System Assessment and Validation for Emergency Responders (SAVER)

Mobile Identification Fingerprint Devices Market Survey Report

January 2015

Homeland Security
Science and Technology

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

Prepared by Space and Naval Warfare Systems Center Atlantic

The *Mobile Identification Fingerprint Devices Market Survey Report* was funded under Interagency Agreement No. HSHQPM-13-X-00024 from the U.S. Department of Homeland Security, Science and Technology Directorate.

The cover image is courtesy of 3M™ Cogent, Inc., and Space and Naval Warfare Systems Center Atlantic. Photos used within the document are courtesy of 3M Cogent, Inc.; Advanced Livescan Technologies, Inc.; Corvus Integration, Inc.; Credence ID, LLC; Cross Match® Technologies, Inc.; Cyber Armed Security, LLC; DERMALOG® Identification Systems GmbH; Green Bit Biometric Systems, S.p.A.; InCadence Strategic Solutions; Integrated Biometrics, LLC; MorphoTrak®, LLC; MorphoTrust USA®, LLC; Secure Planet, Inc.; and Unisys® Corporation.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community. The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency response equipment; and
- Providing information, in the form of knowledge products, that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. As a SAVER Program Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic has been tasked to provide expertise and analysis on key subject areas, including communications, sensors, security, weapon detection, and surveillance, among others. In support of this tasking SPAWARSYSCEN Atlantic developed this report to provide emergency responders with information gathered during a market survey of commercially available mobile identification fingerprint devices, which fall under AEL reference number 05AU-00-BIOM titled Mobile Fingerprint Biometric Devices.

Visit the SAVER website on First Responder.gov (www.firstresponder.gov/SAVER) for more information on the SAVER Program or to view additional reports on mobile identification fingerprint devices or other technologies.

POINTS OF CONTACT

SAVER Program
U.S. Department of Homeland Security
Science and Technology Directorate
FRG Stop 0203
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@hq.dhs.gov
Website: www.firstresponder.gov/SAVER

Space and Naval Warfare Systems Center Atlantic
Advanced Technology and Assessments Branch
P.O. Box 190022
North Charleston, SC 29419-9022

E-mail: ssc_lant_saver_program.fcm@navy.mil

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Biometrics measure the physical and behavioral characteristics of individuals and assign a unique identity through automated methods. Physical characteristics include the anatomical components and physiological functioning of the human body, while behavioral characteristics describe the way an individual reacts or moves within the environment. Mobile fingerprint devices are used to determine or verify the identity of an individual encountered in the field. These devices capture fingerprint samples and create a template for comparison matching against existing fingerprint templates, or can be used to create new templates for later reference. These devices enable law enforcement to collect fingerprints at the scene of a crime, during traffic stops and at important locations, such as border crossings. Rapid fingerprint identification in the field can help identify deceased victims, prevent the unintended release of wanted individuals, and forewarn law enforcement officers when facing individuals with criminal records. To provide emergency responders with information on mobile identification (ID) fingerprint devices, the System Assessment and Validation for Emergency Responders (SAVER) Program conducted a market survey.

This market survey report is based on information gathered from February to June 2014 from vendors, Internet research, industry publications, and a government issued Request for Information (RFI) that was posted on the Federal Business Opportunities website. For inclusion in this report, mobile ID fingerprint devices had to meet the following criteria:

- Incorporate the use of a mobile ID fingerprint scanner listed in the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Information System (IAFIS) Certified Product List; and
- FBI certification at fingerprint acquisition profile (FAP) 30 or above.

Due diligence was performed to develop a report that is representative of products in the marketplace.

2. MOBILE ID FINGERPRINT DEVICES OVERVIEW

Mobile ID fingerprint devices can capture fingerprints taken by a sensor with the subject present (i.e., livescan), as shown in Figure 2-1. Latent fingerprints are taken from surfaces that an individual has touched and typically require treatment with powders and chemicals to enhance visibility before photos can be taken and digitized.

Figure 2-1. Mobile ID Fingerprint Capture

Image courtesy of MorphoTrust USA, LLC

Mobile ID fingerprint devices typically perform three principle functions:

Verification (authentication): A one-to-one comparison can be made between an individual's livescan captured fingerprint template and a stored fingerprint template from a biometric reference in order to confirm an individual's claimed identity.

The reference template may reside on an issued credential, such as a personal identity verification (PIV) card, or in a centralized database.

Identification: A one-to-many matching process is used to identify an unknown person. The captured fingerprints are compared to all records in an automated fingerprint identification system (AFIS) database.[1] An AFIS database offers electronic storage, search capabilities, and exchange of fingerprint references.

Enrollment: Some mobile ID fingerprint devices provide the ability to enroll a person in an AFIS database while in the field rather than require transport to a traditional booking location. Typically, the enrollment process includes the capture and storage of high-quality fingerprint samples from each finger and thumb, as shown in Figure 2-2, in addition to other biometric and biographical information. The time to complete these tasks and maintain a suspect's compliance in an uncontrolled environment may be limiting factors for field enrollment, but will depend on an agency's mission requirements.

Figure 2-2. Mobile ID Enrollment

Image courtesy of Cross Match Technologies, Inc.

Fingerprint matching remains the primary biometric mode of identification used by the law enforcement community. However, many mobile ID fingerprint devices now offer multiple types of biometrics capture, such as facial and iris capture. These devices are called multi-modal. Accessory components may also be available, such as card, bar code, and passport readers that can serve as additional means to verify a person's identity and increase the reliability of a match.

2.1 Mobile ID Fingerprint Device Components

A mobile ID fingerprint device is often an all-in-one handheld unit that includes an embedded fingerprint scanner to capture samples, in addition to the computer processor, memory, user interface, communications module, and any other hardware/software required for the device to operate. In other cases, a portable, peripheral-based system may be used where the fingerprint scanner is separate from the other hardware and software. For example, it may be connected by a USB to an in-vehicle laptop computer or tablet. The following sections describe the typical mobile ID fingerprint device components required for either type of system.

2.1.1 Fingerprint Scanners

All livescan mobile ID fingerprint devices require a fingerprint scanner, also referred to as a capture device. The scanner includes a sensor to capture images of the friction ridges on an individual's fingers, and a flat surface called a platen to place fingers for scanning. There are a variety of sensor types, with optical being the most common. Scanners that use optical sensors take an image of the fingerprint and may or may not be appropriate for use in direct light. Some

[1]Different AFIS databases may be structured to search all records, or to search specific segments; however, the increased speed of limited searches may diminish matching accuracy.

optical sensors include a membrane on the platen to improve image capture for dry fingers. Membrane materials may include silicon pads, epoxy, and urethane coatings. Additionally, another type of sensor has been developed that captures fingerprint samples using a thin film transistor that is unaffected by different lighting environments.

The FBI classifies mobile ID fingerprint scanners with an FAP rating that ranges from 10 to 60. Higher FAP numbers indicate expanded scanner capabilities, such as the capture of more than one fingerprint sample at a time. Fingerprint scanners certified by the FBI may be available on the market in three forms:

- An embedded part of a handheld unit;
- A separate peripheral; or
- An original equipment manufacturer (OEM) product, which can be purchased for integration into another company's mobile ID device.[2]

Mobile ID scanners must be able to capture samples called flat impressions.[3] Flat impressions result from touching a finger to a livescan platen without any rolling motion. Some scanners also have the ability to capture impressions where the finger is rolled from one edge of the nail to the other, but rolled impressions are not required by current mobile ID standards. Mobile ID standards are discussed in more detail in Section 3. A principal feature of these scanners is the ability to automatically capture and assess the quality of the fingerprint samples, minimizing the need for operators with extensive professional training in fingerprinting.

2.1.2 Latent Print Camera

Some mobile ID fingerprint devices are equipped with a camera capable of collecting images of latent prints from active crime scenes. Figure 2-3 shows an image of a latent print displayed by a software application that determines its quality.

Latent print images may be captured and submitted to AFIS databases for identification. A few mobile ID fingerprint devices also offer software applications that can provide onboard analysis; however, latent print examiners are needed to confirm positive matches.

Figure 2-3. Latent Print

Courtesy of 3M Cogent

2.1.3 Electronic Hardware

A mobile ID fingerprint device uses typical computer hardware, such as a processor, memory, user interface, and alert indicators (e.g., colored lights, sounds, or vibration capability), to guide the operator through the collection of fingerprints and subsequent actions. The mobile ID fingerprint device may house all hardware components, or use an intermediary host, such as an in-vehicle computer, smartphone, or tablet, to perform specific functions.

[2]FBI Certified Product List is available at https://www.fbibiospecs.org.
[3]Flat fingerprint impressions may also be called plain. When all four fingers of one hand are simultaneously captured, this is referred to as a slap.

2.1.4 Communications Module

A communications module may be incorporated into a mobile ID fingerprint device to transmit captured fingerprints to an intermediary host or remote AFIS databases for comparison matching. A communications module may offer wireless technologies such as Wi-Fi®, Bluetooth®, and satellite and cellular communications, as well as wired options such as Ethernet or USB. Additionally, GPS may be used to tag the geographic location and timestamp of fingerprint samples taken in the field. Prior to purchase, agencies should consider whether wireless connectivity to internal network resources conflicts with departmental policies or poses security concerns.

2.1.5 Software Applications

Mobile ID fingerprint devices may include software applications for performing verification, identification, and enrollment. Common functions and features include:

- **Fingerprint processing:** captures and processes samples (e.g., assesses their quality and extracts distinguishing features);
- **Compression and transmission:** facilitates the standardized exchange of fingerprint images among different AFIS databases;[4]
- **Security:** authenticates the operator, and encrypts and prevents unauthorized access to fingerprint images and biographical information;
- **Database management and matching:** stores captured fingerprints, compares any reference records available if the mobile ID fingerprint device has an onboard database, and may make match/non-match decisions according to pre-set thresholds; and
- **Graphical user interface (GUI):** presents instructions on operating the mobile ID fingerprint device, displays images of captured fingerprints, and instantly assesses image quality of the sample. The GUI may show any available biographical information (e.g., mug shots) when a match occurs. It also allows the operator to enter data and adjust display features.

Many vendors offer software toolsets called software development kits (SDKs) that aid in integrating mobile ID fingerprint devices and applications for other biometrics, such as facial and iris recognition, into a single system framework. Mobile ID fingerprint devices may use software that functions on one or more operating systems, such as Microsoft Windows®, Linux®, and Apple® Mac OS X®, or mobile operating systems like Google Android™ and Apple iOS®.

2.2 Mobile ID Task Distribution

Mobile ID fingerprint devices vary in their capacity and method to complete the primary tasks of fingerprint capture, image processing, matching, and decision-making. As shown in Figure 2-4, a mobile ID fingerprint device may perform all tasks as a stand-alone system, or the workload may be split with a system accessed over a network (i.e., remote AFIS). The cloud represents a network connection to an AFIS.

[4]The Wave Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Algorithm is the standard for the exchange of 500 pixels per inch fingerprint images within the criminal justice community.

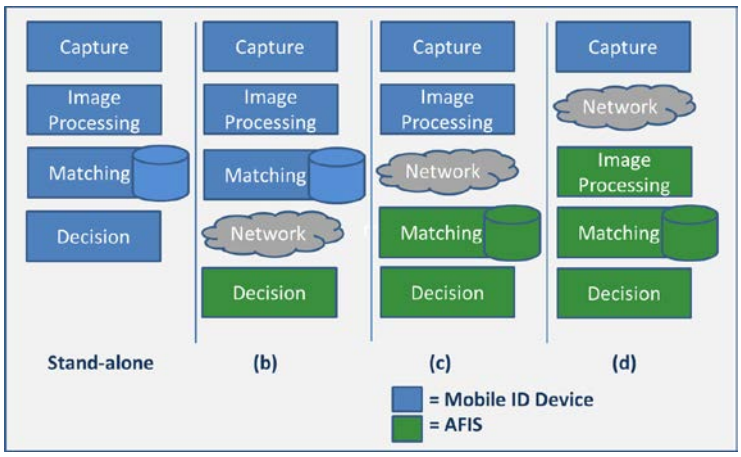

Figure 2-4. Mobile ID Task Distribution

Image Courtesy of Scientific Research Corporation

A mobile ID fingerprint device performing as a stand-alone system may be useful for rapid, localized searches. However, access to remote AFIS databases can offer wider search capabilities and decision support.

2.3 AFIS Databases

Mobile ID fingerprint devices may include an onboard database of fingerprint reference records, and/or the device may remotely access and submit queries to AFIS databases. AFIS databases vary widely in size and interoperability. Local and state law enforcement agencies may implement their own AFIS databases and use them exclusively, or join larger, networked systems that extend to the regional, national, or international level. Typically, searches begin at the local level and progress, as needed, to larger systems. Response time for queries will vary according to the mobile ID fingerprint device and AFIS used, but some law enforcement agencies report that identification can require as little as 30 seconds.

Three of the primary Federal AFIS databases are:

- **FBI IAFIS:** the largest criminal fingerprint database in the world. It houses the fingerprint records and criminal histories of nearly 76 million individuals and over 39 million civil prints. It provides automated livescan and latent print search capabilities, electronic image storage, and exchange of fingerprint images.
- **FBI Next Generation Identification (NGI) project:** an incremental expansion of IAFIS that provides greater efficiency in fingerprint query and matching transactions. Criminal queries are given search priority. It also includes biographical information, palm prints, and latent prints.[5] NGI will soon incorporate facial and iris biometric record-matching capability.

[5]The FBI CJIS provides the Universal Latent Workstation (ULW) software for improved exchange and search of latent friction ridge images. This software is offered free of charge to authorized criminal justice agencies at https://www.fbibiospecs.org/Latent/LatentPrintServices.aspx.

- **Repository of Individuals of Special Concern (RISC):** a subset of the IAFIS, RISC includes records for wanted persons, registered sex offenders, known or suspected terrorists, and other persons of national interest.
- **DHS Automated Biometric Identification System (IDENT):** a DHS-wide system for storage, processing, and comparison of biometric information for immigration control, border security, law enforcement, intelligence, and national security. IDENT adheres to FBI IAFIS standards and offers interoperable search capabilities. In the future, IDENT will receive criminal fingerprint records submitted by law enforcement agencies to the FBI IAFIS.[6]
- **Department of Defense (DoD) Automated Biometric Identification System (ABIS):** the central multi-modal biometric database system of the DoD. ABIS is interoperable with the FBI IAFIS and DHS IDENT.[7]

2.4 Applications

Mobile ID fingerprint devices can aid in the capture of wanted criminals. In a pilot project conducted from September 2011 to January 2012, ten law enforcement agencies in Texas using the devices demonstrated that out of 320 fingerprint submissions, 60 resulted in positive identification and provided reason to detain suspects.[8] Three of those matches were from the FBI RISC database that includes wanted persons and those of national interest.

Law enforcement officers have reported that simply presenting mobile ID fingerprint devices to uncooperative suspects can lead to true-identity admissions prior to any fingerprint collection, or can elicit truthful responses from suspects once positively identified. The San Bernardino County Sheriff's Department reduced the number of people who provided false identification from 701 to 3 after the first year using mobile ID fingerprint devices.[9]

Identification in the field can save time and money associated with transporting a suspect to a location with scanning capability and make efficient use of imposed time limits for detaining suspects without additional cause.

Additionally, law enforcement agencies such as the Stockton Police Department of California participated in a pilot project for latent fingerprint image capture, using mobile ID fingerprint devices. Latent prints were captured at crime scenes to identify persons of interest in near-real time and reduce the time needed to develop leads.

[6]This FBI/DHS information-sharing partnership is called Secure Communities and is mandated by Federal law. http://www.ice.gov/secure_communities.
[7]"Biometric Interoperability," Criminal Justice Information Services Division, November 2011. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/facial-recog-forum-110211b.pdf.
[8]"Mobile Biometric Device (MBD) Technology: Summary of Selected First Responder Experiences in Pilot Projects," Sandia National Laboratories, June 2013.
[9]"Landscape Study of Mobile ID Fingerprint Devices," Forensic Technology Center of Excellence, January 2014.

3. STANDARDS AND INTEROPERABILITY

Livescan fingerprint matching is primarily automated, which makes well-defined standards and specifications essential for interoperability. A reliable match between fingerprints sent by a mobile ID fingerprint device and biometric references stored in a remote AFIS depends heavily on image quality, as well as the processing and transmission methods accepted by the specific AFIS.

Figure 3-1. Fingerprint Features

Image courtesy of Integrated Biometrics, LLC

Current Federal standards and best practices promote vendor-agnostic, non-proprietary solutions that allow for greater interoperability among different AFIS databases. When accessing remote AFIS databases, the transmission of fingerprint images is often preferred to processed templates. Templates are algorithm-derived files of mathematical codes that correspond to specific extracted fingerprint ridge features. An example of feature extraction is shown in Figure 3-1. Templates typically allow for faster processing time and require less storage space, but the fingerprint processing software (e.g., algorithms used) on a mobile ID fingerprint device may not extract and highlight the same features as those processed by another system. This can cause matching errors among different AFIS databases. Images offer the entire fingerprint for feature extraction and promote matching repeatability when exchanged between different systems, but in turn, require significant security measures to protect the fingerprint data.

3.1 U.S. Fingerprint Standards

Two of the primary organizations that provide detailed fingerprint standards are as follows:

- **American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST)**: provides the basis for most U.S. Government biometric standards. The special publication, ANSI/NIST–Information Technology Laboratory (ITL) 1-2011: update 2013, includes the requirements for the electronic exchange of fingerprints. http://biometrics.nist.gov/cs_links/standard/ansi_2012/Update-Final_Approved_Version.pdf
- **FBI Criminal Justice Information Services (FBI CJIS):** maintains the Electronic Biometric Transmission Specification (EBTS) for submitting fingerprints for enrollment and queries to IAFIS. The EBTS 10.0 version July 2013 uses the ANSI/NIST–ITL standards in addition to CJIS-specific requirements. https://www.fbibiospecs.org/ebts.html

3.2 Mobile ID Fingerprint Acquisition Profile

ANSI/NIST and the FBI classify mobile ID fingerprint scanners with a fingerprint acquisition profile (FAP) based on the following:

- Scanner capture area dimensions;
- Image quality specifications (IQS); and

- Number of fingerprint impressions captured simultaneously.[10]

The FBI further categorizes mobile ID fingerprint scanners as follows:

- PIV-071006: a certification standard for scanners designed to primarily support one-to-one verification; and
- Appendix F: a certification standard with strict image quality requirements for scanners that can support large-scale, one-to-many matching.

Table 3-1 details the FAP requirements. Single finger scanners have an FAP rating of 30 or below, and are primarily used for verification and identification. Scanners of FAP 40 and above may be used for enrollment, as well as one-to-one and one-to-many searches. They are capable of capturing more than one finger simultaneously and typically include the option to collect rolled impressions as well as the required flat impressions. However, rolled impressions capability is not required for mobile ID.

Table 3-1. FAP Requirements

FAP	IQS Requirement	Capture Area Dimensions[1]	Fingers Captured Simultaneously[2]	Image Resolution Minimum	Rolled Impression
FAP 10	PIV-071006	0.5 x 0.65	1	500 ppi	No
FAP 20	PIV-071006	0.6 x 0.8	1	500 ppi	No
FAP 30	PIV-071006	0.8 x 1.0	1	500 ppi	No
FAP 40	PIV-071006	1.6 x 1.5	1-2	500 ppi	Optional
FAP 45	Appendix F	1.6 x 1.5	1-2	500 ppi	Optional
FAP 50	Appendix F	2.5 x 1.5	1-3	500 ppi	Optional
FAP 60	Appendix F	3.2 x 3.0	1-4	500 ppi	Optional

Notes:
[1]Width by height in inches
[2]Flat impressions

The FBI provides an IAFIS Certified Product List (CPL) for mobile ID fingerprint scanners that have been tested and are in compliance with the IQS for the capture of friction ridge images. Testing assesses image quality, so other standards and specifications may still need to be met. FAP certification from the FBI ensures interoperability with the IAFIS database.

[10]The number of fingers used and the amount of data captured for each finger significantly affects the overall system accuracy. "NIST Special Publication 500-280: Mobile ID Device Best Practice Recommendation," Version 1.0, NIST, July 2009.

4. EMERGING TECHNOLOGIES

Manufacturers of mobile ID fingerprint devices are increasingly using smartphones and tablets in conjunction with biometric modules to capture fingerprints and other biometric data while in the field. The biometric modules may be integrated or snapped onto a mobile device, or be peripheral-based. Figure 4-1 shows a peripheral fingerprint scanner and commercial-off-the-shelf (COTS) tablet running a fingerprint collection application. Most operators are familiar with these mobile platforms, which reduces training time and promotes ease of use. These devices typically function in different lighting environments, maintain adequate battery life, and offer multiple data transmission options.

Figure 4-1. Fingerprint Application

Image courtesy of InCadence Strategic Solutions

Fingerprint scanning technology continues to advance in multiple ways, including image capture unaffected by lighting environment, spoofing detection of fake fingerprints, and liveness detection. Liveness detection ensures a pulse is associated with the captured fingerprint sample to prevent exploitation.

5. PRODUCT INFORMATION

This section provides general product specifications on fingerprint scanners certified by the FBI as FAP 30 and above. FBI IAFIS IQS certification ensures fingerprint scanners meet or exceed minimum image quality specifications and are interoperable with IAFIS.[11] The section includes 13 handheld mobile ID fingerprint devices, 11 peripheral scanners, and 4 mobile fingerprint collection platforms. The tables in this section are organized as follows:

- Table 5-1 and Table 5-2 provide information on integrated handheld units;
- Table 5-3 provides information on peripheral fingerprint scanners; and
- Table 5-4 includes examples of biometric collection platforms using COTS mobile devices in combination with FBI certified fingerprint scanners.

Handheld devices range in price from $1,299 to $16,800, and vary widely in capability. Peripheral devices range in price from $315 to $800, and collection platforms that include the fingerprint scanner and software, but not the host device range in price from $539 to $989. Specifications presented in Tables 5-1 to 5-4 were obtained directly from vendors and/or specified distributors in an RFI and from Internet and industry publication research. The information has not been independently verified by the SAVER Program. Clarifications on

[11] Appearance on the FBI's certified product list is not, and should not be construed as, an endorsement, nor should it be relied upon for any requirement beyond IQS. Users should contact their State CJIS Systems Officer (CSO) or Information Security Officer (ISO) to ensure compliance with the necessary policies and/or guidelines.

certain specifications in Tables 5-1 to 5-4 are provided below under Biometric Capture, General Specifications, Transmission, and Fingerprint Records and Processing in alphabetic order.

5.1 Biometric Capture

Add-Ons: refers to available or included accessories (e.g., printer, audio recorder, or credential reader). Credential reader may refer to a 1-D or 2-D bar code reader, machine readable zone (MRZ) swipe reader often used for passports, or a contact/contactless smartcard.

Auto Capture: refers to the ability to assess and save captured fingerprints automatically.

FAP: refers to a rating based on a standardized set of mobile ID fingerprint acquisition requirements that assign a number from 10 to 60, according to capability.

Fingerprints: refers to the type of fingerprint impressions that can be collected by the device.

Manual Capture: refers to a feature allowing the operator to override the device to capture and accept an image that may not be of set threshold quality. This feature is useful in situations where samples are repeatedly rejected, such as from dry fingers.

Multi-Modal: refers to the ability to capture more than one type of biometric modality or latent prints in addition to livescan fingerprints.

Sensor Type: refers to the type of sensor the fingerprint scanner uses to capture images.

Simultaneous Capture: refers to the number of fingers that can be captured on the platen at once.

5.2 General Specifications

Adaptors and Chargers: refers to available battery adaptors and chargers for the device. An alternating current (AC) charger/adaptor provides electricity to a rechargeable battery in the appropriate form. A docking station (cradle) may be an AC charger. AC input with direct current (DC) output provides increased voltage, but maintains the low current needed to operate the device. A USB charger is a cable that connects the device to a computer's 5-Volt USB port to recharge the battery by a computer.

Hot Swap Capability: refers to the ability to remove/replace the battery without loss of stored data or programs.

Ingress Protection Rating (IP Rating): refers to a product's resistance to dust and liquids. The first number of the IP rating refers to protection from solid objects and ranges from 0 (no protection) to 6 (full protection). The second number refers to liquid protection and ranges from 0 (no protection) to 8 (protection against long periods of immersion and pressure). Refer to Appendix A for more information on IP rating.

Relative Humidity Range (%): refers to the acceptable environmental humidity level within which the device can operate—where water vapor will not condense to liquid form and render the device inoperable.

5.3 Transmission

These specifications refer to the transmission options available in the device's communication module, such as Bluetooth, cellular, Wi-Fi, satellite communications, and GPS. Wired options, such as Ethernet or USB 2.0, are also available.

FIPS 140-2 Certification: indicates whether the encryption software meets Federal Information Processing Standards (FIPS) authentication requirements.

Requires Host: refers to an intermediary device needed to process, transmit, and/or store the captured fingerprint samples. Connection to a host device may be wireless or through USB.

5.4 Fingerprint Records and Processing Specifications

FIPS 201 Certification: refers to a product meeting Federal PIV standards for credential systems, such as smart cards.

Match Result Display: refers to the types of information available, such as mug shots and biographical data, to display for potential return matches. If accessing a remote AFIS, return information may vary.

Memory: refers to the memory capacity for device operation.

Onboard Matching: refers to the capability to compare the captured fingerprints against stored reference records on the device.

Storage: refers to the amount of data, made up of fingerprint reference records, that can be stored onboard the device. Note: A fingerprint reference record may include images and/or templates. The record may also vary in number of samples and type of impressions (i.e., flat or rolled) included.

Typical Match Speed: refers to the typical speed (matches per second) that an onboard database compares captured fingerprints to onboard reference records. Note: a record may vary in the number of fingerprints included.

WSQ Compression: refers to the Wave Scalar Quantization (WSQ) gray-scale fingerprint image compression algorithm—the standard for the exchange of 500 pixels per inch fingerprint images within the criminal justice community.

Table 5-1. Handheld Mobile ID Fingerprint Devices

Vendor: 3M Cogent	Product: Mobile Ident III (MI3)	
 MSRP: $2,790 • *Click on product name to view additional product information in Table 5-2.	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Multi-Modal:** Facial, Voice **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** Credential reader, docking station	**Weight:** 1.4 pounds **Dimensions (in.):** 7.8 (L) x 3.5 (W) x 2.5 (H) **Display:** 3.5 in. color QVGA LCD backlit touchscreen **Keypad:** Yes **Brightness Adjustment:** Yes **IP Rating:** 65 **Operating Temperature (ºF):** 14 to 122 **Battery Type:** Li-ion 4.2 Volt, 4400 mAh **Hot Swap Capability:** Yes
	Transmission	**Fingerprint Records & Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes	**Storage:** 300,000 records **Onboard Matching:** Yes **Typical Match Speed:** 1,200/sec **Match Result Display:** Alert message, biographical data, face photo **Operating Systems**: Windows CE and Windows Mobile **FIPS 201 Certification:** Yes **WSQ Compression:** Yes
Vendor: 3M Cogent	**Product: Fusion**	
 MSRP: $4,199	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat, Latent **Simultaneous Capture:** 1 **Multi-Modal:** Facial, Iris **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** None	**Weight:** 1.2 pounds **Dimensions (in.):** 8.7 (L) x 4.6 (W) x 2.9 (H) **Display:** 3.5 in. color QVGA LCD backlit touchscreen (option) **Keypad:** Yes **Brightness Adjustment:** Yes **IP Rating**: 65 **Operating Temperature (ºF)**: 14 to 122 **Battery Type**: Li-ion 4.2 Volt, 4400 mAh **Hot Swap Capability**: Yes
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host**: No **FIPS 140-2 Certification:** Yes	**Storage:** 100,000 records **Onboard Matching:** Yes **Typical Match Speed:** 1,200/sec **Match Result Display:** Alert message, biographical data, face photo, text **Operating Systems**: Linux **FIPS 201 Certification:** N/A **WSQ Compression:** Yes

Refer to table notes on page 17.

Vendor: Credence ID Distributor: Unisys Corporation	Product: Trident	
 MSRP: $3,627	**Biometric Capture**	**General Specifications**
	FAP: 45 **Fingerprints:** Flat, Rolled, Latent **Simultaneous Capture:** 2 **Multi-Modal:** Facial, Iris **Sensor:** Thin Film Transistor **Auto Capture:** Yes **Manual Capture:** Yes **Add-Ons:** Credential reader, external battery	**Weight:** 2.75 pounds **Dimensions (in.):** 10.4 (L) x 6.6 (W) x 3.5(H) **Display:** 5.0 in. LCD touch panel **Keypad:** Capacitive 5-point, multi-touch panel **Brightness Adjustment:** Yes **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 122 **Battery Type:** 1 Li-ion 10,000 mAh **Hot Swap Capability:** No
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes	**Storage:** 250,000 records **Onboard Matching:** Yes **Typical Match Speed:** 3,000/sec **Match Result Display:** Alert message, biographical data, face photo **Operating Systems:** Android 4.1.2 **FIPS 201 Certification:** Yes **WSQ Compression:** Yes

Refer to table notes on page 17.

Vendor: Corvus Biometrics	Product: Unity	
 MSRP: $7,500	**Biometric Capture**	**General Specifications**
	FAP: 45 **Fingerprints:** Flat, Rolled, Latent **Simultaneous Capture:** 2 **Multi-Modal:** Facial, Iris, Voice **Sensor Type:** Thin Film Transistor **Auto Capture:** Yes **Manual Capture:** Yes **Add-Ons:** Credential reader/writer, videostreaming, extra battery	**Weight:** 30 ounces **Dimensions (in.):** 7.2 (L) x 4.2 (W) x 2.9 (H) **Display:** 5.0 in. color LCD TFT, backlit **Keypad:** Touchscreen **Brightness Adjustment:** Yes **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 120 **Battery Type:** Li-ion 6,000 mAh **Hot Swap Capability:** Yes
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: No **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes	**Storage:** DoD BEWL[12], 100,000 + records **Onboard Matching:** Yes **Typical Match Speed:** 100K/sec **Match Result Display:** Alert message, biographical data, face photo **Operating Systems:** Windows 7 and 8 **FIPS 201 Certification:** No[13] **WSQ Compression:** Yes
Vendor: CrossMatch Technologies	**Product: Seek II**	
 MSRP: $16,800	**Biometric Capture**	**General Specifications**
	FAP: 45 **Fingerprints:** Flat, Rolled, Latent **Simultaneous Capture:** 2 **Multi-Modal:** Facial, Iris **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** Credential reader, voice capture	**Weight:** 3.6 pounds **Dimensions (in.):** 8.8 (L) x 5.5 (W) x 3.5 (H) **Display:** 4.1 in. backlit touchscreen **Keypad:** Yes **Brightness Adjustment:** Yes **IP Rating:** IP 65 **Operating Temperature (ºF):** 35 to 120 **Battery Type:** 2 Li-ion 2.4 Ah **Hot Swap Capability:** Yes
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes **WSQ Compression:** Yes	**Storage:** 120,000+ records **Onboard Matching:** Yes **Typical Match Speed:** 2,500/sec **Match Result Display:** Alert message, biographical data, face photo **Operating Systems:** Windows XP SP3 and Windows 7 **FIPS 201 Certification:** Yes

Refer to table notes on page 17.

[12]DoD Biometrically Enabled Watchlist (BEWL)
[13]Currently, the Unity is FIPS 201 compliant, awaiting certification, using vendor components and software with FIPS 201 certification.

Vendor: CrossMatch Technologies	Product: Seek Avenger	
 MSRP: $10,800	**Biometric Capture**	**General Specifications**
	FAP: 45 **Fingerprints:** Flat, Rolled, Latent **Simultaneous Capture:** 2 **Multi-Modal:** Facial, Iris **Sensor Type:** Thin Film Transistor **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** Credential reader	**Weight:** 3.2 pounds **Dimensions (in.):** 9.5 (L) x 6.2 (W) x 1.8 (H) **Display:** 5.0 in. resistive backlit touchscreen **Keypad:** Yes **Brightness Adjustment:** Yes **IP Rating:** 65 **Operating Temperature (ºF):** 35 to 120 **Battery Type:** 2 Li-ion 2.9 Ah **Hot Swap Capability:** Yes
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes	**Storage:** 250,000 records **Onboard Matching:** Yes **Typical Match Speed:** 2,500/sec **Match Result Display:** Alert message, biographical data, face photo **Operating Systems:** Windows 7 Ultimate **FIPS 201 PIV:** Yes
Vendor: CrossMatch Technologies	**Product: Verifier Mw**	
 MSRP: $2,199	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Multi-Modal:** No **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** Holster	**Weight:** 1.4 pounds **Dimensions (in.):** 8.0 (L) x 1.9 (W) x 1.9 (H) **Display:** 2.0 in. TFT color LCD **Keypad:** Push button controls **Brightness Adjustment:** No **IP Rating:** 65 **Operating Temperature (ºF):** 32 to 105 **Battery Type:** 1 Li-ion 2 Ah **Hot Swap Capability:** No
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** No **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** No **Requires Host:** Portable/mobile computer **FIPS 140-2 Certification:** No	**Storage:** 10 records **Onboard Matching:** No **Typical Match Speed:** N/A **Match Result Display:** On host **Operating Systems:** Linux **FIPS 201 Certification:** Yes **WSQ Compression:** No

Refer to table notes on page 17.

Vendor: MorphoTrak	Product: HIIDE 5	
 MSRP: $15,622	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat, Latent **Simultaneous Capture**[14]**:** 1 **Multi-Modal:** Facial, Iris **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Add-Ons:** Credential reader, external battery	**Weight:** 3.25 pounds **Dimensions (in.):** 8.0 (L) x 3.0 (W) x 5.0 (H) **Display:** 5.0 in. touchscreen **Keypad:** Touchscreen **Brightness Adjustment:** Yes **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 122 **Battery Type:** 2 Li-ion 7.2 Volt, 2.4 Ah **Hot Swap Capability:** Yes
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: No **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** No **FIPS 140-2 Certification:** Yes	**Storage:** 1.5 million records **Onboard Matching:** Yes **Typical Match Speed:** 2,000/sec **Match Result Display:** Demographics, face photo, BEWL search results **Operating Systems:** Windows XP **FIPS 201 Certification:** Yes **WSQ Compression:** Yes
Vendor: MorphoTrak and MorphoTrust USA	**Product: IBIS Extreme**	
 MSRP: $1,800	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Multi-Modal:** No **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** None	**Weight:** 0.99 pounds **Dimensions (in.):** 9.7 (L) x 2.6 (W) x 2.5 (H) **Display:** No **Keypad:** No **Brightness Adjustment:** N/A **IP Rating:** 54 complaint (uncertified) **Operating Temperature (ºF):** 32 to 104 **Battery Type:** 4 NiMH rechargeable 1.2 Volt **Hot Swap Capability:** No
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Through aircard or PDA **Wi-Fi:** No **USB/Wired:** No **GPS:** No **Requires Host:** Windows PC/laptop, Android PDA **FIPS 140-2 Certification:** Yes	**Storage:** 10 records **Onboard Matching:** No **Typical Match Speed:** N/A **Match Result Display:** On host **Operating Systems:** Windows XP/6.5 or 7, Android **FIPS 201 Certification:** No **WSQ Compression:** Yes

Refer to table notes on page 17.

[14]HIIDE 5 has the capability to capture two simultaneous prints; however, its scanner is FBI certified for single capture.

Vendor: MorphoTrak	Product: BA500	
 MSRP: $1,875	**Biometric Capture**	**General Specifications**
	FAP: 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Multi-Modal:** Facial **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** No **Add-Ons:** Credential reader	**Weight:** 15.8 ounces **Dimensions (in.):** 9.7 (L) x 2.6 (W) x 2.5 (H), hood extends 0.75 **Display:** 3.5 in. backlit touchscreen **Keypad:** Yes **Brightness Adjustment:** Yes **IP Rating:** 54 (host) **Operating Temperature (ºF):** 32 to 104 **Battery Type:** Li-ion 3.7 Volt, 3,600 mAh **Hot Swap Capability:** No
	Transmission	**Fingerprint Records and Processing**
	Bluetooth: Yes **Cellular:** Yes **Wi-Fi:** Yes **USB/Wired:** Yes **GPS:** Yes **Requires Host:** MC75A Enterprise Digital Assistant **FIPS 140-2 Certification:** Yes	**Storage:** 200,000 records **Onboard Matching:** Yes **Typical Match Speed:** 3,300/sec **Match Result Display:** AFIS dependent **Operating Systems:** Windows Mobile 6.5 **FIPS 201 Certification:** No **WSQ Compression:** Yes

Notes:
Battery Type: Lithium ion (Li-ion)
Nickel Metal Hydride (NiMH); ampere-hour (Ah); Milli-ampere hours (mAh)
N/A: Not applicable
NP: Information not provided by vendor

Information in this table is based on data gathered from vendors and their websites from February to June 2014.

Table 5-2. Handheld Mobile ID Fingerprint Device Supplemental Specifications

Vendor and Product	Processor	Memory	Storage	Storage Temperature Range (°F)	Relative Humidity Range	Continuous Hours of Operation	Adaptors and Chargers	Warranty Period
3M Cogent **Mobile Ident III (MI3)** *Click on product name to view additional product information in Table 5-1	Marvell PXA310	DDR SDRAM: 128MB (supports up to 256MB)	Flash: 128MB (stores up to 256) Expansion Slot: 8GB std. 16GB MicroSD (option)	-13 to 149	10 - 90	8+	Wall and vehicle chargers, ethernet cradle, and USB cable	1 year
3M Cogent **Fusion**	Marvell PXA310	DDR SDRAM: 128MB (supports up to 256MB)	Flash: 128MB (stores up to 256)	-13 to 149	10 - 90	8+	Wall and vehicle chargers, USB cable	1 year
Credence ID **Trident**	Qualcomm Snapdragon S4 Pro Quad-Core 1.7 GHz Cortex-A9 ARM	RAM: 2GB DDR3	Flash: 16GB eMMC (64GB option)	14 to 122	10 - 90	8	120V to 240V, 5V DC, USB	1 year (parts & labor)

Vendor and Product	Processor	Memory	Storage	Storage Temperature Range (°F)	Relative Humidity Range	Continuous Hours of Operation	Adaptors and Chargers	Warranty Period
Corvus Biometrics **Unity**	Intel Atom Dual core 64 bit 1.8 GHz	RAM: 4GB	256GB	32 to 120	0 - 90	4-6	90 to 260V AC, 24V, 2.5A DC	1 year
CrossMatch **SeekII**	Intel Atom Z530, 1.6 GHz	DRAM: 2GB	64GB	28 to 160	10 - 95	6	AC, 48V to 12V DC, USB	1 year Ltd./Ext. option
CrossMatch **Seek Avenger**	Intel Atom N2600 Dual Core 1.6 GHz	2GB DRAM (4GB option)	32GB (64GB option)	28 to 160	10 - 95	8	AC, 48V to 12V DC, USB	1 year Ltd./Ext. option
CrossMatch **Verifier Mw**	Marvell PSA 270	SD RAM: 64MB	SD Card 1GB	-10 to 140	10 - 95	8	AC, 12V DC, USB	1 year Ltd./Ext. option
MorphoTrak **HIIDE 5**	Intel Atom 1.6 GHz	DDR2 SDRAM: 2GB	80GB SSD (120GB option)	NP	NP	8	100 to 240V AC 12V DC	1 year

Vendor and Product	Processor	Memory	Storage	Storage Temperature Range (°F)	Relative Humidity Range	Continuous Hours of Operation	Adaptors and Chargers	Warranty Period
MorphoTrak & MorphoTrust **IBIS Extreme**	ARM Processor	NP	NP	4 to 120	10 - 90	8+	External connectors: 12 VDC	1 year
MorphoTrak **BA500**	Marvell PXA320, 800 MHz	RAM: 256MB	Flash: 1GB 32GB option	4 to 120	10 - 90	NP	Powered through MC75A Enterprise Digital Assistant	1 year

Notes:
N/A: Not applicable
NP: Information not provided by vendor
VDC: Volts direct current

Information in this table is based on data gathered from vendors and their websites from February to June 2014.

The peripheral fingerprint scanners listed in Table 5-3 require host devices, such as smartphones, tablets, or laptops, for operation. Typically, vendors have SDKs available for integration with host devices. Scanner capability to perform verification, identification, and enrollment may be determined by FAP rating and available software applications. Platforms that use peripheral devices may be available as kits and include a ruggedized suitcase.

Table 5-3. Peripheral Mobile ID Fingerprint Scanners

Vendor: 3M Cogent	Product: CSD330
 MSRP: $315	**Fingerprint Scanner Specifications** **FAP:** 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 0.64 pounds **Dimensions:** 3.8 (L) x 2.7 (W) x 2.0 (H) **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 131 **Storage Temperature (ºF):** 4 to 140 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP, 7, and 8 **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Adjustable brightness
Vendor: 3M Cogent	**Product: CSD450**
 MSRP: $480	**Fingerprint Scanner Specifications** **FAP:** 40 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 1.0 pounds **Dimensions:** 4.5 (L) x 2.6 (W) x 2.8 (H) **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 131 **Storage Temperature (ºF):** -4 to 140 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP, 7, and 8 **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Adjustable brightness
Vendor: 3M Cogent	**Product: CSD450f**
 MSRP: $574	**Fingerprint Scanner Specifications** **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 0.88 pounds **Dimensions:** 3.9 (L) x 3.3 (W) x 3.0 (H) **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 131 **Storage Temperature (ºF):** -4 to 140 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP Professional or 2000 Professional **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Adjustable brightness

Refer to table notes on page 24.

Vendor: Cross Match Technologies	Product: Verifier 310 LC
 MSRP: $560	**Fingerprint Scanner Specifications** **FAP:** 40 **Fingerprints:** Flat **Simultaneous Capture:** 2 **Sensor:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 1.2 pounds **Dimensions:** 6.8 (L) x 3.8 (W) x 2.6 (H) **IP Rating:** Not rated **Operating Temperature (ºF):** 35 to 100 **Storage Temperature (ºF):** 35 to 100 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP, 7, and Vista **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Ambient light rejection
Vendor: Cross Match Technologies	**Product: Verifier 320 LC**
 MSRP: $800	**Fingerprint Scanner Specifications** **FAP:** 40 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 1.4 pounds **Dimensions:** 6.8 (L) x 3.8 (W) x 2.6 (H) **IP Rating:** Not rated **Operating Temperature (ºF):** 35 to 104 **Storage Temperature (ºF):** 35 to 104 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP, 7, and Vista **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Ambient light rejection
Vendor: Cross Match Technologies	**Product: Verifier EF 200**
 MSRP: $395	**Fingerprint Scanner Specifications** **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Thin Film Transistor **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 10 ounces **Dimensions:** 3.4 (L) x 3.8 (W) x 2.6 (H) **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 122 **Storage Temperature (ºF):** 32 to 122 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP and Vista **FIPS 201 Certification:** Yes **Warranty:** 1 year **Special Features:** Operates in direct sunlight

Refer to table notes on page 24.

Vendor: Dermalog	Product: ZF2
 MSRP: NP	**Fingerprint Scanner Specifications** **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 1.3 pounds **Dimensions:** 4.1 (L) x 4.1 (W) x 2.1 (H) **IP Rating:** NP **Operating Temperature (ºF):** 14 to 131 **Storage Temperature (ºF):** 14 to 140 **Relative Humidity Range:** 10 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows, Linux **FIPS 201 Certification:** No **Warranty:** 1 year **Special Features:** NP
Vendor: Green Bit **Distributor: Advanced Livescan Technologies**	**Product: DactyScan40i**
 MSRP: $403	**Fingerprint Scanner Specifications** **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Optical **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 1.0 pound **Dimensions:** 4.8 (L) x 3.4 (W) x 3.1 (H) **IP Rating:** 54 **Operating Temperature (ºF):** 32 to 122 **Storage Temperature (ºF):** -4 to 140 **Relative Humidity Range:** 30 – 90% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows XP, Vista, 7, 8, and 8.1; Linux Ubuntu and Fedora **FIPS 201 Certification:** Yes **Warranty:** 1 year (extended available) **Special Features:** GUI includes 10 3-color LEDs for finger capture (in sequence)
Vendor: Integrated Biometrics	**Product: Sherlock**
 MSRP: $600	**Fingerprint Scanner Specifications** **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Thin Film Transistor **Auto Capture:** Yes **Manual Capture:** Yes **Weight:** 2.1 ounces **Dimensions:** 2.6 (L) x 2.4 (W) x .56 (H) **IP Rating:** 65 (67 optional) **Operating Temperature (ºF):** -4 to 140 **Storage Temperature (ºF):** -10 to 140 **Relative Humidity Range:** 30 – 85% non-condensing **Transmission & Power:** USB 2.0 **Supported Operating Systems:** Windows 7, 8 and 8.1; Linux; Android 4.0 **FIPS 201 Certification:** Yes **Warranty:** 1 year (extended available) **Special Features:** Operates in direct sunlight; auto-calibrates for wet/dry fingers

Refer to table notes on page 24.

Vendor: Integrated Biometrics	Product: Watson Mini

MSRP: $360

Fingerprint Scanner Specifications

FAP: 45
Fingerprints: Flat, Rolled
Simultaneous Capture: 2
Sensor Type: Thin Film Transistor
Auto Capture: Yes
Manual Capture: Yes
Weight: 3.0 ounces
Dimensions: 2.4 (L) x 2.4 (W) x 1.4 (H)
IP Rating: 65 (67 optional)
Operating Temperature (ºF): -4 to 140
Storage Temperature (ºF): -10 to 140
Relative Humidity Range: 30 – 85% non-condensing
Transmission & Power: USB 2.0
Supported Operating Systems: Windows 7, 8 and 8.1; Linux; Android 4.0
FIPS 201 Certification: Yes
Warranty: 1 year (extended available)
Special Features: Operates in direct sunlight; auto-calibrates for wet/dry fingers

Vendor: Suprema Distributor: Cyber Armed Security	Product: RealScan-G1

MSRP: $379

Fingerprint Scanner Specifications

FAP: 30
Fingerprints: Flat
Simultaneous Capture: 1
Sensor Type: Optical
Auto Capture: Yes
Manual Capture: Yes
Weight: 2.1 ounces
Dimensions: 4.2 (L) x 2.2 (W) x 1.8 (H)
IP Rating: 54
Operating Temperature (ºF): 32 to 158
Storage Temperature (ºF): 14 to 140
Relative Humidity Range: 30 – 90% non-condensing
Transmission & Power: USB 2.0
Supported Operating Systems: Windows 2000, XP, Vista, 7; Linux Ubuntu and Fedora
FIPS 201 Certification: Yes
Warranty: 1 year (extended available)
Special Features: Liveness detection

Notes:
NP: Information not provided by vendor
LED: Light-emitting diode

Information in this table is based on data gathered from vendors and their websites from February to June 2014.

Table 5-4 provides examples of mobile fingerprint collection platforms that use COTS mobile devices in conjunction with peripheral fingerprint scanners and biometric software applications.

Table 5-4. Mobile Fingerprint Collection Platforms

Vendor: CyberArmed Security	**Product: BioAdaptor**	
 MSRP: $989 (software & fingerprint scanner) *Host device not included	**Fingerprint Scanner Specifications** **Fingerprint scanners:** RealScan G-1 (Suprema, Inc.) **FAP:** 30 **Fingerprints:** Flat **Simultaneous Capture:** 1 **Sensor Type:** Optical **Transmission & Power:** USB 2.0	
	Host Device	**Fingerprint Records & Processing**
	Type: Tablet **Supported Operating Systems**: Windows 7, 8, Vista, and XP; Linux Ubuntu and Fedora **Multi-Modal:** Facial, Iris (option) **Transmission:** Bluetooth, Cellular, GPS, Wi-Fi, USB/Wired **Software:** BioAdaptor **Brightness Adjustment:** Yes **Add-Ons:** Credential reader, storage expansion	**Onboard Storage:** No **Onboard Matching:** No **Typical Match Speed:** N/A **Match Result Display:** photos, biographical data **FIPS 140-2 Certified Encryption:** Yes **WSQ Compression:** Yes **Special Features:** Optional temporary data storage in case of network outage
Vendor: InCadence Strategic Solutions	**Product: Ares Biometric Collection Platform**	
 MSRP: NP	**Fingerprint Scanner Specifications** **Fingerprint scanners:** Sherlock or Watson Mini (Integrated Biometrics) **FAP:** 45 **Fingerprints:** Flat, Rolled **Simultaneous Capture:** 2 **Sensor Type:** Thin Film Transistor **Transmission & Power:** USB 2.0	
	Host Device	**Fingerprint Records & Processing**
	Type: Smartphone or tablet **Supported Operating Systems**: Android 4.0 and above **Multi-Modal:** Facial, Iris (option) **Transmission:** Bluetooth, Cellular, GPS, Wi-Fi, USB/Wired **Software:** Ares v1.0 **Brightness Adjustment:** Yes **Add-Ons:** Storage expansion	**Onboard Storage:** 10,000 records **Onboard Matching:** No **Typical Match Speed:** N/A **Match Result Display:** Alert message, biographical data, face photo, rapsheet **FIPS 140-2 Certified Encryption:** Yes **WSQ Compression:** Yes **Special Features:** Finger sequence checking

Refer to table notes on page 26.

<table>
<tr><th colspan="3">Vendor: InCadence Strategic Solutions</th><th colspan="2">Product: Mars Biometric Collection Platform</th></tr>
<tr><td rowspan="3"> 
MSRP: NP</td><td colspan="4">Fingerprint Scanner Specifications</td></tr>
<tr><td colspan="4">Fingerprint scanners: Sherlock or Watson Mini (Integrated Biometrics)
FAP: 45
Fingerprints: Flat, Rolled
Simultaneous Capture: 2
Sensor Type: Thin Film Transistor
Transmission & Power: USB 2.0</td></tr>
<tr><td colspan="2">Host Device</td><td colspan="2">Fingerprint Records & Processing</td></tr>
<tr><td colspan="2">Type: Windows PC or tablet, or CrossMatch Seek II
Supported Operating Systems: Windows
Multi-Modal: Facial, Iris (option)
Transmission: Bluetooth, Cellular, GPS, Wi-Fi, USB/Wired
Software: MARS v3.0
Brightness Adjustment: Yes
Add-Ons: Storage expansions, supports multiple biometric peripherals</td><td colspan="2">Onboard Storage: Yes
Onboard Matching: Device dependent
Typical Match Speed: Device dependent
Match Result Display: Alert message, biographical data, face photo, rapsheet
FIPS 140-2 Certified Encryption: Yes
WSQ Compression: Yes
Special Features: Finger sequence checking, multilingual GUI</td></tr>
<tr><th colspan="3">Vendor: Secure Planet</th><th colspan="2">Product: BRaVe</th></tr>
<tr><td rowspan="3"> 
MSRP: $539
(software & fingerprint scanner)
*Host device not included</td><td colspan="4">Fingerprint Scanner Specifications</td></tr>
<tr><td colspan="4">Fingerprint scanners: Watson Mini (Integrated Biometrics)
FAP: 45
Fingerprints: Flat, Rolled
Simultaneous Capture: 2
Sensor Type: Thin Film Transistor
Transmission & Power: USB 2.0</td></tr>
<tr><td colspan="2">Host Device</td><td colspan="2">Fingerprint Records & Processing</td></tr>
<tr><td colspan="2">Type: Smartphone or tablet
Supported Operating Systems: Android 4.0 and above
Multi-Modal: Facial, Iris (option)
Transmission: Bluetooth, Cellular, GPS, Wi-Fi, USB/Wired
Software: BRaVe mobile application
Brightness Adjustment: Yes
Add-Ons: Storage expansion</td><td colspan="2">Onboard Storage: 100,000 records
Onboard Matching: Yes
Typical Match Speed: 100/sec
Match Result Display: Alert message, biographical data, face photo
FIPS 140-2 Certified Encryption: No
WSQ Compression: Yes
Special Features: Offline matching capability and synchronization of records among Android devices</td></tr>
<tr><td colspan="5">Notes:
N/A: Not applicable
NP: Information not provided by vendor</td></tr>
</table>

Information in this table is based on data gathered from vendors and their websites from February to June 2014.

6. VENDOR CONTACT INFORMATION

Additional information on mobile ID fingerprint devices included in this market survey report can be obtained from the vendors listed in Table 6-1.

Table 6-1. Vendor Contact Information

Vendor	Phone Number	Website/E-Mail Address
3M Cogent Inc.	(626) 325-9600	http://www.3M.com/identitymanagement
Advanced Livescan Technologies Inc. (Distributor for Green Bit Americas Inc.)	(440) 759-7028	http://www.advancedlivescantech.com
Corvus Integration Inc.	(703) 871-5066	http://corvusid.com corvus@corvusid.com
Credence ID LLC	(888) 243-5452	http://credenceid.com
Cross Match Technologies Inc.	(561) 622-1650	http://www.crossmatch.com
Cyber Armed Security LLC (Distributor for Suprema, Inc.)	(202) 536-4943	http://www.cyberarmed.com sales@cyberarmed.com
DERMALOG Identification Systems, GmbH	+49 4041 32270	http://www.dermalog.com info@dermalong.com
Green Bit Biometric Systems, S.p.A.	(703) 279-6414	http://www.greenbit.com
InCadence Strategic Solutions	(703) 552-2810	http://www.incadencecorp.com contracts@incadencecorp.com
MorphoTrak LLC	(703) 797-2600	http://www.morphotrak.com
MorphoTrust USA LLC	(978) 215-2556	http://www.morphotrust.com
Secure Planet Inc.	(571) 393-1777	http://www.secureplanet.com info@secureplanet.com
Suprema Inc.	+82 3171 02464	marketing@supremainc.com
Unisys Corporation (Distributor for Credence ID)	(703) 439-5477	http://www.unisys.com

7. SUMMARY

This market survey report provides information on 13 handheld mobile ID fingerprint devices, 11 peripheral scanners, and 4 mobile fingerprint collection platforms. Handheld devices range in price from $1,299 to $16,800, peripherals from $315 to $800, and collection platforms (fingerprint scanner and software only) from $539 to $989.

Emergency responder agencies that consider purchasing mobile ID fingerprint devices should carefully research each product's overall capabilities and limitations in relation to their agency's operational needs.

APPENDIX A. INGRESS PROTECTION (IP) RATING

The International Electrotechnical Commission (IEC) Ingress Protection (IP) Rating is composed of two digits. The first number in the rating refers to resistance to ingress of solid foreign objects, and the second number represents resistance to ingress of liquids. protection against solids, and the second number refers to protection against liquids. The highest possible rating is IP68.

First Number	Meaning	Second Number	Meaning
(Refers to protection against solids)		(Refers to protection against liquids)	
0	No protection.	0	No protection.
1	Protected against solid objects over 50 mm (e.g., accidental touch by hand).	1	Protected against water falling vertically.
2	Protected against solid objects over 12 mm (e.g., accidental touch by finger).	2	Protected against direct sprays up to 15 degrees from vertical.
3	Protected against solid objects over 2.5 mm (e.g., tools, wires).	3	Protected against direct sprays up to 60 degrees from vertical.
4	Protected against solid objects over 1 mm (e.g., small wires).	4	Protected against sprays from all directions. Limited ingress permitted.
5	Protected against dust-limited ingress (no harmful deposit).	5	Protected against low pressure jets of water from all directions. Limited ingress permitted.
6	Totally protected against all dust.	6	Protected against strong jets of water. Limited ingress permitted (e.g., acceptable for use on ship decks).
		7	Protected against temporary effects of immersion between 15 cm and 1 m for 30 minutes.
		8	Protected against long periods of immersion under pressure.