custody.

Unclassified for Official Use Only
Draft Rapid DNA Message Flow

Enrollment of Known DNA from Arrest Event

State AFIS/State CSA

1. SD

2. UCN

State WAN

Booking Agency

Hillsborough County Florida Sheriff’s Office

3. Specimen Enrollment Request

4. UveScan

5. Fingerprints

CODIS RE DNA

Portal GFE Software

CODIS SDIS

6. Rapid DNA Instrument

7. Rapid Hit Notification (RHN)

Unsolicited DNA Notification (UDN)

8a. Booking Agency

Hillsborough County Florida Sheriff’s Office

8b. Arreting Agency

Tallahassee, Florida

8c. State CJIS Systems Agency (CSA)

State CJIS Systems Agency (CSA)

CODIS LDIS

Orlando, Florida

CODIS Lab

Rapid Integration of Unknown DNA from an Investigation

Note: The forensic specimen was rapidly enabled following “no hit” at LDIS, SDIS and NDIS. Rapidly enabled hits only occur with arrestee DNA being processed at a booking station.

Investigative Agency

City of Orlando Police Department

Request to Rapidly Enable a Forensic Specimen from a Crime of Special Concern.

Investigative Agency

City of Orlando Police Department
Thank You

Kevin M. Ellis
CODIS Unit
703-216-2852
Kevin.Ellis2@ic.fbi.gov
MOBILE DEVICE USABILITY FOR BIOMETRIC ACQUISITION

Kristen K. Greene
NIST Visualization and Usability Group
Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.
OUTLINE

- Usability
- Mobile device constraints
- WSABI (Web Services for Acquiring Biometric Information)
- Designing for touch and gesture
USABILITY MATTERS

- It matters A LOT
- Better usability = faster task completion times, fewer errors
- Better usability = less training
Usability is defined (ISO 9241, 1998) as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."
**USABILITY: ISO 9241**

- **Effectiveness**: Accuracy and completeness with which users achieve specified goals.
- **Efficiency**: Resources expended in relation to the accuracy and completeness with which users achieve goals.
- **Satisfaction**: Freedom from discomfort, and positive attitudes towards the use of the product.
- **Context of use**: Users, tasks, equipment (hardware, software and materials), and the physical and social environments in which a product is used.
Smaller devices = BIGGER usability problems
Smaller buttons and keys
- Onscreen keyboards
Lack of tactile feedback
Icon sizing and spacing
Can’t port directly from desktop to mobile
**Onscreen Keyboards**

- Sizes vary *between* mobile devices
  - Based on physical differences in maximum available touchscreen real estate
- Sizes vary *within* a single device
  - Depending on device orientation (landscape versus portrait mode)
  - “splitting” the keyboard, which changes the relative distance between some keys more so than others
Web Services for Acquiring Biometric Information

Touchscreen interface for multimodal biometric capture

Has undergone formal usability testing

https://github.com/NIST-BWS/wsabi2

http://dx.doi.org/10.6028/NIST.IR.8003

Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture
Consistency is key
Regardless of the biometric modality or sensor, users perform same actions to capture, annotate, clear, and retake biometric data
Same method of sensor setup regardless of biometric modality or sensor
### Finger sensor

<table>
<thead>
<tr>
<th>Network Address</th>
<th>test.me/finger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Finger sensor</td>
</tr>
</tbody>
</table>

### New Sensor

- **Found a sensor at this address.**

<table>
<thead>
<tr>
<th>Network Address</th>
<th>test.me/finger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Fingerprint Sensor</td>
</tr>
</tbody>
</table>
Design biometric acquisition software to be user- rather than sensor-centric
- Keep the core capture primitives constant
- Be consistent
- Use internationally tested, standardized symbols where possible
- Be aware of differences between desktop and mobile computing paradigms
**QUESTIONS?**

- [Hyperlink](http://dx.doi.org/10.6028/NIST.IR.8003)
  - Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture

- kgreene@nist.gov
- bws.nist.gov
Remote Subject Identification
- 1:N based on iris only
- 1:N multimodal
- Tablet device (peripheral or built-in camera)

Detainee Management
- 1:1 based on iris only
- Tablet device, multiple use cases
  - Verify identity before transfer of custody
  - Verify deportation at point of departure
  - Track detainee movement using iris
GIU Biometric Tools Initiative

• MISSION: to give FBI users the tools to access the biometric identification power of the US Government in real time at any point on the planet in support of operations.

• VISION: to be the premier United States government provider of mobile identification solutions by delivering 1) the best tools, 2) and the most data, 3) with the fastest speed, 4) to the most locations, 5) for the greatest operational impact.
QCP - Components

- **Current**
  - Quick Capture Platform: backpack (laptop, scanner, battery, camera)

  - Panasonic Toughbook Laptop
  - Air card (Not in all kits)
  - BGAN Satellite (Not in all kits)
  - Fingerprint Scanner
Basic messaging model

- End user
- Create transaction through application
- Open communication path
- Open transaction manager
- Transmit transaction to CJIS

- Response sent back to the transaction manager
- Notification can be viewed on the device
BCIP Software

Fingerprint
Mark the missing fingers

Amputated
Unable To Print
Healthy

Missing Capture

Start
Transaction manager (Possible Rap Sheet)

Rapsheet

This record is being sent for identification purposes only. It does not convey the individual’s immigration status and is not an immigration detainer.

Statement on Disclosure of Visa Records

According to the Immigration and Nationality Act, section 222(f). The records of the Department of State and of diplomatic and consular offices of the United States pertaining to the issuance or refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States.
Mobile Device

- Laptop (Current)
  - Size (footprint): Large
  - Weight: Heavy
    - ~5 lbs

- Tablet (Interim)
  - Size (footprint): Medium
  - Weight: Light
    - ~1 lbs

- Phone (Future)
  - Size (footprint): Small
  - Weight: Light
    - ~5 ounces
Mobile - Capabilities

Laptop
Primary Capabilities
• Fingerprint
• Face
• Iris
Future Capabilities
• Voice
• ...

Smartphone/Tablet
Primary Capabilities
• Fingerprint
Future Capabilities
• Face
• Iris
• Voice
• ...
Future Communication Path

Start/End QCP transaction

Send/Receive transactions to CIIS

VPN or Other protocol

Authentication

Client Remediation
- Virus Definition
- DS updates
- Third party software updates

Software inspection

DMZ

YES/NO

Mobile Device Management (MDM)

CIIS infrastructure

Legend:
- Decision
- Manual query
- Process
- Premade process
- End
Transmission

• Desktop/Laptop (Current)
  – Software
    • EBTS compliant (ebts files)
  – Communication
    • Air/Satellite
    • VPN – Cisco AnyConnect

• Mobile (Future)
  – Software
    • EBTS Compliant (ebts files)
  – Communication
    • Cellular, ....???
    • VPN, Web Service, ....???
Scenarios

**Scenario 1**
- A SWAT Agent is going into a house with a potential suspect. The area the house is located has optimal cellular communication for laptop to be set up or mobile device.

**Scenario 2**
- A CAC Agent is conducting a prostitution sting operation in a hotel in a major city. Cellular communication for laptops and mobile phones will either be good or bad depending on the buildings and the city.
Scenarios

- **Scenario 3**
  - An VC agent is going to be traveling to a remote dessert location in New Mexico where an unidentified person of interest has been located. Cellular communication is spotty, at best.

- **Scenario 4**
  - A CTD agent is going to a foreign country for an operation. Cellular connectivity is very low to nonexistent.
Scenarios

- **Scenario 5**
  - An team of NYC agents are conducting a mass arrest. Cellular communication is typically good depending on the building material and location.

- **Scenario 6**
  - A natural disaster occurs, i.e. Hurricane Katrina. Cellular connectivity can be very low to nonexistent. Agents conduct fingerprinting on the bodily remains to help identify individuals.
Questions?

Peter Alex
Global Initiatives Unit
304-625-5019
Peter.Alex@ic.fbi.gov
Specific hardware and software products identified in this report were used in order to perform the evaluations described. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.
ISO/IEC SC 37 24779

Information Technology - Pictograms, Icons and Symbols for Use with Biometric Systems Has 4 Active Parts

- Part 1: General
- Part 4: Fingerprint
- Part 5: Face
- Part 9: Vascular
General guidance for use with all biometric systems/modalities:

- Move forward
- Move backward
- Move left
- Move right
- Failure
- Success
- Retry
- Seek Assistance
PART 4: FINGERPRINT APPLICATIONS - EXAMPLE SYMBOLS

General guidance
- General overlay guide for slap

Hand positioning corrections:
- Move forward - thumb;
Also have animated symbols

Move your fingers up
Symbols Include:

- Facial Image Capture
- Look at a point
- No Hats
- No glasses
- Move hair away from face
Symbols Include:
- Vascular Image Recognition
- Hand Vascular Image
- Finger Vascular Image
ISO 9241-210 Human Centered Design for Interactive Systems

- 2506n Field Data Report
  - ISO/IEC 25062 CIF for Usability Test Reports
- 25063 Context of Use Description
  - ISO/IEC 15288 6.4.1 Stakeholders Requirements Definition Process
- 25064 User Needs Report
  - ISO/IEC 15288 6.4.1 Stakeholders Requirements Definition Process
- Evaluation
  - ISO/IEC 15288 6.4.6 Verification Process
- Users
  - ISO/IEC 15288 6.4.3 Architectural Design Process
- User & Organizational Requirements
  - ISO/IEC 15288 6.4.2 Requirements Analysis Process
- Design Solution
  - ISO/IEC 15288 6.4.4 Implementation Process
- 25065 User Requirements Specification
  - 2506n User Interaction Specification
  - 2506n User Interface Specification
CONTACT INFORMATION

Mary Theofanos
National Institute of Standards and Technology
maryt@nist.gov

Acknowledge: Department of Homeland Security Science and Technology Directorate for their support of this research
NETWORK & COMMUNICATION CONSIDERATIONS FOR DIFFERENT MOBILE ARCHITECTURES

Ross J. Micheals
NIST
Mobile Best Practices Update Workshop
30 Oct 2014
BPR recognizes that different components may be separated by a network.
• Generalize the “network” to an interoperability point; crossing a logical or physical boundary
• Multiple interop points (e.g. networks) are not just possible, but likely
EXAMPLE ARCHITECTURES

- Consider two components
  - sensors: (data capture and signal processing)
  - matchers: (matching and decision)
- Different ways they might be ‘componentized’
- Illustrative and intended to stimulate discussion; not authoritative or a comprehensive treatment of all possible architectures
**SENSOR—ALL EMBEDDED**

- Most flexible with respect to interoperability points
- Explicit interoperability points may not be present; if they are, they would not require traversing a physical network
- Component communications could happen in within the same process or though a variety of interprocess communications
- Easier to make decisions that resist changes later
- Network traversal as client device requests capture and gets results
- Degree of signal processing may vary (e.g., does a template or an image come back?)
- (Typically) wireless communication might be Bluetooth, NFC, WiFi, or proprietary; *suggestion: make wired backup a best practice*
- Physical and logical integration is a sliding scale, (e.g. an intelligent ‘sleeve’)
Sensor—Client Device to Tethered Sensor

- Ability to leverage a great deal of computational and communications capabilities
- Network: Wireless/wifi (with Ethernet backup?)
- Enables the use of the widest variety of sensors with mobile devices:
  - Legacy
  - Luggable (e.g., DNA)
  - Fixed location (e.g., high resolution palm)
Matcher—No Matcher

- Different scenarios may use a matcher at different stages during their usage
  - Data input preparation for a deployment
  - Offline matching
  - Research & development
- Systems supporting these must be designed to accommodate stages in which a matcher may not be ‘online’
Matcher—Local Matcher

- Matcher lives “inside” device; i.e., local ‘watch list’ with persons of interest;
- Similar to fully integrated client device
  - Most flexible with respect to interoperability points
  - Explicit interoperability points may not be present; if they are, they would not require traversing a physical network
  - Component communications could happen in process or though a variety of interposes communications
  - Easier to make decisions that resist changes later
Matcher—Remote

- Different scenarios may require different payloads
- Scenario/deployment
  - Centralized station specific to an incident response (ad hoc server)
  - Proprietary or “local” data formats may be okay
- Large-scale matcher
  - Cellular or satellite communications
  - Formal, “curated” formats (think EBTS, ANSI/NIST)
- Branch office
  - Matcher specific to a municipality;
  - Wifi or law enforcement-dedicated communications network
  - Could be a hybrid of custom and curated formats
WEB SERVICES

- Can be applied across a diverse set of architectures (even the all embedded)
  - Use the protocols that underlie the web for machine-to-machine communications
    - Evolution of existing practice (e.g., SMTP for IAFIS)
    - Nearly universal; COTS friendly
    - Well tested
OPEN BIOMETRIC WEB SERVICE SPECIFICATIONS

- OASIS Biometrics TC
  http://tinyurl.com/biometricstc
- Biometric Identity Assurance Services (BIAS)
  - biometric operations (enroll, verify, identify)
  - OASIS Standard SOAP Profile; based on INCITS 442:2010
- WS-Biometric Devices
  - command and control of a biometric sensor
  - OASIS Biometrics TC: Committee Specification Draft
QUESTIONS?

rossm@nist.gov
http://bws.nist.gov
http://tinyurl.com/biometricstc
OTHER ISSUES TO CONSIDER
Removing Glasses: Impact on Facial Recognition

- Slides presented separately
Repository for Individuals of Special Concern (RISC) Pilot 2007
RISC Deployment 2014

+ U.S. Marshals Service
+ Railroad Police
RISC Stats

Over 1.3 Million Transactions Processed

- **Average Daily Submissions**
  - 1,605 (Peak 3,082)

- **Average Response Time**
  - 4.71 seconds

- **Average “Hit” Rate**
  - 4.16%

  **Yellow Responses** = 0.39%
  - Yellows to “Red” = 72.5%

- **Reject Responses** = 0.14%
NIST Study

As a result of a CJIS Advisory Policy Board (APB) request, an independent study was conducted to examine the impact of Fingerprint Acquisition Profiles (FAPs) on the accuracy of RISC.

In March 2014 the National Institute of Standards and Technology (NIST) completed a study titled:

**NISTIR 7950**

*Examination of the Impact of Fingerprint Spatial Area Loss on Matcher Performance in Various Mobile Identification Scenarios*
NIST Study

RISC Testing / Summary

- FPIR “False Positive” performance between FAP10 & FAP30 on the NGI RISC matcher appears to not be impacted significantly.

- FNIR “False Negative” performance between FAP10 & FAP30 is significant for #2 and #7 two finger submissions
  - 3.272% @FAP10
  - 1.844% @FAP20
  - 1.616% @FAP30

- If you must keep your FAP10 device, you may be able to get near-FAP30 performance by using FAP10 with 4 fingers (#2, #3, #7, #8 with FNIR of 1.714%) but sequencing errors may cause other headaches.

- EBTS- Study Results will be highlighted in a TOU and the document will be referenced in EBTS
FAP 10 and FAP 30

- CJIS “highly recommends” agencies deploying mobile ID devices searching RISC to procure FAP 30 or higher devices.
  - If agencies want to meet the RISC accuracy rate and submit only two fingerprint images, a FAP 30 device is optimal.
  - Agencies continuing to submit only two fingerprint images with FAP 10 devices may accept some risk.
Questions?

David L. Jones
Lead Analyst
david.jones3@ic.fbi.gov
304-625-4850
# Adding a New FAP 55 Code for 3.2” x 2.0” in Mobile Platforms

<table>
<thead>
<tr>
<th>Capture&lt;sup&gt;1&lt;/sup&gt;</th>
<th>5</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>45</th>
<th>50</th>
<th>60</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquire flat images</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Acquire rolled images</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>Minimum resolution</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td>500 ppi ± 5 ppi</td>
</tr>
<tr>
<td>Minimum Gray levels</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Minimum Image Dimensions (w/h)</td>
<td>.5” x .65”</td>
<td>.5” x .65”</td>
<td>.6” x .8”</td>
<td>1.6” x 1.5”</td>
<td>1.6” x 1.5”</td>
<td>2.5” x 3”</td>
<td>3.2” x 3”</td>
<td>3.2” x 2”</td>
<td></td>
</tr>
<tr>
<td>Minimum image area</td>
<td>.325 sq in</td>
<td>.325 sq in</td>
<td>.48 sq in</td>
<td>2.4 sq in</td>
<td>2.4 sq in</td>
<td>3.75 sq in</td>
<td>9.6 sq in</td>
<td>6.4 sq in</td>
<td></td>
</tr>
<tr>
<td>Compression algorithm&lt;sup&gt;3&lt;/sup&gt;</td>
<td>N/A</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
</tr>
<tr>
<td>Maximum compression ratio</td>
<td>N/A</td>
<td>10:1</td>
<td>10:1</td>
<td>15:1</td>
<td>15:1</td>
<td>15:1</td>
<td>15:1</td>
<td>15:1</td>
<td>15:1</td>
</tr>
<tr>
<td>Simultaneous number of fingers</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1 to 2</td>
<td>1 to 2</td>
<td>1 to 3</td>
<td>1 to 4</td>
<td>1 to 4</td>
</tr>
<tr>
<td>Sensor certification</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>Appendix F</td>
<td>Appendix F</td>
<td>Appendix F</td>
<td>Appendix F</td>
</tr>
<tr>
<td>Minutiae extractor certification</td>
<td>PIV</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## Interchange

<table>
<thead>
<tr>
<th>Image / template</th>
<th>Minutiae</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard used</td>
<td>INCITS 378-2004</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
</tr>
</tbody>
</table>
FAP45 (two finger) sensors OK for ABIS field enrollment

FAP45 not accepted by FBI/CJIS/Police for field booking.

Need for mobile field enrollment is growing in US and international

LES (film/TFT based) FAP55 sensor can take shape compatible with cell phone size and thickness goals.

FAP55 (3.2” x 2”) size meets “type 4” enrollment standard suitable for field booking (10print rolls)
ANSI/NIST-ITL has been updated to include new modalities that may be useful in mobile applications:
- Voice
- DNA

The Acquisition Profiles of the first BPR have been incorporated into the standard for face, fingerprint and iris.

Updated data acquisition and data storage requirements and data transmission fields should be reflected in the new BPR.
Based on DHS S&T Mobile Biometric Handheld Device (MBHD) Testing & Evaluation (2010-12)

Work was sponsored by DHS S&T HSARPA Resilient Systems Division (RSD)

Scope included:
- Scenario & Use Case Analysis
- Requirements Development
- Test Framework Development
MBHD TAXONOMY

- Structural decomposition that provides a defined way to depict a mobile biometric handheld device into 5 subsystems
  - Each subsystem consists of components
    - Hardware
    - Software
MBHD Taxonomy

Mobile Biometric Handheld Device

System

Form Factor
- Chassis
- Ingress Protections
- Battery Casings
- Access Panels

Biometrics
- Imager (size/characteristics)
- Processor/Controller
- Imager Housing
- Illuminator

Data Input
- Keyboard
- Programmable Buttons
- Pointing Devices
- Touchscreen
- Microphone
- Readers
- Other

Platform
- Processor & Memory
- Power
- Output
- Display Device
- Storage
- Interfaces
- Feedback

Communication
- Wired Connectivity
- Wireless Connectivity

Hardware Components

Software Components

N/A

- Data Acquisition
- Signal Processing
- Matching
- Data Management
- Template Generator*
- Interface Control
- Biometric Status Monitoring
- Dynamic Workflow Manager
- Spoofing/Evasion

- Acquisition
- Encoding/Decoding
- Metadata Management

- Operating System
- Applications
- Formatting/Template
- Security
- Template Generator*
- Protocol Management

* Exists in multiple subsystems
## MBHD Expanded Taxonomy

<table>
<thead>
<tr>
<th>System</th>
<th>Mobile Biometric Handheld Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form Factor</strong></td>
<td><strong>Biometrics</strong></td>
</tr>
<tr>
<td><strong>Chassis</strong></td>
<td><strong>Imager (size/characteristics)</strong></td>
</tr>
<tr>
<td>(Camera)</td>
<td>(Programmable)</td>
</tr>
<tr>
<td><strong>Sensor</strong></td>
<td>(Mouse)</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td>(Stylus)</td>
</tr>
<tr>
<td><strong>Processor/Controller</strong></td>
<td><strong>Imager Housing</strong></td>
</tr>
<tr>
<td>(Frame)</td>
<td>(Microphone)</td>
</tr>
<tr>
<td><strong>Seals</strong></td>
<td><strong>Readers</strong></td>
</tr>
<tr>
<td><strong>Protective Coating</strong></td>
<td><strong>Internal Connectors</strong></td>
</tr>
<tr>
<td><strong>Imager</strong></td>
<td><strong>Network Connectors</strong></td>
</tr>
<tr>
<td>(Optical)</td>
<td><strong>Power</strong></td>
</tr>
<tr>
<td><strong>Flash</strong></td>
<td><strong>USB</strong></td>
</tr>
<tr>
<td><strong>Multi-Spectral</strong></td>
<td><strong>Firewire</strong></td>
</tr>
<tr>
<td><strong>IR</strong></td>
<td><strong>Docking Station Interface</strong></td>
</tr>
<tr>
<td><strong>Access Panels</strong></td>
<td><strong>Wiegand Interface</strong></td>
</tr>
<tr>
<td><strong>Battery Casings</strong></td>
<td><strong>LEDs</strong></td>
</tr>
<tr>
<td><strong>External Connectors</strong></td>
<td><strong>Symbols/Pictograms</strong></td>
</tr>
<tr>
<td><strong>Switches</strong></td>
<td><strong>Aural</strong></td>
</tr>
<tr>
<td><strong>Hardware Components</strong></td>
<td><strong>Tactile (Haptic)</strong></td>
</tr>
<tr>
<td><strong>Software Components</strong></td>
<td><strong>Network Management Protocols</strong></td>
</tr>
<tr>
<td>N/A</td>
<td>Data Acquisition</td>
</tr>
<tr>
<td></td>
<td>Signal Processing</td>
</tr>
<tr>
<td></td>
<td>Segmentation</td>
</tr>
<tr>
<td></td>
<td>Quality</td>
</tr>
<tr>
<td></td>
<td>Feature Extraction</td>
</tr>
<tr>
<td></td>
<td>Template Generator*</td>
</tr>
<tr>
<td></td>
<td><strong>Operating System</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Spoofing/Evasion</strong></td>
<td><strong>Biometric Status Monitoring</strong></td>
</tr>
<tr>
<td><strong>Liveness</strong></td>
<td><strong>Dynamic Workflow Manager</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Data Management</strong></td>
</tr>
<tr>
<td></td>
<td>Storage</td>
</tr>
<tr>
<td></td>
<td>Case Management</td>
</tr>
<tr>
<td></td>
<td><strong>Template Generator</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Interface Control</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Exists in multiple subsystems
## DEVICE COMPARISONS - BIOMETRICS

<table>
<thead>
<tr>
<th></th>
<th>HIIDE 5</th>
<th>Fusion</th>
<th>SEEK II</th>
<th>Mobile Ident II</th>
<th>MC75</th>
<th>BlueCheck</th>
<th>DSV2+ turbo</th>
<th>MorphoIdent</th>
<th>PIER-T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Single Flat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Double Flat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Rolled</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Face</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iris</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Single Iris</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Simultaneous</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-board Matching</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.*
<table>
<thead>
<tr>
<th>Readers</th>
<th>HIIDE 5</th>
<th>Fusion</th>
<th>SEEK II</th>
<th>Mobile Ident II</th>
<th>MC75</th>
<th>BlueCheck</th>
<th>DSV2+ turbo</th>
<th>Morpholdent</th>
<th>PIER-T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Smartcard</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Contactless Smartcard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Barcode Reader</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Magnetic Stripe Reader</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>MRZ Encoding</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.*
<table>
<thead>
<tr>
<th></th>
<th>HIIDE 5</th>
<th>Fusion</th>
<th>SEEK II</th>
<th>Mobile Ident II</th>
<th>MC75</th>
<th>BlueCheck</th>
<th>DSV2+ turbo</th>
<th>Morphoident</th>
<th>PIER-T</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weight</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt; 1 lb</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>1 - 3 lbs</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>&gt; 3 lbs</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td><strong>Size (LxWxD)</strong></td>
<td>5 x 8 x 3</td>
<td>8.74 x 4.61 x 2.91</td>
<td>8.75 x 5.5 x 3.5</td>
<td>6 x 3.15 x 1.30</td>
<td>6 x 3.1 x 1.7</td>
<td>4.45 x 1.69 x 0.87</td>
<td>7.3 x 7.3 x 2</td>
<td>5.2 x 2.6 x 0.7</td>
<td>3.5 x 5.0 x 2.6</td>
</tr>
<tr>
<td>S/M/L</td>
<td>Large</td>
<td>Large</td>
<td>Large</td>
<td>Medium</td>
<td>Medium</td>
<td>Small</td>
<td>Large</td>
<td>Small</td>
<td>Medium</td>
</tr>
<tr>
<td>MIL-STD-810F</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>IP Rating</td>
<td>54</td>
<td>65</td>
<td>65</td>
<td></td>
<td>54</td>
<td>54</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.*
Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

<table>
<thead>
<tr>
<th></th>
<th>HIIDE S</th>
<th>Fusion</th>
<th>SEEK II</th>
<th>Mobile Ident II</th>
<th>MC/5</th>
<th>BlueCheck</th>
<th>DSV2+ turbo</th>
<th>MorphoIdent</th>
<th>PIER-T</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Atom</td>
<td></td>
<td></td>
<td>Intel Xscale</td>
<td></td>
<td>Renesas SH4 7760</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>80 GB SSD</td>
<td>128 MB Flash</td>
<td>64 GB SSD</td>
<td>128 MB Flash</td>
<td>256 MB Flash</td>
<td>2 MB Flash</td>
<td>256 MB Flash</td>
<td>64 MB Flash</td>
<td></td>
</tr>
<tr>
<td>Display</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>5&quot;</td>
<td>3.5&quot;</td>
<td>4.1&quot;</td>
<td>3.5&quot;</td>
<td>3.5&quot;</td>
<td>3.5&quot;</td>
<td>2.4&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolution</td>
<td>800x480</td>
<td>320x240</td>
<td>800x480</td>
<td>320x240</td>
<td>640x480</td>
<td>96x64</td>
<td>240x320</td>
<td>320x240</td>
<td>220x176</td>
</tr>
<tr>
<td>Battery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot-swappable</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lasts 8+ Hours</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Peripheral</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Required?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Feature</td>
<td>HIIDE 5</td>
<td>Fusion</td>
<td>SEEK II</td>
<td>Mobile Ident II</td>
<td>MC75</td>
<td>BlueCheck</td>
<td>DSV2+ turbo</td>
<td>MorphIdent</td>
<td>PIER-T</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>--------</td>
<td>---------</td>
<td>-----------------</td>
<td>------</td>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>WiFi</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>GSM</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>CDMA</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>4G</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Ethernet</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>USB</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Docking Station</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>GPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.*
COTS DEVICES MAPPED TO THE TAXONOMY (2011-12)

- Analyzed over 30 COTS MBHD devices*

---

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.
SECTION 12.2 WIRELESS COMMUNICATION

Original BPR Sections
- Wireless Connectivity
- Cellular Connectivity
  - GSM/GPRS/EDGE/UMTS
  - CDMA/1XRTT/EVDO/EVDM
  - HSDPA/WCDMA
- Satellite Communications
- 802.11 b/g
- Bluetooth
- Global Positioning System (GPS)
- Integrated Wireless Antenna
- Wireless Connection Status

Updates needed to reflect current technology
- Wireless Personal Area Networks (WPANs)
  - BlueTooth® (IEEE 802.15.3)
  - ZigBee (IEEE 802.15.4)
  - 6IoPAN (IEEE 802.15.4)
  - Mesh sensor networks (IEEE 802.15.5)
  - Body Area Networks (IEEE 802.15.6)
- Wireless Local Area Networks (WLANs)
  - IEEE 802.11a/g/n/ac
- Wide Area Networks (WANs)
  - HSPA and HSPA+
  - WiMAX (IEEE 802.16e and IEEE 802.16m)
  - LTE and LTE-Advanced
- Regional Area Networks (TV White Space) [IEEE 802.22]
- Mobile Satellite Communication Systems
- Global Navigation Satellite Systems (GNSS)

Note: List is non-exhaustive.
# Section 13 Env't Considerations - Updates Needed?

<table>
<thead>
<tr>
<th>Environmental Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indoor (Normal)</strong></td>
<td>Office environments such as an office building, court of law, etc.</td>
</tr>
<tr>
<td></td>
<td><strong>Operating temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Storage temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Relative humidity</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Ingress Protection Rating (IP Code)</strong></td>
</tr>
<tr>
<td><strong>Law Enforcement (Moderate)</strong></td>
<td>Indoor/outdoor, i.e. patrol officer or in patrol car</td>
</tr>
<tr>
<td></td>
<td><strong>Operating temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Storage temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Relative humidity</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Ingress Protection Rating (IP Code)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Drop resistance</strong></td>
</tr>
<tr>
<td><strong>Military (Extreme)</strong></td>
<td>Harsh environments, such as extreme temperatures, exposure to dust, sand, rain, water splashes, vibrations, and dropping of the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Operating temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Storage temperatures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Relative humidity</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Rain</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Ingress Protection Rating (IP Code)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Drop resistance</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Vibration resistance</strong></td>
</tr>
</tbody>
</table>
Several different types, some including multiple modalities (usually face and voice):

- Google glasses
- Near-field communications
  - Disney’s MyMagic wristband
  - Bionym electrocardiogram bracelets
- Cameras worn by police to record incidents
  - Built-in facial recognition to compare against local watchlists
  - Voice capture for later forensic analysis
- Medical device monitors
- Helmets with iris recognition (to ID wearer) in goggles
- Micro-feature recognition and gesture recognition
- Biometrically verified weapons use
- And more!
Some Challenges for Mobile ID that may be different than fixed location units

- 3D printing of body parts / Reconstructive surgery
- Spoofing and non-cooperative / un-cooperative behavior that is not likely or typical at fixed location units
- Failure-to-acquire protocols
- Privacy and use of data (particularly for DNA)
- Disposal of the mobile unit (including erasure of data)
  - Some units may designed for one-time or limited use
- Protocols for data handling (including erasure of data) during field ops
- Remote or timed disabling operations of the unit (if stolen or misplaced)
- Mobile medical screening combined with biometrics
- Admissibility of data / match results for law enforcement applications
- Interoperability and verified linking of data
- Additional automated modalities (hair pattern growth on face, ear shape, ocular region, blood type, classifiers for ‘soft’ biometrics: height / weight / age / ethnicity / gender / tattoo and scar, etc.)
- Combination with / in devices designed to show exposure to explosives, illegal drugs, pathogens, etc.
- Combination with / in devices to detect health and responsiveness of persons under medical care, in battlefields, or under supervised detention or quarantine
- Operation in harsh environments and under dangerous situations
- Verification of identity of the unit operator and data entry personnel
MobileID BPR for iris images should be consistent with current and emerging standards:

- ISO/IEC 19794-6:2011 Information technology - Biometric data interchange formats - Iris image data
- FDIS 29794-6 Information technology - Biometric sample quality - Iris image data

Three areas of inconsistency

- Image MTF and pixel resolution
- Illumination wavelength
- Minimum distance (margin) from iris outer boundary to closest image boundary
# MTF AND PIXEL RESOLUTION

<table>
<thead>
<tr>
<th>Attribute</th>
<th>MobileID BPR</th>
<th>19794-6</th>
<th>29794-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contrast</td>
<td></td>
<td>0.60</td>
<td>0.50</td>
</tr>
<tr>
<td>Spatial frequency, cycles/mm</td>
<td></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Spatial sample rate, pixels/mm</td>
<td>10.8 - 21.0*</td>
<td>10</td>
<td>15.7</td>
</tr>
<tr>
<td></td>
<td>no upsampling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*derived from specified range of iris diameter in pixels (140 - 210) and typical range of iris diameter of 10mm - 13mm*
Recommendations:

- Specify spatial sampling rate directly in pixels/mm, not iris diameter
- Spatial sample rate of 10 pixels/mm is reasonable estimate of Nyquist rate for typical imaging system using COTS optics
- Allow upsampling from 10 pixels/mm if algorithms require higher minimum iris diameter (in pixels)
Iris imaging systems use near-IR illumination within the 700-900 nm wavelength range. Experience indicates that a wide range of wavelengths is needed to accommodate a variety of eye colors. Mobile devices may require more limited spectral distributions to reduce size and power requirements.
# ILLUMINATION WAVELENGTH

<table>
<thead>
<tr>
<th>MobileID BPR</th>
<th>19794-6</th>
<th>29794-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any 100 nm band within 700-900</td>
<td>Illumination energy should be emitted at wavelengths in 700-900 nm</td>
<td>≥90% of energy shall be within 700-900 nm band; ≥35% of energy</td>
</tr>
<tr>
<td>nm must contain ≥ 35% of total</td>
<td>range, and should be ≥5° off-axis to prevent “red-eye” effect</td>
<td>in 700-900 nm range shall be within 800-900 nm band</td>
</tr>
<tr>
<td>energy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommendation: Adopt specification from 29794-6 to provide maximum design flexibility for mobile devices
**Parameter** | **MobileID BPR** | **19794-6** | **29794-6**
--- | --- | --- | ---
Vertical margin | 0.5 x diameter | 0.2 x radius | 0.2 x radius
Horizontal margin | 0.25 x diameter | 0.6 x radius | 0.6 x radius

Recommendation: Adopt 19794-6, 29794-6 specifications
OPEN DISCUSSION

- Additional topics to be considered
- Formation of subject matter groups
- Selection of working group leads
- Development of a timeframe