Report on ABIS Interoperability

Prepared by the IAI's Biometric Information Services Subcommittee
For the 106th Educational Conference in Omaha, Nebraska
July 31–August 6, 2022

Michael French
Gregory Fiumara

Contributing Editors
Kurt Aebersold
Joshua Connelly
Ed German
Karley Hujet
Bethany Retton

This article is reprinted with the permission of the IAI. It originally appeared in ***Identification News***, Vol. 52, No. 2, 2022.

Executive Summary

Identification through systematic classification and searching of human physical characteristics dates back to the late 1800s when pioneers Alphonse Bertillon, Sir Edward Henry, and others developed manual systems for search and retrieval at about the same time in history.

Bertillon invented the system called anthropometry (or signaletics) for the Paris Prefecture of Police that relied on a combination of body measurements, and traits such as eye and hair color, to create a searchable filing system. Sir Edward Henry on the other hand, created the Henry classification system to store and search fingerprint records in the Bengal province of India. In that system, criminal tenprint cards were hand-coded for manual search and retrieval.

The Henry system was brought to the United States in the early 1900s and became the means to search criminal and civil fingerprint records at the FBI's Identification Division (later known as Criminal Justice Information Services or CJIS) from 1924 until replacement with computerization in a series of advances from 1970 to 2000.[1] By the mid-1980s states were purchasing their own Automated Fingerprint Identification Systems (AFIS), and individual city, county, state, and regional AFIS sprung up across the U.S. The term AFIS has recently been replaced by ABIS (Automated Biometric Identification System), to account for modalities other than fingerprints incorporated into modern systems (i.e.. palm prints, facial and iris recognition).

Since multiple AFIS vendors historically produced incompatible systems sold to different jurisdictions, proprietary technology formed barriers to cross-jurisdictional interoperability as well as information sharing necessary to automate the update of criminal history records on a national level. In the mid-1980s standards development organizations began work to homogenize the exchange of biometric data in order to achieve automation, but standards did not mature until the publication of the *ANSI-NIST Data Format for the Interchange of Fingerprint Information* in 1997. Today a comprehensive and mature set of biometric standards enable disparate

[1] On May 19, 2000 CJIS began electronically scanning all new arriving civil fingerprint records.

systems to communicate, connect remote equipment such as live scan and mobile search devices, reduce integration costs, and provide alternatives to biometric vendor "lock-in".

This is all good news; however, the early proliferation of AFIS that initially were not interoperable created a culture and set of practices which became cemented in systems that generally do not communicate across jurisdictions. This means that biometric searches that could assuredly be performed on remote systems are not permitted due to a variety of interwoven technical and non-technical issues.

These unnecessary barriers do a disservice to public safety stakeholders by reducing access to potentially valuable information. The fact that most ABIS across the U.S. are not searchable by neighboring jurisdictions has been criticized by the 2009 National Academy of Sciences (NAS) report *"Strengthening Forensic Science in the United States: A Path Forward"* [1]. This problem was further detailed by the *NIJ/NIST Latent Print AFIS Interoperability Working Group* as well as the National Council of Science and Technology 2014 report *"Achieving Interoperability for Latent Fingerprint Identification in the United States"*[2].

In addition to ABIS proprietary barriers, states sometimes have privacy laws that are either perceived to be conflicting or are in real conflict with the sharing of biometric information [3]. Achieving interoperability will require either updating some of these laws or engineering workarounds that allow searches to be performed lawfully.

Universal cross-jurisdictional biometric searching is considered a necessity by many forensic practitioners and clearly can be achieved considering the amount of interoperability already taking place. However, this is a complex topic, and improvement requires technical awareness, leadership, governance, specification, and funding.

History of AFIS and Interoperability in the United States

In 1963 the FBI's Identification Division realized that the manual system of filing and retrieving fingerprint records required an electronic solution. The national repository of fingerprint cards had become unmanageable due to its size and operations threatened to be overwhelmed under the weight of tens of millions of fingerprint files requiring brute force labor to conduct timely searches using the Henry classification and filing system.

In addition to automated criminal identity management, researchers also envisioned latent fingerprint searches via electronic means in order to advance investigation techniques. This vision paralleled thought leadership generated by the 1973 RAND Corporation report: *"The Criminal Investigation Process"*, which estimated that merely 3% of all criminal convictions were the result of traditional cold case investigative practices [4]. The RAND report issued a clarion call for greater use of physical evidence to solve cases. This movement coincided with the invention of the silicon chip, which would prove to revolutionize law enforcement access to information technology systems [5].

With the help of the National Bureau of Standards, later named the National Institute of Standards and Technology (NIST), the FBI began prototyping emerging AFIS technologies in 1970 and began operationally scanning fingerprint cards in 1976. These efforts were paralleled by AFIS initiatives in France, the United Kingdom, and Japan. These emerging technologies eventually made their way into national law enforcement conversation and sparked what was known as the "San Francisco Experiment". In 1983 the city issued a Request for Proposal (RFP) to purchase the first fully operational AFIS in the U.S., to combat a skyrocketing burglary rate at that time. The NEC Corporation surprisingly won that first AFIS benchmark over a Printrak system that was perceived as the only one capable of operational use. The resulting San Francisco AFIS did indeed have a major impact on lowering the city's crime rate over subsequent months and years.[5] In 1984 the Swiss National AFIS became the first of its kind in Europe. See Appendix C for an historical overview of the Swiss AFIS.

From the mid-1980s to about 2000, AFIS deployments spread across the U.S., and around the world, culminating in the eventual deployment of the FBI Integrated Automated Identification System (IAFIS). Unfortunately, this proliferation of mostly incompatible systems from different vendors superseded the development of standardized biometric data necessary to facilitate AFIS interoperability. The *ANSI-NIST Data Format for the Interchange of Fingerprint Information*, a standards document to support interoperability with the FBI IAFIS, would not be published until 1997.

In 1998 the International Association for Identification's (IAI) AFIS Committee tested this new standard in a technical demonstration of latent print searches between three different AFIS vendor systems: Printrak, Cogent, and Sagem Morpho[6]. This demonstration proved that interoperability was not only possible between disparate systems sending and receiving transactions to the not yet operational IAFIS, but also across different proprietary systems at the state and local level.[2]

IAFIS went live in 1999, processing tenprint records from all 50 states' systems, and latent searches against the first of its kind national repository in the U.S. At this time, Mitretek Systems (now Noblis) conducted the *Image Quality Study* to evaluate the feasibility of cross-searching the Immigration and Naturalization Service (INS) IDENT system, created in 1994, with IAFIS.

Even though biometric transmission standards had matured, and AFIS interoperability had become a way of life between state systems and IAFIS, cross-jurisdictional AFIS interoperability was—and still is—out of the ordinary. This deficiency was called out in the 2009 National Academy of Science (NAS) report *"Strengthening Forensic Science in the United States: A Path Forward" [1]*. From the report:

> *"At present, serious practical problems pose obstacles to the achievement of nationwide AFIS interoperability. These problems include convincing AFIS equipment vendors to cooperate and collaborate with the law enforcement community and researchers to create and use baseline standards for sharing fingerprint data and create a common interface. Second, law enforcement agencies lack the resources needed to transition to interoperable AFIS implementations. Third, coordinated jurisdictional agreements and public policies are needed to allow law enforcement agencies to share fingerprint data more broadly".*

At the same time of the NAS report, the Law Enforcement Standards Office (OLES) at NIST had already begun organizing an interoperability task group that eventually became known as the *NIJ/NIST AFIS Latent Print Interoperability Working Group*. The working group convened experts from government stakeholders, vendors, and private sector consultants to study the problem and provide recommendations and resources. This working group concluded in 2012 and published Request for Proposal (RFP) writing guidance documents intended for states to use when developing specifications for newly purchased AFIS replacements or upgrades that would help ensure interoperability.

Shortly after the NIJ/NIST AFIS interoperability group concluded, The *Latent Interoperability Transmission Specification* (LITS)[7] was published to augment existing biometric transmission standards and close gaps in cross-jurisdictional latent print AFIS searching. The publication of LITS coincided with the Noblis report *"Latent Print Interoperability: State and Local Perspectives* [8]*"* that further described the deficiencies in cross-jurisdictional AFIS interoperability.

And lastly, the National Science and Technology Council published the report "*Achieving Interoperability for Latent Fingerprint Identification in the United States"*, echoing the same issues reported by so many over decades of AFIS operations, as well as providing some remedial recommendations [2].

Landscape of Biometric Interoperability

[2] The 1998 IAI AFIS Committee Report on Cross-Jurisdictional Use of AFIS Systems detailed the interoperability test between vendor systems from Cogent Systems (Ontario, CA Police Department), Printrak International (North Carolina Bureau of Investigation), and Sagem Morpho (Arizona Department of Public Safety). The test adhered to the *ANSI-NIST Data Format for the Interchange of Fingerprint Information* and the *Electronic Fingerprint Transmission Specification*, and while it exposed some flaws in the application of the standard, the test conclusively proved that cross-jurisdictional interoperability was technically feasible.

Most ABIS interoperability across the United States has evolved to maintain and share criminal history information across all 50 states and with the FBI. This involves arrestees being fingerprinted at the city or county level, and those arrest records flowing up to the state level, and then up again to the FBI.

In this system, arrestees are assigned a state identification (SID) number as well as an FBI number, all based on friction ridge biometrics. Each time a subject is arrested, those new fingerprint acquisitions are either added to an existing SID and FBI number, or new SID and FBI numbers are generated for first time offenders. The system that organizes the criminal history information, or "rap sheets," across all 50 states is called the Interstate Identification Index (III). All of the arrest information in the III is intended to be verified to fingerprints on file in each state.

In this hierarchical system each state is required to have access to an ABIS in order to perform the identity management necessary to maintain criminal history records. Decades ago, this was performed by identification units at the city and county level mailing paper fingerprint cards with typed arrest information to the state, and then each state would forward copies to the FBI. In this way the entire process could take up to 60 days to complete, and many records would fall through the cracks. Today with live scan and electronic transmission, as well as lights out ABIS processing advances, the task can usually be completed in 20 minutes without human interaction.

These electronic networks also support latent print searches either directly on the state AFIS, or sometimes at a city or county AFIS if one is available. Since the FBI IAFIS was upgraded to the Next Generation Identification (NGI) System in 2013, with faster and more accurate latent print matching algorithms, some agencies now have a policy to search NGI first and then search at the state or local level second if the NGI search does not return a match. In 2017 CJIS discontinued direct connectivity to NGI for agencies at the city and county levels, requiring these agencies to perform searches through network gateways managed by state agencies.

The vast majority of these biometric searches can only take advantage of hierarchical networks, and don't allow for cross-jurisdictional connections. ABIS cross-jurisdictional networks do exist in the U.S., but usually only between agencies that use the same ABIS vendor and are not the norm. One such example is the Western Identification Network (WIN) that includes NEC ABIS users Alaska, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming that share a common database. Other examples involve the Northern Virginia Regional Identification System (NOVARIS) as well as the National Capital Region network. At the Federal level a cross-jurisdictional network exists between the FBI, Department of Homeland Security (DHS), and Department of Defense (DoD), yet this network was slow to develop and offers limited search capabilities. Despite these examples the vast majority of state and local ABIS in the U.S. cannot connect on a peer-to-peer basis.

Cross-jurisdictional interoperability is somewhat available in Europe under the Prüm treaty signed in 2005. As of 2022, numerous countries participate in the exchange of fingerprints (including latent prints), DNA, and vehicle registrations. There is no central ABIS for law enforcement agencies in the European Union (EU). Under the Prüm treaty, individual countries coordinate access to their national law enforcement biometric databases, including limits on daily searches.

Technical vs. Non-Technical Issues

ABIS interoperability poses both technical and non-technical challenges that are often interwoven. Technical interoperability relies on common data interchange formats, interfaces, terminology, as well as applications that can use the data correctly. Additionally, this data must be transmitted over secure networks, not the general Internet. Non-technical issues generally involve agreements such as memoranda of understanding (MOUs) between agencies that will exchange information, as well as achieving compliance from vendors that will develop the required interfaces and subsystems that use the data.

Barriers impeding biometric data exchange between ABIS are largely non-technical thanks to a mature set of standards that include ANSI/NIST-ITL, EBTS, ISO/IEC, FIPS, and the CJIS Security Policy (see Appendix–A for a complete list of acronyms and their definitions). These standards have been implemented for decades, are continually updated, and used in all types of criminal justice interfaces, e.g. ABIS, live scan, booking, criminal history, background checks; as well as the INTERPOL implementation of the NIST standard worldwide, a planned biometric hub that should go live at the end of 2022 (1 'INTERPOL NIST file' allowing transmission of fingerprint sets, mugshots, and DNA to the central INTERPOL database, etc.).

U.S. networks that enable this exchange of information include regional networks run by state and local law enforcement, CJIS WAN, NLETS, LEEP, as well as government cloud providers such as Amazon Web Services and Microsoft Azure. Prior to any large-scale interoperability effort, the amount of network volume must be estimated so bandwidth can be purchased and scaled appropriately.

Non-technical challenges involve the necessity for agencies to envision all interoperability use-cases they can foresee. Then they must negotiate access with remote agencies, by defining workflows and responsibilities, as well as broker search volumes and timing through MOUs. When these preconditions are met, vendors then need to be approached with a clear set of interoperability requirements so engineering costs can be accurately estimated and competitively bid if necessary. Finally, any deployment must be validated with test cases that prove contract compliance.

Prior to developing any technical solution, planners must foresee and then scope technical requirements in a collaborative process, and this is more complicated than simply sending and receiving search data and results. A Biometric Information Systems (BIS) 2021 survey [9] indicated that the vast majority of respondents "agree" or "strongly agree" that *lack of interoperability impedes criminal investigations*.[3] Survey respondents also provided commentary that sheds light on the complexities of planning for interoperability in the RFP process. Here are some sample comments:

> *"Any attempt for developing (sic) Interoperability MOU ended up in the Legal Department of either agency, and no movement was made from there."*

> *"The biggest issue is proprietary software that doesn't communicate well with one another. Yes, we can search, but we don't necessarily have all the features/tools necessary to easily compare."*

> *"State systems/requirements are mostly proprietary and do not encourage interoperability."*

> *"Required to search state [AFIS Vendor] first and to not bypass even though hits are low to nil. Implied repercussions limiting and throttling (sic) number of searches for noncompliance."*

These survey comments are reflective of feedback from practitioners throughout the industry, and the above comments describe difficulty in the non-technical planning stages of ABIS development, which if left unresolved lead to technical shortcomings in the deployment of any system designed through an RFP process.

Biometric Interoperability Standards

All interoperable technology systems have a method in which data can be shared seamlessly between all members. For the interchange of fingerprint and other biometric data, there are a handful of common data formats which can encode images, features, and other pertinent information about biometric samples. The remainder of this section will primarily focus on standards for the friction ridge modality.

Template Formats

Fingerprints are a unique biometric modality in that features of fingerprint samples can be identified and commonly understood without sharing the original image. Files containing extracted features are referred to as *templates*. Templates containing features

[3] In 2021 the IAI Biometric Information Services (BIS) Subcommittee circulated a 13-question survey through the IAI social media platform, CLPEX.com message board, and several wide-ranging email distribution channels aimed at latent print examiners. Survey questions focused on ABIS interoperability capabilities and practitioner attitudes. Between March and October 2021, the survey captured 72 responses. **https://forms.gle/H5eGY5htjXkcerNy6**

such as minutiae locations and pattern classification can be used by AFIS to make comparisons. Use of feature-only interoperable templates allows for a compact representation of a fingerprint.

ANSI/INCITS 378

In November 2001, the International Committee for Information Technology (INCITS)'s Technical Committee M1 was formed, focusing on 1:1 verification [10]. INCITS is a U.S.-based and ANSI-accredited standards development organization. By 2004, Task Group M1.1 on Biometric Data Interchange Formats completed one of their first projects, *INCITS 378: Finger Minutiae Format for Data Interchange* [11]. This format allows for a compact encoding of one or more encounters of fingers, solely using features. No image is included in the file, but pertinent information about the source image, such as sensor type, image dimensions, and resolution are included. Fingerprint feature information included in the record format include minutia position, type, angle, and quality. The record also allows for "extended information" to be included, such as core/delta locations and ridge counts.

An international analog to Technical Committee M1, ISO/IEC JTC1 Subcommittee (SC) 37 was also formed at the end of 2002[12]. A working group on SC 37 adopted the U.S. standard into a similar format, originally published in 2005 as ISO/IEC 19794-2[13]. Although there are slight differences in encoding, the fundamentals of the record formats remain the same. The international version of the standard went on to introduce even more compact fingerprint formats for use on integrated circuit cards. A working group within SC 37 is actively developing an extensible version of the standard, ISO/IEC 39794-2[14].

Versions of both ANSI/INCITS 378 and ISO/IEC 19794-2 are widely used today. The U.S. Government's Personal Identity Verification (PIV) card stores fingerprint information in ANSI/INCITS 378 templates on each card. Those PIV cards that make use of on-card comparisons also store ISO/IEC 19794-2 files. The Unique Identification Authority of India (UIDAI) stores over one billion fingerprint minutiae records for its citizens as ISO/IEC 19794-2 files. In each of these systems, a wide network of feature extraction algorithms is used to generate templates, and various comparison algorithms are used to perform verifications. ANSI/INCITS 378 is a shining example of successful operability.

Image Formats

While interoperable template formats have their place, the information stored in them is only as good as the algorithm or examiner that extracted features from the source sample. Sometimes it's desired to save the image itself so that different feature extraction algorithms can reprocess an image without recapturing. While there are many familiar standard image *codecs* (e.g., JPEG, PNG, TIFF, etc.), these files do not always contain all the information needed by a feature extractor.

ANSI/INCITS 381

At the same time M1 was working on an interoperable minutiae standard, the technical committee also worked on an interoperable image interchange format. This format, published in 2004 as *INCITS 381: Finger Image-Based Data Interchange Format* [15], allows concatenation of multiple images of fingerprints in a single file. Information like resolution, image quality, and scanner model can be encoded into the header of the record. The format also allows for uncompressed ("raw") image data read from a sensor to be placed in the record, avoiding potential lossy compression. Much like the minutiae standard, ISO/IEC 19794-4[16] tracked ANSI/INCITS 381 for an international audience and was made extensible in ISO/IEC 39794-4[17].

Interchange Formats

Although there are valid use cases for interoperable formats that contain limited information (e.g., an individual sample or set of features), it's often necessary to include significantly more information when transmitting data to other agencies. For example, on prisoner intake, there may be several types of information collected that may need to be shared. Such information might include fingerprints, mugshots, iris images, tattoos, biographic data, related case or evidence identifiers, and so much more. Rather than transmit countless files of individual standards, the ANSI/NIST-ITL standard was created to house all of this information.

ANSI/NIST-ITL

In 1986, the National Institute of Standards and Technology (NIST)—previously named the National Bureau of Standards (NBS)—released ANSI/NBS-ICST 1-1986. This standardized and open binary file format allowed for encoding of information on a Federal Bureau of Investigation *Arrest and Institution Fingerprint Form*, FD-249, including fingerprint images and a host of biographical and case identification information. Taking the digital medium a step further, extracted features, such as minutiae and pattern classification, could also be encoded into the record, serving as a precursor to ANSI/INCITS 378.

The standard—now ANSI/NIST-ITL 1-2011 Update 2015[18]—has been revised many times over the years. The most recent revision from 2015 supports interchange of a host of additional modalities, from face and tattoos, to DNA, voice, dental, and more.

Extended Feature Set

A workshop was held in 2005 that tasked the Scientific Working Group on Friction Ridge Analysis (SWGFAST) to identify fingerprint features beyond the traditional minutiae point information stored in records like ANSI/INCITS 378. SWGFAST convened a committee to standardize an encoding of the features. The committee's work, dubbed *Extended Feature Set (EFS)*, was merged into the following revision of the standard in 2011.

EFS defines an open encoding method for dozens of vendor-neutral features fingerprint examiners routinely extract in their work. It goes beyond simple minutiae and classifications, adding concepts like ridge flow maps, quality regions, tonal inversion, orientation, pores, creases, regions of interest, and more.

Profile Specifications

Because there are so many possible features in EFS, it would take an examiner a considerable amount of time to populate them all. In 2013, NIST released EFS profile specifications that identify subgroups of features that should present to simplify markup and enable greater interoperability among AFIS and examiners. It creates a clearer language about the contents of a transaction and could be used as a reference for "completion" of an examiner's duties on a print. For example, an agency might define a policy of annotating to *EFS Profile 3* for a murder investigation but only require *EFS Profile 1* for a petty theft, in order to make best use of an examiner's time.

Four basic profiles were defined. *Image-only (Profile 0)*, as the name suggests, includes no EFS data, and only an image is searched. *Minimal Markup (Profile 1)* includes annotating the most basic of features that could be performed quickly, namely cores/deltas, orientation, pattern classification, and region of interest. This helps eliminate errors that could be introduced by a poor performing algorithm. *Quick Minutia Search (Profile 2)* adds an enumeration of all minutiae present in an image. The final basic profile, *Detailed Markup (Profile 3)* adds more time-consuming features, like quality maps, dots, incipient ridges, and ridge counts.

Electronic Biometric Transmission Standards

ANSI/NIST-ITL defines an extensible data format that allows for the encoding of all sorts of information, as well as dozens of pre-defined types and fields used for the interchange of pertinent biometric data between various federal, state, local, tribal, and international systems. However, individual systems may require specific information to be more useful. One such system is hosted by the FBI. Transactions that come to the FBI must be ANSI/NIST-ITL transactions formatted in the Electronic Biometric Transmission Standard (EBTS)[19].

Like EFS Profile specifications, EBTS is an open specification that builds upon ANSI/NIST-ITL. EBTS defines certain required fields and values within an ANSI/NIST-ITL transaction to be useful in FBI systems. For instance, ANSI/NIST-ITL defines fields for transaction control numbers, but does not go so far as to define a format for such identifiers. However, to be used in the FBI, those control numbers must meet the formatting guidelines to be usable in FBI systems.

EBTS also defines a request and response flow using transactions. ANSI/NIST-ITL requires a *type of transaction* field to be populated. Depending on the value specified, the transaction submitted to an FBI system will be routed for a different action and expect different records and values within the transaction to be specified. The system will often return its results with another EBTS file containing results, for instance, in the form of biometric or biographic information about a candidate in a reference database.

The FBI is not the only agency that inherits the basic requirements for logical records in ANSI/NIST-ITL but has specific requirements for its contents and composition. The DoD also has an EBTS specification [20]. The DHS defines IDENT Exchange Messages (IXM) [21]. Internationally, Germany defines the German Standard for AFIS Transactions (GSAT) [22], Switzerland defines a Swiss Implementation [23], INTERPOL defines INTERPOL Implementation (INT-I) [24], and countless other examples. All these systems build upon the open foundations of ANSI/NIST-ITL with added open functionality to control their identification systems.

Latent Transmission Interoperability Specification

While EBTS builds specifications upon ANSI/NIST-ITL, the Latent Transmission Interoperability Specification (LITS)[7] builds upon the FBI's EBTS. LITS is a system-level specification that takes certain basic latent transaction features from EBTS and makes them a requirement for AFIS builders. This means that the specifications for interaction with the FBI system are the basis for how all AFIS supporting LITS should work. If an AFIS supports LITS, a latent transaction from an FBI system will work flawlessly with the AFIS. The LITS specification also supports types of transactions that facilitate transmission of fingerprint annotation information between human examiners that an AFIS might not use, such as correlation of features from latent to exemplar fingerprints.

While this seemingly appears trivial, the benefits of LITS are enormous. With *zero* effort, a high-profile latent transaction can be run through every AFIS that supports LITS. No implementation details need to be considered and no agency-specific information needs to be added. The transaction can be run as-is. The benefit of this interoperability in time-sensitive investigations cannot be overstated.

Other Considerations

NIEM

In 2005, the DHS and Department of Justice (DOJ) launched the *National Information Exchange Model (NIEM)[25]*. NIEM is a common vocabulary among various fields to communicate data among systems. For instance, if a database stored information about a person, a common field might be "Last Name," but there are many ways to refer to a person's last name, such as "surname" and "family name." NIEM essentially picks one of these representations as a standard, allowing any system that needs to interact with a person to always know the piece of information they need. Developers can write systems against NIEM and always have access to the correct information. In 2012, a *Biometrics* domain was added to NIEM, creating a common digital vocabulary for the exchange of biometric information. The ANSI/NIST-ITL standard is compliant with the NIEM Biometrics domain, allowing interchange of biometrics data in Extensible Markup Language (XML) format to a wide variety of systems. In the European Union, a similar project exists called the Universal Message Format (UMF) [26].

Image Codecs

Interchange formats like ANSI/NIST-ITL allow for easy transmission of biometric data, but don't define the structure of the *image* data stored within. Many existing standards for image formats exist, like Portable Network Graphics (PNG) and Tagged Image File Format (TIFF). Images are stored in these standardized formats within the biometric interchange files. Nearly all operating systems provide built-in methods to convert these encoded files into something that can be displayed or manipulated by AFIS.

One major exception is the image format Wavelet Scalar Quantization (WSQ) [27]. This is a standardized format for the compression of 8 bit per pixel, 500 pixel per inch (ppi), grayscale fingerprint data. The format was developed in 1993 with support from the FBI, NIST, and the Los Alamos National Lab, to include as part of the original ANSI/NIST-ITL standard. The large size of 500 PPI fingerprint images necessitated image compression, but existing image compression formats created "block" artifacts, which altered ridge structure and obscure minutiae. Compression techniques developed for WSQ avoided this problem. WSQ is a freely available specification and remains the de-facto standard for 500 ppi fingerprint image compression. FBI certifies WSQ codecs for use in NGI.

For 1000 ppi fingerprints used in NGI, the FBI requires the use of a Joint Photographic Experts Group (JPEG) 2000 codec. Like WSQ, FBI certifies JPEG 2000 codecs for use in NGI, but unlike WSQ, most operating systems provide support for this format.

Image Content

In recent years, there has been increased interest in using new types of sensor technologies to capture fingerprint images. One such technology is the use of a sensor that does not contact the finger skin whatsoever, including the use of cameras built into mobile phones. The result is an image whose content is often vastly different from optical live scan or ink fingerprints. This new style of image content and constant advancements of image post-processing has created a new barrier for AFIS interoperability, due to the requirement of new types of algorithms for processing. The challenges have been widely reported [28], and the industry continues to work on advancing the interoperability of the image data [29].

Interoperability Resources

Interoperability is more complicated than establishing a common transmission protocol. The transmitted data must be converted in and out of proprietary formats with fidelity and parity. Applications must be able to make use of that information and present it to the end-user in a useful way. It is one thing for a system to receive and search standard fingerprint minutiae, but it is quite another for a system to receive standard minutiae in a search result and render those for comparison purposes. Without the latter, the ability to search remotely may not be as valuable as portrayed since this can severely impact examiner efficiency.

It is not in any ABIS vendor's best interest to fund the engineering of more expensive systems not required by the customer; therefore it is imperative that these specifications are well thought out by the procurement team in the early stages of planning.

The *NIJ/NIST AFIS Interoperability Working Group* addressed the lack of widespread cross-jurisdictional interoperability between AFIS and published several resources to assist agencies in the design and procurement of these systems. As a result of these meetings the working group published two guidance documents: "*Writing Guidelines for Requests for Proposals for Automated Fingerprint Identification Systems"* [30], and "*Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems*" [31].

These two documents recognize the need for requirements and specifications provided to ABIS vendors that are the basis for any contract award, as well as the inter-agency agreements needed for agencies to use each other's systems.

The *"Writing Guidelines for Requests for Proposals for Automated Fingerprint Identification Systems"* document describes the procurement process and makes clear that there needs to be a vision for interoperability from the agency's leadership planning any ABIS purchase or replacement. The document lays out four phases of the procurement lifecycle: 1) establish leadership, 2) create the RFP, 3) evaluate proposals and award contract, and 4) manage procurement and implementation. Without clarity and cohesion between all four project phases it is unlikely that any system will achieve meaningful interoperability.

Recommendations

Editor's Note: This section will not be completed until after the public commenting period has closed, and a panel discussion has occurred at the 2022 IAI Conference in Omaha, Nebraska.

Appendix A–Glossary

ABIS	Automated Biometric Identification	System
AFIS	Automated Fingerprint Identification	System
ANSI	American National Standards Institute	
ANSI/NIST-ITL	Standard that specifies formats to be	used for exchanging fingerprint
and	other image data	
Appendix F	EBTS appendix defining image quality	specifications
CJIS	FBI-Criminal Justice Information	Services Division
EBTS	Electronic Biometric Transmission	Specification - the FBI's
EFS	Extended Feature Sets - Additional	features added to Type-9 minutiae
	implementation of the ANSI/NIST-ITL	Standard
FIPS	Federal Information Processing	Standard

IAFIS	Integrated Automated Fingerprint Identification System - the FBI’s old system for integrating fingerprint records with criminal history record Processing
IAI	International Association for Identification
III	Interstate Identification Index – Data sharing repository across all 50 U.S. states linking SID numbers and criminal histories
JPEG	Image format standard from the Joint Photographic Expert Group
LEEP	FBI Law Enforcement Enterprise Portal
LITS	Latent Interoperability Transmission Specification - Intended to augment EBTS for cross-jurisdictional latent print AFIS interoperability
MOU	Memorandum of Understanding
NAS	National Academy of Sciences
NGI	Next Generation Identification - The FBI’s new system for integrating fingerprint records with criminal history records processing
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunications System
OLES	NIST Office of Law Enforcement Standards
PIV	Biometric Specifications for Personal Identity Verification
RFP	Request for Proposal
SID	State Identification Number - Unique assignment based on fingerprint match
TOT	ANSI/NIST Type of Transaction
WSQ	Wavelet Scalar Quantization (the compression method required for submitting fingerprint images to the FBI)

Appendix B–Bibliography

[1] *Strengthening Forensic Science in the United States: A Path Forward* | Office of Justice Programs. 2022. [online] Available at: www.ojp.gov/ncjrs/virtual-library/abstracts/strengthening-forensic-science-united-states-path-forward#additional-details-0 [Accessed 8 February 2022].

[2] *Achieving Interoperability for Latent Fingerprint Identification in the United States.* 2014. Washington D.C: National Science and Technology Council: Committee on Science: Subcommittee on Forensic Science. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/afis_10-20-2014_draftforcomment.pdf.

[3] *Biometric Privacy Laws Create New Avenue for Data Breach Class Actions.* Buchanan Ingersoll & Rooney PC, November 17, 2020. www.bipc.com/biometric-privacy-laws-create-new-avenue-for-data-breach-class-actions.

[4] Greenwood, Peter W., *The RAND Criminal Investigation Study: Its Findings and Impacts to Date*. Santa Monica, CA: RAND Corporation, 1979. www.rand.org/pubs/papers/P6352.html. Also available in print form.

[5] National Institute of Justice (U.S.). 2011. *The fingerprint sourcebook: Chapter 6 Automated Fingerprint Identification Systems*. Washington, DC: U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice. http://purl.fdlp.gov/GPO/gpo18039.

[6] Higgins, Peter, and Cynthia Way. 1998. *IAI AFIS Committee Report on Cross-Jurisdictional Use of AFIS Systems*. International Association For Identification. https://drive.google.com/file/d/1fM_CFzz_xG9vdGV_rb0nYUgSgPzBoxs0/view.

[7] Chapman, et al., *NIST SP 1152: Latent Interoperability Transmission Specification*. January 2013. https://doi.org/10.6028/NIST.SP.1152

[8] *Latent Print Interoperability: State and Local Perspectives: April* 2012. Noblis, Inc. https://www.winid.org/wp-content/uploads/2019/08/Case_Studies_Final_Report_v1.1_2012-04-02.pdf

[9] French, Michael, 2021. IAI BIS Subcommittee ABIS Interoperability Survey. https://forms.gle/vZWjZnWfziZwTCpv8

[10] INCITS. *M1 - Biometrics*. https://standards.incits.org/a/public/group/m1.

[11] ANSI/INCITS. *378-2004: Information Technology - Finger Minutiae Format for Data Interchange*.

[12] ISO. *ISO/IEC JTC 1/SC 37 Biometrics*. www.iso.org/committee/313770.html

[13] ISO/IEC. *19794-2:2011: Information technology - Biometric data interchange formats - Part 2: Finger minutiae data*.

[14] ISO/IEC. *CD 39794-2.3: Information technology - Extensible biometric data interchange formats - Part 2: Finger minutiae data.*

[15] ANSI/INCITS. *381-2004: Information Technology - Finger Image-Based Data Interchange Format*. 2004.

[16] ISO/IEC. *19794-4:2011: Information technology - Biometric data interchange formats - Part 4: Finger image data*.

[17] ISO/IEC. *39794-4:2019: Information technology - Extensible biometric data interchange formats - Part 4: Finger image data*

[18] Mangold, Kevin, editor. *NIST SP 500-290e3: Information Technology: American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. December 2015. https://doi.org/10.6028/NIST.SP.500-290e3

[19] Criminal Justice Information Services Division - Federal Bureau of Investigation. *Electronic Biometric Transmission Specification with Technical and Operational Updates, Version 10.0.9*. www.fbibiospecs.cjis.gov/EBTS

[20] Department of Defense. E*lectronic Biometric Transmission Specification: Version 4.1.* April 2019. www.dfba.mil/functions/library/standards_docs/DoD%20EBTS%20v4.1.pdf

[21] Office of Biometric Information Management. *Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification—v6.0.9.0.1 (For Official Use Only)*. December 2017.

[22] Federal Office for Information Security. *Technical Guideline TR-03121-3: Biometrics for Public Sector Applications. Part 3.* Volume 4. Version 4.2. www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03121/TR-03121-3_4_Biometrics_4-2.pdf?__blob=publicationFile&v=5

[23] Swiss Federal Department of Justice and Police. *ANSI/NIST ITL-1 2011–Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information: Swiss Implementation.* April 2020.

[24] INTERPOL AFIS Expert Working Group. *INTERPOL Implementation for Data Format for the Interchange of Fingerprint, Facial and Biometric Information*. August 2020. www.interpol.int/ar/content/download/15373/file/NIST%20INTERPOL%20standard%20v6.00.01.pdf

[25] National Information Exchange Model. *Biometrics*. www.niem.gov/communities/biometrics

[26] Europol, *Universal Message Format : faster, cheaper, better*. Publications Office. 2014,

[27] Federal Bureau of Investigation, Criminal Justice Information Services. *WSQ Gray-Scale Fingerprint Image Compression Specification - Version 3.1.* October 2010. https://fbibiospecs.fbi.gov/file-repository/wsq_gray-scale_specification_version_3_1_final.pdf

[28] Orandi, S., Libert, J., Bandini, B., Ko, K., Grantham, J., Watson, C. *NISTIR 8315: Evaluating the Operational Impact of Contactless Fingerprint Imagery on Matcher Performance.* September 2020. https://doi.org/10.6028/NIST.IR.8315

[29] Orandi, S., Watson, C., Libert, J., Fiumara, G., Grantham, J. *NIST SP 500-334: Contactless Fingerprint Capture and Data Interchange Best Practice Recommendation.* March 2021. https://doi.org/10.6028/NIST.SP.500-334

[30] Ballou, S., Clay, A., Dickerson, J., Garris, M., Higgins, P., Hoin, J., Jackson, L., Komarinski, P., Lesko, M., Morrissey, J., Norton, L., Owens, B., Polski, J., and Taylor, M. (2013), Writing Guidelines for Requests for Proposals for Automated Fingerprint Identification Systems, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1155 (Accessed January 20, 2022)

[31] Ballou, S., Clay, A., Dickerson, J., Garris, M., Higgins, P., Hoin, J., Jackson, L., Komarinski, P., Lesko, M., Morrissey, J., Norton, L., Owens, B., Polski, J., and Taylor, M. (2013), Writing Guidelines to Develop an Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1156 (Accessed January 20, 2022)