White Paper

Use Case and Scenario Development

for

ANSI/NIST-ITL 1-2011 SUPPLEMENT: Mobile Identification, Draft, January 2013

This white paper is intended to better define the concepts presented in the referenced draft proposal for an ANSI/NIST Lite standard for use in mobile handheld biometric devices (MBHDs).

The impetus for the development of a new standard to be used for MBHDs is as follows:

- The need to minimize manual data entry by the officer both from an officer safety viewpoint and operational efficiency (small MBHDs require more attention and dexterity than is usually available to an officer handling a potentially dangerous subject)
- The need to provide the officer a small and light weight device (most officers are already carrying other equipment)
- The growth in new MBHD technology needs to be standard conformant so that interoperability between the MBHDs and the identification systems that they interact is maximized

Recognizing these needs, NIST has proposed developing an ANSI/NIST Lite standard that addresses these issues. This paper provides a discussion of how the MBHDs might be used so as to provide a basis for the development of the new standard.

The format of this paper is as follows:

- A concept description as stated in ANSI/NIST-ITL 1-2011 SUPPLEMENT: Mobile Identification , Draft, August, 2012 (authored by Brad Wing)
- A more detailed description of a scenario for each concept
- A diagram showing the functional relationships of the concept organized into related functional sections
- A generalized use case discussion of each scenario

It is anticipated that the scenarios and use cases presented in this paper will be further developed. The scenarios provided in Appendix A are based on existing applications which provide an overview of the functions that have been addressed by mobile devices. They will need to be upgraded to be consistent with the newest technology and use cases which will be defined by a working group as part of the Mobile ID meeting at NIST on January 28. In all use cases, possible variations and options will need to be defined. Most importantly, an analysis of the impact of the proposed standard on current MBHD configurations and their interoperability with AFIS systems (both Federal and state) will need to be conducted. It is also likely in additon to the ANSI/NIST-LITE standard, a transmission profile may be required for MBHD's that is compatible with ANSI/NIST-ITL and the CJIS and DoD EBTS.

1. Concept 1: Separate mobile units collecting data on the same person in different places and/or times

The following section is extracted without editing from the ANSI/NIST LITE concept paper.

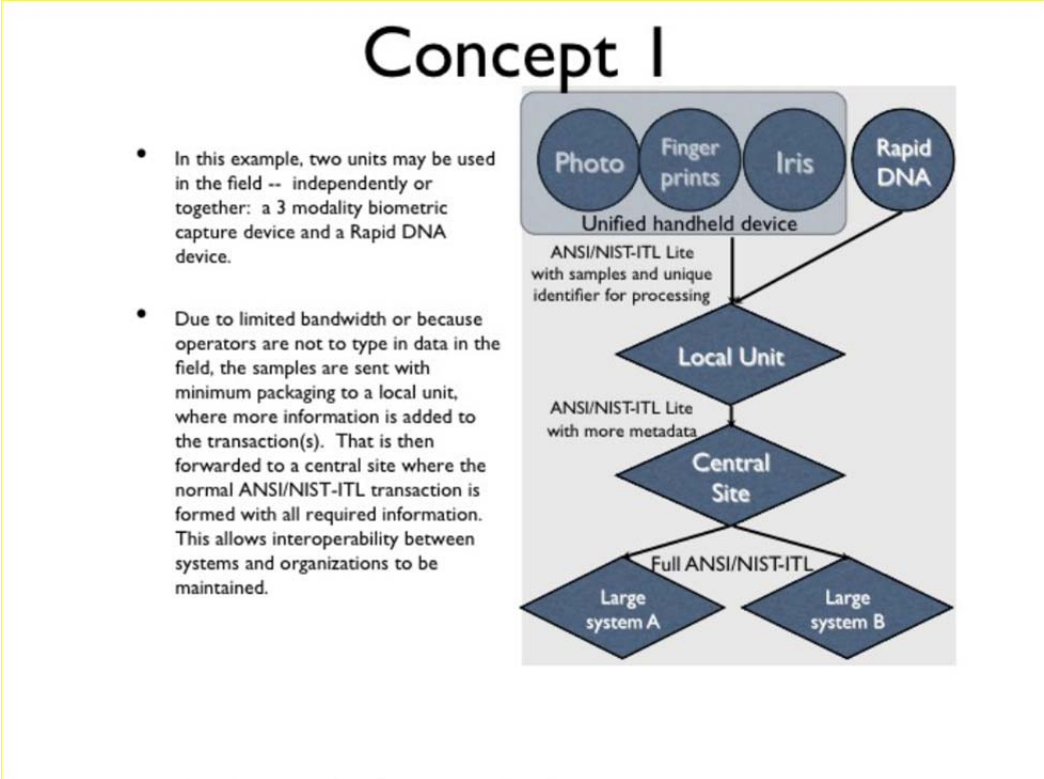

Figure 1 Separate mobile units collecting data on the same person in different places and/or times

Concept 1 illustrates that with the addition of Rapid DNA systems, the range of possible configurations of mobile applications involving biometrics has greatly expanded. An example of how this Concept could come into play is a Disaster Victim Recovery scene. Photos, fingerprints and iris images (if possible) would be taken using one unit, DNA samples using another. The information would be brought to the local processing center and sent to a law enforcement agency for formatting into ANSI/NIST-ITL transactions that could be submitted to the FBI, US-VISIT, INTERPOL or other organizations that accept ANSI/NIST-ITL formatted transactions.

The key is that there must be enough information collected by the operator or collection device at the scene to uniquely associate the data with the deceased individual. This can be accomplished in a variety of ways, including automated GPS data entry, time/date entry, and voice capture from the operator describing how the samples were taken. Note that the voice recording from the operator can be included as an associated context data record Type 21 in the ANSI/NIST-ITL full transaction.

1.1. Scenario: Disaster Recovery Site Operations (minimal manual data entry)

This section develops Concept 1 in greater detail:

Disaster recovery team arrives at site with mobile devices and a local server. Prior to start of operations, each team member is issued a mobile biometric device and some specialists are provided with a rapid DNA processing device. As part of the issue process, each device is registered onto the local server to the receiving team member and as part of the process, the team members biometric is also captured for security purposes.

The team members start their identification work by first logging-on using their biometric. The log-on is valid for one hour (after that period a repeat of the log-on will be necessary). The log-in biometric is sent to the local server for validation together with the device identifier. A successful log-in is acknowledged with a message back to the device. The team member now sets about capturing the disaster identification data. The first image to be captured will be an image of the disaster victim; if needed multiple images may be captured. With each captured image, the device asks the disaster team member if this is a new subject or if additional data is being captured for the subject being processed. The query is simply a sequence number that is updated or continued. GPS location data is captured with each image. (This will later be used as an aid in integrating the captured data).The team member may acknowledge with a simple key entry or by voice. Following the overall evidence image(s) capture, the team member will proceed to capture fingerprint and face images and if possible iris images. This process will be repeated for all subjects to be processed. A data capture sequence number will be assigned internally for tracking the data and for later use in integrating the data for each subject.

It should be noted that there is little or no manual data entry in the field. All entries are automated and are sent to the local server for integration into a single subject record. If additional data is desired on the same subject at a later time or by a different team member, the data will be collected as a new acquisition which will be integrated into a subject centric record at a later time by the local or central server.

Those team members issued a DNA collection device will need to log-on to their device which also had been previously registered onto the local server. The device will need to be equipped with a standard biometric capture or with a GPS location capture capability in order to associate the subject's DNA with the other biometric data. Operation of the ancillary biometric capability will be the same as described above.

Following the capture of each biometric, the local server will calculate if the captured image data is of sufficient quality. If the captured data is of insufficient image quality a message will be sent to the mobile device indicating a potential problem. The team member will than have the option of recapturing or accepting the old data. This will be communicated to the device via voice or a simple key entry. The local server will assemble a complete subject record from the previously captured biometric data every time that the team member indicates that a new subject is being processed. This record will be sent to the central site server for further integration.

The central site server will determine which records are associated with the same subject using the information provided from one or more mobile devices. The data to be used for the integration will include registered device and team member identification numbers, the capture subject sequence number, and where necessary, a biometric verification of data captured from multiple devices. Failures to integrate will result in error messages and a manually assisted resolution capability will be provided. This will include the ability to display all data associated with the subject and if needed, data for other subjects that may be in question. An operator will make the final determination as to when to send the data to a large biometric identification system for identification purposes and if appropriate for enrolment.

The local server and central site server will have security provisions and will log all data for later archiving.

1.2. Alternative Scenario: Disaster Site Operations or Refugee Identification Operations

Alternative scenarios can be defined for other situations that would be similar to the disaster recovery operation. For example a refugee or displaced person situation such as the one experienced in New Orleans during the Katrina disaster could readily use the same concept. While a DNA unit normally would not be needed, it is conceivable that in some cases it may be required.

1.3. Use Case Diagram

This diagram provides greater detail to the ideas presented as part of Concept 1.

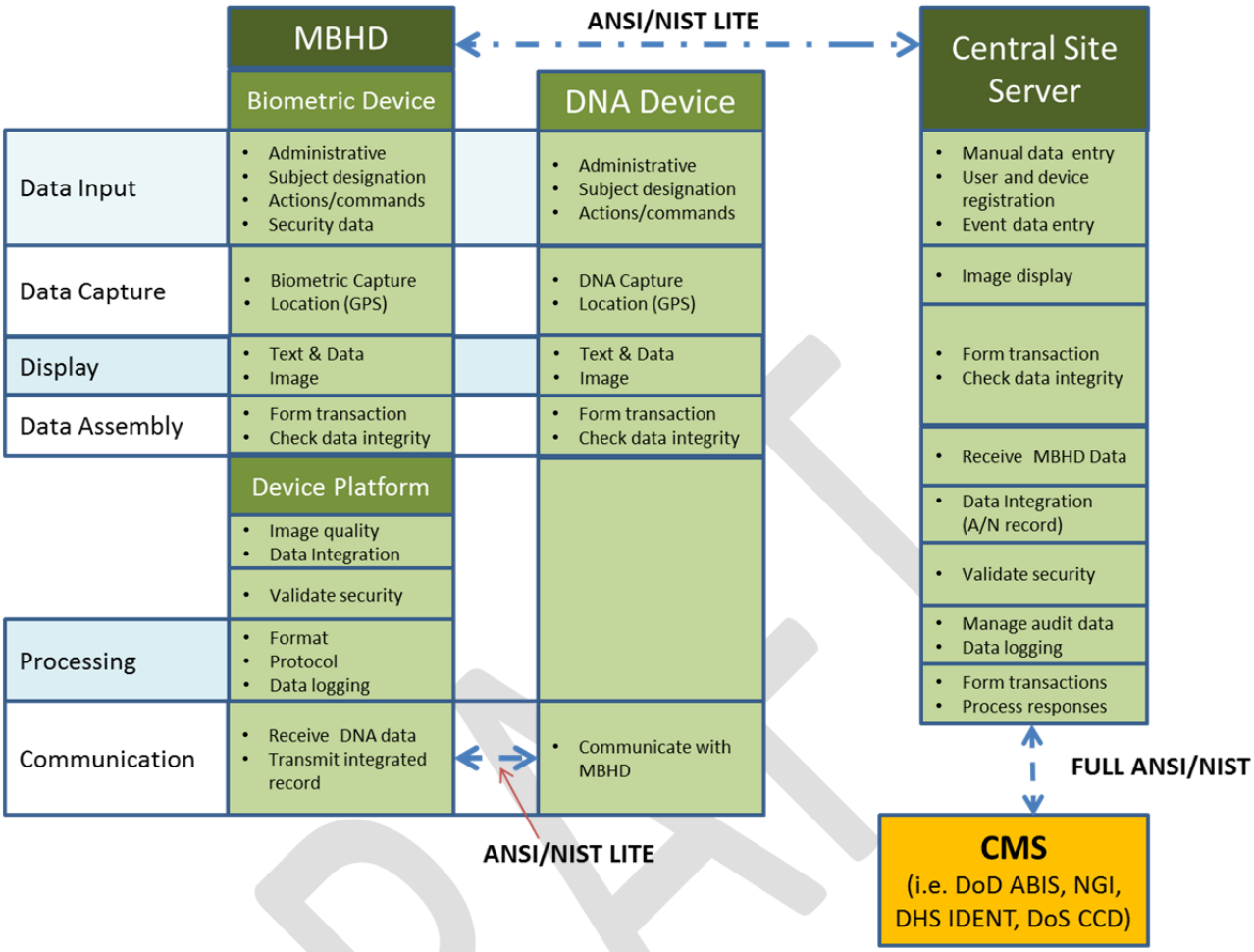

Figure 2 Integrated MBHD with an auxiliary DNA device

The integrated device would have one or more biometric data capture capabilities such as fingerprint, face, or iris, a voice capture for transaction data input and possibly for security applications, WiFi or Blue Tooth capability, and/or e-mail connectivity. It would also have the ability to accept data from a rapid DNA collection device.

A local site server with local database would be used for logging data and integrating records related to designated data samples, security provisions, registering capability for user and device, and communications with device and central server.

Data entry requirements at each device would include biometrics associated with subject or body parts (including scene image), designated identity via voice entry (e.g. subject or subject part number, body part description - optional), optional GPS data, device ID (pre-registered at local unit).

Minimal functionality required at the device level includes multiple biometric captures, possibly using different capture devices (subsystems) for some biometrics (e.g. DNA), location identifier capability provided by GPS, voice record providing data designation, and the capability for the devices to send a

unique device identifier. The device must also communicate with the local site server and have the ability to send data and receive error and enrolment messages

Functionality required at the local site server includes the ability to integrate the acquired data received from all sensors with the subject identifiers, calculate data quality metric to generate acceptable enrolment or error message, registers device and user, communications with devices, and the ability to add user and device metadata to transaction record (GPS, type of operation, date). The server will record all acquired data, added metadata, and all computed data (e.g. image quality metrics). It may also perform recognition of the voice data entry. The local site server would also provide security management, audit functionality, and connectivity management with the central server.

Functionality at the central site server includes checking data for duplication and if needed adding more metadata such as incident related data. The central site server would transmit data to large identification systems (e.g. IAFIS, ABIS) which is herein called a central matching system (CMS), on line or in a batch mode. The central site system receives identification from CMS, performs additional identity consolidations if needed. A search response request would be generated by the CMS which would be sent to the central or local site servers. . It is not clear if search results would be sent to the device or to the local server only for this scenario. Alternatively, the central site server could have preloaded subject database and could perform matching locally.

Issues:

- Security level requirements at device
- Data quality metric could be performed at device or local sever
- Identity consolidation may need to be performed at both local and central server
- Is a split between local and central serve required?
- Types of connectivity to be used between device and server and between servers and server and CMS
- Are search responses to be sent to the central site server, local site server, and/or the device?
- Are search decisions to be confirmed at the central or local server?
- Type(s) of biometric to be captured, enrolled, and matched
- Method of biographic/encounter data entry (card reader and/or touchscreen or keyboard)
- Data use by the CMS (verification, identification, and/or enrollment)
- It is also not clear if the scope of this requirement definition should be limited to the device only or if it should address the local and central site servers.

High level requirement for the device:

- Text entry method:
  - Voice
  - Touch screen
  - Keyboard
- Type of biometric to be captured:
  - Fingerprint (single touch print scanner)

    - Fingerprint (four finger touch print scanner)
    - Facial Image
    - Iris
- Multiple biometric capability
- Logging
- Data Formatting – Scope of ANSI/NIST Lite
- Connectivity:
    - Direct Internet connectivity
    - Cellular network
    - Dedicated network
    - Satellite link
    - Data buffering capability
- Security requirements, Sign-on & Encryption

2. Concept 2: Rapid Identification with Limited Bandwidth

The following section is extracted without editing from the ANSI/NIST LITE concept paper.

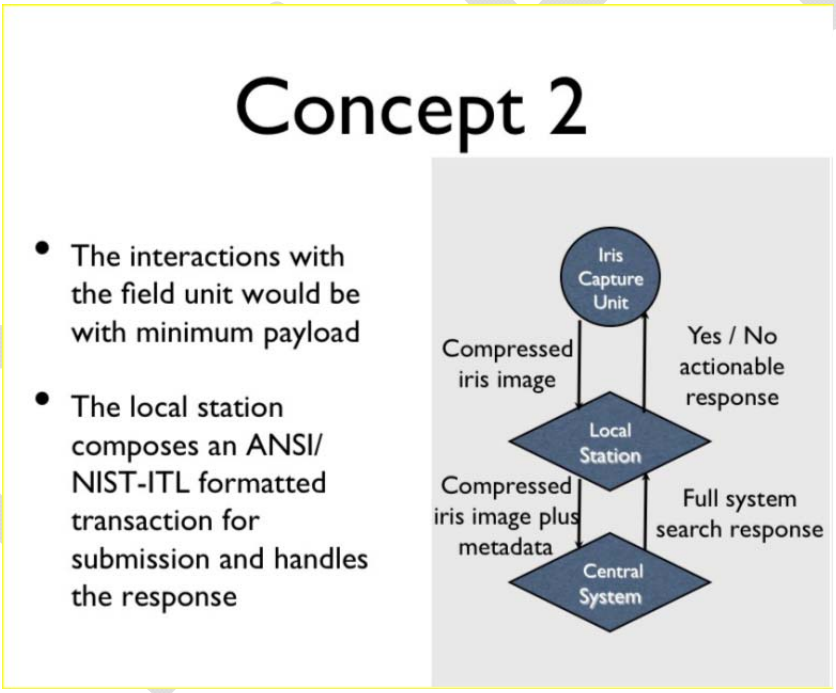

Figure 3 Rapid Identification with Limited Bandwidth

In this concept, a mass-processing of individuals is being performed, with a quick turn-around requirement. An iris image is captured and forwarded to a local station for processing. Only if a 'Yes' is returned with an identifier for the individual does the operator spend more time collecting metadata

about the individual and possibly more biometric samples. The exact response would, of course, depend upon the situation and the Standard Operating Procedures (SOP).

2.1. Scenario: Fast enrollment and identification of a group of subjects (minimal manual data entry)

Team of law enforcement officers is sent to a civil disturbance site where numerous subjects have been detained. It is necessary to quickly identify the subjects to determine if any of the subjects are on a watch or wanted list or have a criminal history that warrants additional processing.

The team members are equipped with a rapid identification device and the site has a local server (possibly in a patrol car) that will act as a data integrator and includes a store and forward capability. Prior to start of operations, each team member is issued a mobile biometric device. As part of the issue process, each device is registered onto the local server to the receiving team member and as part of the process, the team members biometric is also captured for security purposes. Each device will be logged on for one hour prior to requiring a repeat of the log on data capture. An officer will also enter the incident information into the local server.

Once logged on, the officer will capture the subjects biometric (iris, face, or finger) which will be transmitted together with the device identification number to the local server. The local server will determine image quality and send a message back to the officer requesting a re-capture or a decision to go ahead with the original image. The officer will see the display and will either toggle a response to use the data or to re-acquire. No other manual data entry will be re required. Once the biometric data capture is complete (either image quality is sufficient or approved by the officer), the data with the device identification number will be transmitted to the local server. GPS location data may be an optional capability. The local server will assemble a record containing the officer identification, biometric data, incident data, and if available, the GPS location data. The record will be formatted as a search request against a CMS (central matching system such as IAFIS).

A search response from the CMS will be provided to the local server. Identification information will be of the type known as green, yellow, or red. A red response will contain subject demographic data, a face image, and any information related to the wants/warrants and watch list status. Green response will not include any information. A yellow response will indicate to the officer that additional data is required for positive identification or for secondary processing. All data received at the local site server will be logged for later archiving and audit.

2.2. Concept 2 Use Case Diagram

The use case configuration is described in Figure 4 Rapid Identification with minimal bandwidth and limited manual data input.

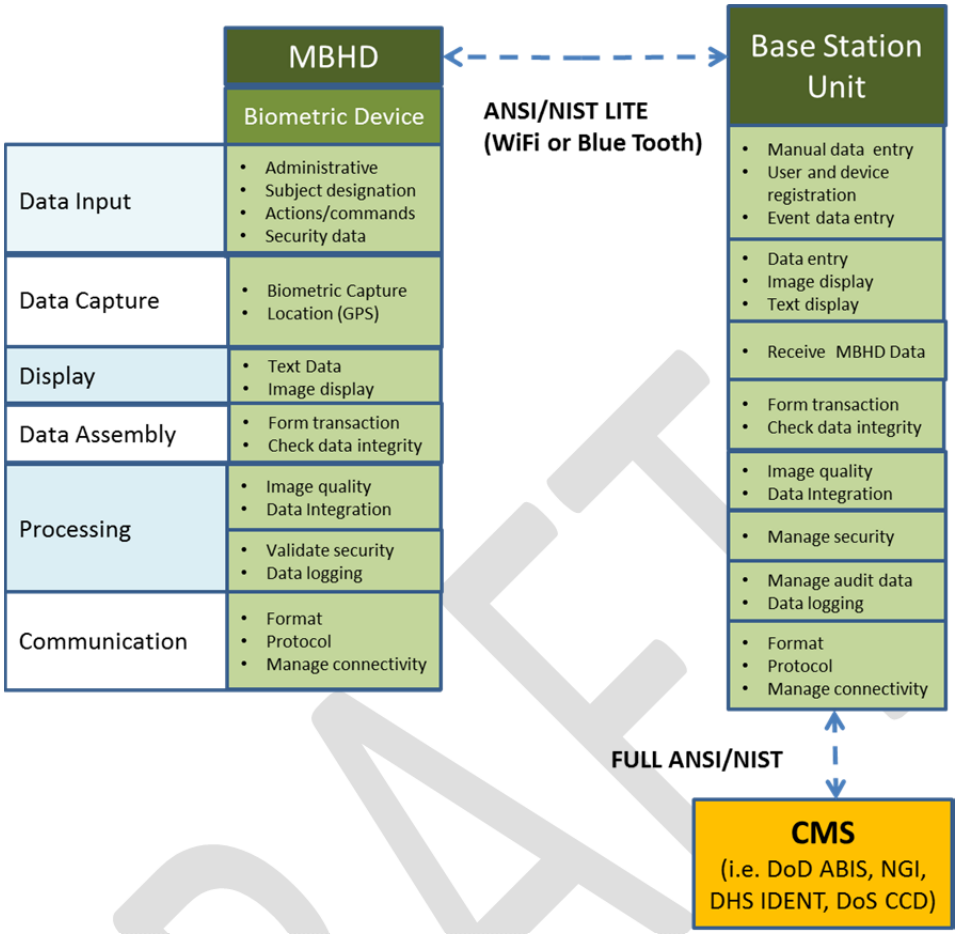

Figure 4 Rapid Identification with minimal bandwidth and limited manual data input

This use case is applicable to scenarios that require fast enrollment and identification of a group of subjects. Note that the use case assumes that multiple MBHDs could be connected to a single local site server or base station unit.

The MBHD is equipped with an iris capture capability, minimal manual data entry capability (accept or reject switch or button), security application, and WiFi or Blue Tooth connectivity.

A local server is used to register the user and device, and to provide formatting and communications with the device and central server. Data entry at the device may use other biometrics such as face, voice, or fingerprint as an alternative or in a multimodal manner. Optional GPS location data may also be included.

Minimal functionality required at the device level includes biometric capture (one or more biometrics), message and image display, accept/reject biometric image data entry, communication with the local site server (base station unit), and the ability to send data and receive response and error messages.

Minimal functionality required at the local site server includes the capability to integrate the data received from the device, calculate a data quality metric to generate acceptable data quality or

recapture message, registering the device and user, communications with the devices, and the addition of user and device metadata to the transaction record (GPS, incident data, officer identification, device identification, date). The local server unit will store all acquired data, added metadata, and all computed data (e.g. image quality metrics) for archiving and audit purposes. It will manage connectivity with the CMS and transmit the response to the appropriate device.

Issues:

- Security level requirements at device
- Data quality metric could be performed at device or local sever
- Types of connectivity to be used between device and server and server and CMS
- Are search decisions to be confirmed at the device or local site server?
- Are search decisions to be confirmed at the central or local site server?
- Type(s) of biometric to be captured, enrolled, and matched
- Method of biographic/encounter data entry (card reader and/or touchscreen or keyboard)

High level requirements:

- Text entry method:
  - Voice
  - Touch screen
  - Keyboard
- Type of biometric to be captured:
  - Fingerprint (single touch print scanner)
  - Fingerprint (four finger touch print scanner)
  - Facial Image
  - Iris
  - Voice
- Multiple biometric capability
- Logging
- Data Formatting – Scope of ANSI/NIST Lite
- Connectivity:
  - Cellular network
  - Data buffering capability
- Security requirements, Sign-on & Encryption

3. Concept 3: Capture Modules Physically Separated from Control Unit.

The following section is extracted without editing from the ANSI/NIST LITE concept paper.

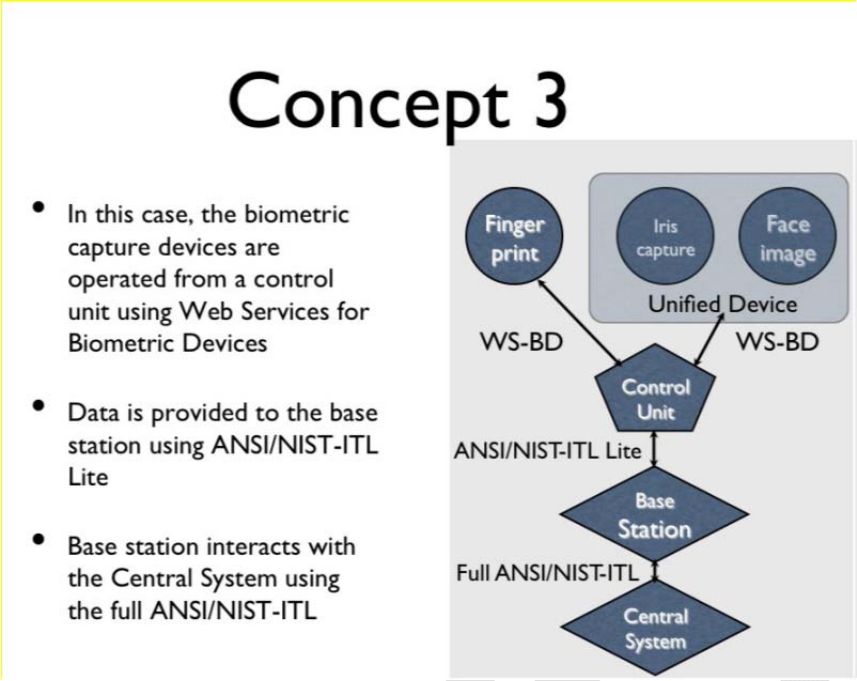

Figure 5 Capture Modules Physically Separated from Control Unit

WS-BD indicates formatting according to the *Specification for WS-Biometric Devices (WS-BD), NIST Special Publication 500-288.* A coordinator could actually provide the commands to capture units that are physically separate. All responses would be sent to the control unit and not forwarded to the capture units. This may be important when the operator does not want to have the response possibly visible to the subject. Another concept would be that the operator is holding the capture device in one hand, and must maintain the other hand free for safety.

3.1. Scenario 3: Biometric Identification (Capture Modules Physically Separated from Control Unit)

This is virtually identical to scenario 1 except that the local site server is separate from the devices. Less data integration is required. Communications between the devices and the local site server (control unit) uses WS-BD standard.

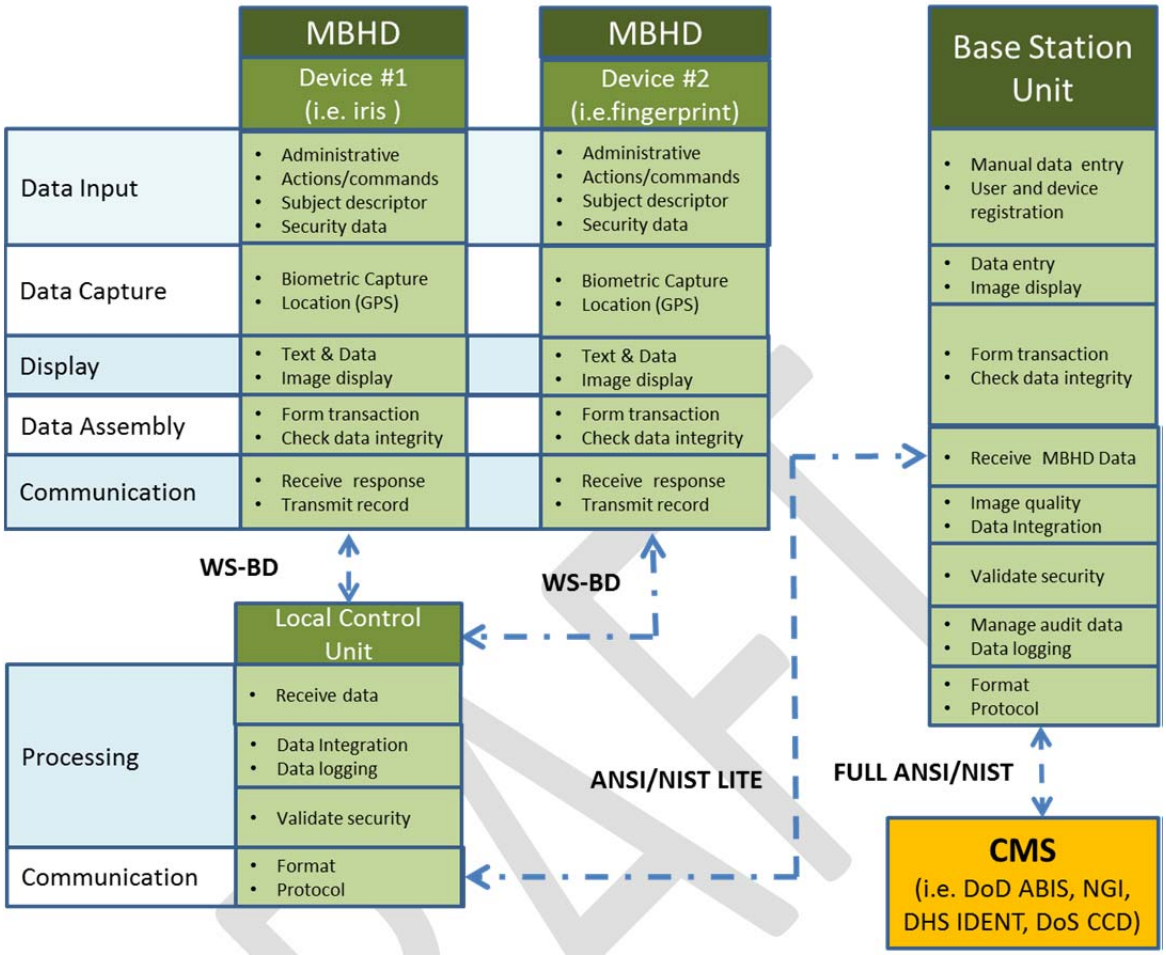

Figure 6 Use Case for Capture Modules Physically Separated from Control Unit

Use case description for Concept 3 is very similar to Concept 1 except that the local control unit is separate from the devices. It is possible that this use case could be made a sunset of Concept 1.

Issue:

- The capabilities addressed by this scenario are a subset of scenario 1.
- Application needs to be better defined.

4. Concept 4: Mobile Modules Communicating to Different Systems

The following section is extracted without editing from the ANSI/NIST LITE concept paper.

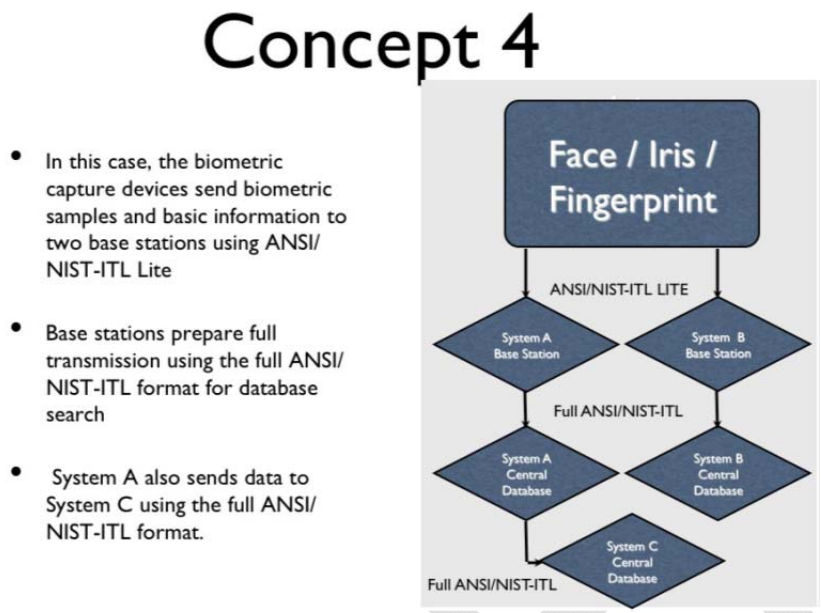

Figure 7 Mobile Modules Communicating to Different Systems

4.1. Scenario 4: Mobile Modules Communicating to Different Systems

This scenario is an extension of Concept 1 except that the search and response transactions are communicated with multiple large scale identification systems (CMSs). The use case configuration can be a variation on Use case 1 or 3. The only difference is in the ability of the device to communicate with multiple search systems.

Issue:

- The scenario should be a subset of Use Case 1.

Appendix A

The following are extracts for a set of scenarios developed for DHS that potentially could use the proposed new standards (ANSI/NIST Lite and WS – BD). These are included as provided to DHS S & T and are intended for discussion purposes only. These scenarios have not been approved by any of the referenced agencies; they reflect our high level understanding of the application and are not necessarily representative of actual operations.

1. Law Enforcement Patrol Activities - Variation A

Officer stops a car because of suspicious behavior. The driver is asked for his driver's license which is examined and is transmitted to the National Crime Information Center (NCIC) using the patrol car computer for a routine license check. The license appears valid and there are no outstanding wants or warrants, but the officer is suspicious of the license as the photograph is somewhat different from the driver's face. He takes the MBHD and enters his password to enable the device. The password input is also used to associate the officer identification with any data that will be created and sent by the system. With MBHD unlocked he manually enters a text command (or special function key or voice command) to start the processes for capturing the subject's fingerprints. Once the subject has placed the finger on the device platen, the officer activates the capture image function key. The fingerprint image is captured (a plain touch print) and the device evaluates the image quality providing a feedback response to the officer indicating either the acceptability or non- acceptability of the fingerprint image. If it is unacceptable, the officer tries again until such time as either the image quality is acceptable or else the officer overrides the quality criteria via a text command (the device may be preprogrammed to perform only three tries, accepting the last try automatically). On completion of the capture of the first fingerprint, the officer captures the second fingerprint using the same process. With both finger image captured the officer activates the search function. The MBHD sends the message via a wireless link to the patrol car computer which formats the message into ANSI/NIST and forwards the search to IDENT. IDENT searches its files and provides the response to the patrol car computer which forwards it to the MBHD. The IDENT response is a text message that shows that the driver has had several encounters with the Border Patrol and has been deported to his country of origin on two occasions. The officer requests a photo of the identified subject, which was transmitted with the text data by activating a command (or voice) on his MBHD. IDENT returns a photograph, which looks more like the driver than the image on the driver's license. The officer realizes that the driver is an illegal immigrant driving on a stolen license. He takes the driver into custody and informs the Border Patrol of the identification via telephone.

2. Law Enforcement Patrol Activities - Variation B

Officer stops a car because of suspicious behavior. The driver is asked for his driver's license which is examined and is transmitted to the National Crime Information Center (NCIC) using the patrol car

computer for a routine license check. The license appears valid and there are no outstanding wants or warrants, but the officer continues to be suspicious. He takes the MBHD and performs a fingerprint image capture from the driver. The MBHD indicates that the fingerprint quality is poor, repeated attempts result in failure to capture the image (see 3.1.1.1.1 above). The officer examines the finger and finds scarring possibly indicating intentional mutilation. He then proceeds to capture the driver's irises. The MBHD evaluates the iris image quality and provides an indication of acceptability or non-acceptability. The officer performs a recapture if it is unacceptable or else over-rides the quality indication and activates the search request function via a keyboard command. (The MBHD may have dual iris or a single iris capture camera. If the camera is a single iris type, the officer than captures the second iris using the same process as described previously). The iris images are sent to the local patrol car computer which formats the data and sends it to NGI for a search of the iris database. A match is obtained against a subject on the watch list and NGI forwards a response to the server which forwards the response to the MBHD. The text response is coded to indicate that the subject may be armed and dangerous. The officer arrests the driver and takes him into custody.

3. Law Enforcement Public Event Disturbance

Law enforcement officers at a political event see a fight break out between the legally sanctioned demonstrators favoring immigration reform and a large numbers of counterdemonstrators. It seems that about twenty individuals from each side are fighting and that the fight is escalating. The officers move in and detain the individuals involved. This confrontation was expected and the officers have set up a temporary booking site nearby. The officers take the individuals to the temporary booking area where an MBHD is available for entering data for search against several national biometric recognition systems. The officer first enters his password to enable the device. The password input is also used to indicate the officer identification with any data that will be created and sent by the device. With the MBHD unlocked, he manually enters a text command (or special function key) to start the processes for capturing the subject's fingerprints. The MBHD is equipped with a four plain finger scanner and a facial image capture camera. The officer enters the subject's biographic data as provided by the subject. An automated program prompts the officer to enter all required text data and following completion of the text entry, it prompts for a start of a fingerprint scan of all ten fingers (4+4+2). The MBHD performs an image quality check on each image and if a retry is necessary informs the officer with a text message. The image data is recaptured, if necessary, or else data is accepted because the officer decides that additional attempts would not be productive. The acceptance is done via a manual text entry. Once the fingerprint capture process is complete, the officer initiated a facial image capture for each individual. The complete data record, including text, fingerprint image data, facial image data , and encounter data (location, type of encounter, officer ID, etc.) is formatted in accordance with the EBTS data exchange format and is sent to IAFIS where it is determined that two of the individuals are on parole for previous aggravated assault convictions. The response on each of the individuals is coded for safety reasons. A parallel search of IDENT, using the same data shows that one of the demonstrators has a previous voluntary removal and is therefore likely to be an illegal immigrant. A further search is initiated by the officer via text command against the DoS CCD facial image watchlist and several records are returned indicating a potential match on two more individuals. The CCD response provides candidate facial

images which are compared side by side with the images captured at the encounter. These are analyzed by the officers and further identifications are made. All identified individuals are arrested, this action is indicated on the MBHD and the arrest action with the complete record are enrolled in the IDENT and NGI databases (this could be done at the time of the search if an arrest charge is made). The officers take these men into custody and inform CBP of the detention via telephone. The rest are released with a warning.

4. POE Identity Verification

A POE inspector at the US-Mexico border is presented with a US travel document that he suspects is fraudulent. The inspector has previously enabled the passport reader device by entering his password which automatically causes all subsequent data entries to be associated with his identification number and name. On attempting to read the document on a passport reader, he finds that the encoded image has been corrupted and cannot be read. The subject claims to be handicapped and cannot leave his vehicle without assistance. The inspector takes his MBHD (password protected) to the car and the document text is read by the MBHD mage stripe reader and a biometric (facial image) is captured. The data, including the encounter data, document text data, and the facial image are sent to DOS Consular Consolidated Database where it is matched against the biometric indicated by the document identification number (verified). The biographic data is also checked against the CCD watchlist. The identity is verified, no listing in the watchlist is found, and the subject is allowed entry.

5. POE Identity Verification - Fingerprint and Facial Image Identification MBHD

Those individuals that cannot have their passport read or do not have a passport are asked to enter the guard house where their biometrics are captured (fingerprints and photograph) on a larger MBHD with full identification capability. The officer first enters his password to enable the device. The password input is also used to indicate the officer identification with any data that will be created and sent by the device. With the MBHD unlocked, he manually enters a text command (or special function key) to start the processes for capturing the subject's fingerprints. The MBHD is equipped with a four plain finger scanner and a facial image capture camera. The officer enters the subject's biographic data as provided by the subject. An automated program prompts the officer to enter all required text data and following completion of the text entry, it prompts for a start of a fingerprint scan of all ten fingers (4+4+2). The MBHD performs an image quality check on each image and if a retry is necessary informs the officer with a text message. The image data is recaptured, if necessary, or else data is accepted because the officer decides that additional attempts would not be productive. The acceptance is done via a manual text entry. Once the fingerprint capture process is complete, the officer initiated a facial image capture for each individual. The complete data record, including text, fingerprint image data, facial image data , and encounter data (location, type of encounter, officer ID, etc.) is formatted in accordance with the EBTS data exchange format and is sent to IDENT. IDENT searches the data to determine if a past encounter exists and returns the appropriate text response.

6. At Sea Interdiction

Officers board a small ship in US waters looking for potential contraband. Once on board they find about thirty individuals suspected of trying to enter the US illegally. With a password protected MBHD, the officers enters minimal biographic data and captures the fingerprints (two fingers), facial image, and irises (future capability) of each individuals found on board. All captured data is checked for image quality acceptability and the officer has an opportunity to recapture or accept the data using a keyboard command. The captured record for each individual, including the encounter data (officer identification, ship, location, type of interdiction, etc.), subject biographic, and the two sets of biometrics are formatted and sent to IDENT via a satellite link to be searched. (To facilitate the entry of encounter data, much of the data can be pre-entered and enabled by associating it with the password owner identity). IDENT returns a response indicating previous encounters and facial image of the previously detained individual or of an individual on a watchlist. The device allows the officer to continue capturing data without waiting for the response to each search request. All responses are queued and can be displayed on request using a keyboard command. Each response includes a facial image so that the officer can associate the response to the specific subject.

7. Maritime Interdiction Operation

Officers are conducting a compliant maritime interdiction operation seeking terrorists. The Coast Guard is equipped with MBHDs that are password protected, have a satellite link, and provide image quality assessment for each biometric being captured (tenprints, face, and optionally iris). After obtaining flag state consent, the team boards a large container ship and collects biometric samples from each crewman. The data is transmitted to an authoritative source, and is followed up with acknowledgment of receipt. The biometric data is compared against all stored files, and shared with mission partners. A subsequent match is made on three of the crewmen. Furthermore, the matched files show a link to the National Counterterrorism Center (NCTC) terrorist watchlist. The authoritative source updates the applicable biometric files with newly collected biometric samples and contextual data. The interdiction team is informed of the match result and watchlist status. Each response is linked to the captured facial image to facilitate association of data with each individual.

Further analysis of the biometric files and additional associated information indicates the three crewmen have travel patterns consistent with those of previously apprehended terrorists. Based on this information, the on-scene commander detains the three crew members pending further disposition.

The on-scene commander further requests, and is granted, flag state authorization to conduct a detailed search of the vessel. In the course of the search, 40 undocumented individuals are discovered in a cargo hold. They are determined to be attempting illegal entry into the US. Also during the search, documents related to the design of an improvised nuclear device are discovered and collected. Biometric samples are collected on the ship's crew and undocumented individuals. The biometric data is again transmitted to an authoritative source and compared to all stored files. No match is made. Each individual's biometric data is enrolled into a biometric file, linked to the WMD information, and stored for later use. The on-sight commander analyzes the results of the biometric match processes and other available

information to determine a course of action. The biometric files and related associated information are shared with the mission partners and entered into interagency systems, including the FBI Criminal Justice Information Systems (CJIS), DoD, and DHS Immigration Systems. The on-scene commander informs the appropriate authority and, after receiving flag state and US Government authorization, takes the undocumented individuals into custody pending further disposition.

8. Disaster Site Operations

Officers are sent to a disaster site to process applicants who need immediate shelter and financial assistance. To guard against duplicate applications and to ensure that the persons are not on a wants and warrants list and therefore ineligible for assistance, the applicants will be fingerprinted. The officers use an MBHD that is password protected and has a two fingerprint and a facial image capture capability. All biometrics are assessed for image quality and repeat capture is allowed to obtain an acceptable image. All biographic data is entered manually using a keyboard. Automated entry is not possible as most of the individuals do not have readable credentials.

Since the disaster has rendered local communications inoperative, all enrolled data must be searched later at another site where there are communications. The locally captured data is uploaded at the central site to a local server for searching against IAFIS and IDENT. Duplicative applications are flagged and ineligible applicants are identified. The list of eligible subjects is entered onto eligibility lists for assistance and applications are automatically forwarded for processing. Individuals attempting duplicate enrollment may be charged and arrested.

9. First Responders Access Control

First responders are required to enter a secure facility to deal with the situation resulting from an accident that has led to an explosion resulting in injuries and a fire. Using their first responder access card, a PIV-I card issued by their state/local jurisdiction, the first responders are screened using an MBHD handled by the secure agency security staff, which allows the identified personnel access to the explosion site. The MBHD is password protected. Data for all first responders has been previously preloaded on the MBHD. The access card is based on the PIV standard and it contains fingerprint templates for verification of the first responder's identity using a plain (touch) finger reader. The reader has multiple attempt capability with an image quality reject function. The process of identity verification and first response attribute conformation authorizes the first responder to enter a restricted zone and the authority to perform certain functions (such as medical support).

10. Mobile Applications of TWIC

The USCG is notified of the identity of all persons aboard a Liquid Natural Gas vessel 96 hours prior to their arrival in US waters. USCG personnel board the vessel as it approaches US waters and using an MBHD read the TWIC cards of all persons aboard. The MBHDs are password protected and have an image quality check capability for the fingerprint image capture process. The MBHD checks each person's biometric (two plain fingerprints) to make sure that the card belongs to the person holding the

card. The data is also checked against a watchlist (optional capability) to ensure that the card holder has not been placed on a watchlist since the arrival notification. USCG finds that there are some crew substitutions. These individuals are detained pending further identification in port.

11. Identification of Deceased

A body has washed up on Coronado Island and an officer is called to the scene. The agent using a mobile biometric handheld device captures the fingerprints on the beach. The agent logs onto his device, enters a password and inputs text data related to the encounter. The text data includes location, approximate description of the diseased (sex and age). Because the fingerprints are of poor quality, the agent captures all ten fingers and initiates a search of the authoritative databases using all ten fingers. Within thirty seconds a response is received indicating that the subject is a previously deported aggravated felon with an outstanding State felony arrest warrant. On returning to his office, the agent retrieves the identification data and re-enters it manually (using an internet connection) into the State AFIS and IAFIS to update the criminal records and the warrants list.

12. Checkpoint Operations

SIG agents conducted a vehicle stop on Interstate 15 which resulted in the discovered of 28 grams of marijuana. The agent signs-on to his mobile biometric handheld device and proceeds to book the subject. The agent captures all of the driver's identification information by automatically reading his driver's license and captures all ten-fingerprints. The data is sent to the State AFIS as an arrest record and also to IDENT to ensure that the subject is not on a watchlist or has derogatory information in IDENT. The search response shows no previous records in either of the searched systems. The captured data is entered into the State system as a simple possession (21 USC 844). The agent releases the driver after seizing the marijuana. A court appearance date will be sent to the subject from the State computer.

13. Joint Operation

Agents are contacted by the San Diego City Police Department to identify a male that was hospitalized due to cold weather exposure. Using their MBHD, the SIG agents sign-on to the device, enter encounter data and fingerprint the subject (two fingers). The data is sent for a search of IDENT. IDENT provides a response, identifying the subject as an illegal alien. Following an interview with the subject, additional individuals are identified by the subject as deceased smuggled aliens. Using the MBHD, identification data (location of bodies – part of encounter data) supplied by the subject is used to retrieve the data on the unknown individuals and the unknowns records is updated.

14. Detention Facility Operations

Agents are deployed to a detention facility to perform identity screening. After signing-on on their MBHD, the agents capture the inmate biographic (name, sex, date of birth, etc.) and their biometrics

(fingerprint - tenprint, face, and iris). The MBHD also supports recapture of biometric data if necessary to meet minimal image quality metric thresholds. The data is sent via a WiFi connection to a local server which sends the data to IDENT to determine if there is any derogatory information. In all cases, the encounter data is updated on IDENT and the biometric data is enrolled. All data sent to the local server is also checked for possible duplication. Responses from IDENT are received at the server, which retransmits the data via WiFi to the MBHDs. The agents interview the identified subjects and fill in any additional data obtained from the interview into the local server. The list of all positive identifications, after consolidation, as well as any interview data is reported to the appropriate authorities.

15. Los Angeles County Sheriff's Department - Patrol Stop

An officer with the Los Angeles Sheriff's Department stops an individual acting suspiciously in an alley in back of a strip mall. The subject claims that he was merely looking for scrap materials. When asked for identification, he says that he has no identification document. The officer takes out his Blue Check MBHD and scans his own index finger to enable access to the device. He then captures the subjects' fingerprints (right and left index fingers) on the same device and requests a search of the Los Angeles County Regional Identification Systems (LACRIS). The request is relayed from the MBHD to a BlackBerry, also carried by the officer, using Blue Tooth communications. The BlackBerry sends the search request via a secure communications' link to LACRIS using a public cell carrier. Within 40 seconds the Blackberry receives a response indicating the identity of the subject. A fingerprint display is provided showing a side by side comparison of the submitted fingerprint and a returned fingerprint. These appear to be for the same individual. A photograph of the subject is also included which is corresponds to the detained individual. The officer, using the MBHD, requests a search of State AFIS to determine if there is an outstanding want or warrant on the subject. The State ID number and name of subject, as provided by LACRIS, are used as the search parameters. This request is processed in the same manner, but this time, the request is relayed by the patrol car computer to the State AFIS. A negative response is received from the AFIS and it is forwarded to the MBHD. The subject is released.

16. Interdiction at Sea

USCG stops a small boat in US waters that is suspected of drug smuggling. Two officers board the boat, one of them with an MBHD. Previous to boarding, the officer had signed on to the device using a password. Once aboard, one of the officers proceeds to capture the fingerprint data (two index fingers) and entering subject text data (name, sex, DOB) using the device keyboard. The fingerprint is evaluated by the software on the MBHD as to fingerprint image quality and an appropriate message is displayed following each fingerprint image capture. Up to three attempts are allowed to capture a fingerprint of sufficient quality for AFIS processing. The data is sent via Bluetooth to the cutter where a server sends the data via a satellite link to US-VISIT. All data sent by the server and received by the server related to the searches is logged for audit and analysis purposes. The search record is sent to US-VISIT where it is checked against a recidivist database and a watchlist of outstanding wants and warrants. The server also has a store forward capability where all search requests and responses are managed so as to minimize total transaction time. The response, once received by the server, is forwarded to the MBHD indicating a

positive or negative identification. A photograph of the identified individual is included in the response. If a positive identification is received, the subject is brought aboard the cutter for later processing on-shore.

17. Stockton Police Department - *Field Capture Latent Pilot*

An officer is called to a scene of a crime. There has been a break-in and an attempted sexual assault. The suspect left through the rear door when he heard someone entering in the front of the house. In his hurry, he dropped a flashlight. The victim provides the officer a brief description of the suspect. The officer, who is trained in latent fingerprint capture, dusts the flashlight and discovers several fingerprints. Using a camera that is on his MBHD, the officer captures the latent fingerprint image. The officer enters the suspect descriptor data (sex, race, approximate age) and initiates a search of the local AFIS database. One of the latents is of good quality and two fingerprints are of lower quality. The search results in a rank one score on the good quality latent and a rank 8 and 10 on the other two latents. These scores are displayed as part of three candidate lists indicating State ID numbers and a photograph for the subjects identified by the search. The photograph is shown to the victim who positively identifies the suspect. At this time the officer posts a wants notice from his MBHD to the local and the State AFIS on the suspect. All data captured and processed by the MBHD is archived. The poor quality latents that did not produce a hit are manually encoded by a latent examiner using a lift obtained from the scene as part of the evidence collection process.

18. National Park Service

A National Park Service (NPS) officer finds an illegally camped individual who he suspects is an illegal alien. Upon questioning, the individual admits to being an illegal immigrant. The officer requests the individual to provide fingerprint (index fingers), iris, and facial biometric data for a search of the US-VISIT system. This data is captured on the MBHD which transmits the data via a USB cable to a patrol car computer (future upgrade to WiFi). Text data is also entered via the MBHD keyboard (or touchscreen). The entered data is searched against the US-VISIT system to determine if the individual is a recidivist. The US-VISIT search reveals that the subject has had prior deportations. Additional fingerprint data is captured to form a tenprint record and the data is enrolled in IDENT and is sent to IAFIS to determine if the subject has a criminal record. All of the captured data is also enrolled in US-VISIT and IAFIS. As part of the IAFIS enrollment process the enrolled ten-print data is searched against the unsolved latent database and the resulting candidates are compared through the FBI's Universal Latent Workstation (editor's note: this scenario is not fully developed – mention is made of two finger capture and tenprint enrollment, reverse search requires a ULW, however, data is sent to a patrol car computer. What happens to iris and facial data is not explained. Need clarification). A match signifies probable involvement in a criminal enterprise and the individual is targeted for further investigation and case development.

Table: Scenario to Use case Relationships

	Scenario	Use Case 1	Use Case 2	Use Case 3	Use Case 4	Use Case 5
1	Law Enforcement Patrol Activities - Variation A					
2	Law Enforcement Patrol Activities - Variation B					
3	Law Enforcement Public Event Disturbance					
4	POE Identity Verification					
5	POE Identity Verification - Fingerprint and Facial Image Identification MBHD					
6	At Sea Interdiction					
7	Maritime Interdiction Operation					
8	Disaster Site Operations					
9	First Responders Access Control					
10	Mobile Applications of TWIC					
11	Identification of Deceased					
12	Checkpoint Operations					
13	Joint Operation					
14	Detention Facility Operations					
15	Los Angeles County Sheriff's Department - Patrol Stop					
16	Interdiction at Sea					
17	Stockton Police Department - Field Capture Latent Pilot					
18	National Park Service					