CJIS Division

U.S. Government Interagency Symposium for Investigatory Voice Biometrics

Interoperability Committee Report

Version 1.0

02/03/2010

CJIS Document Number — CJIS-DOC-17963-1.0

Prepared by

Interoperability Committee

Produced for:
Federal Bureau of Investigation

Criminal Justice Information Services Division
1000 Custer Hollow Road, Clarksburg, WV 26306

TABLE OF CONTENTS

LIST OF TABLES

1. Executive Summary

The U.S. government's interest in developing automated techniques to recognize people by their voices has a nearly 70-year history. Although significant challenges remain, the consensus is that sufficient progress has been made to enable U.S. government agencies in general and, specifically, the Federal Bureau of Investigation (FBI) to further consider fielding speaker recognition technology in support of their missions. Therefore, the FBI Science and Technology Branch Biometric Center of Excellence (BCOE) asked the National Institute of Standards and Technology (NIST) to launch a program directed at developing voice biometric collection and interoperability standards capable of supporting the common investigatory needs of all interested U.S. government agencies.

To begin this process, NIST organized a two-day Interagency Symposium for Investigatory Voice Biometrics March 24–25, 2009. Approximately 80 international stakeholders from government, academia, and industry attended. The symposium marked the beginning of a multiyear program to develop investigatory voice biometric collection and interoperability standards. A symposium steering committee was established, which then created four committees, each assigned to create and deliver a "challenge" document. The four committees are Use Case, Interoperability, Collection Standards, and Science and Technology.

This document, the "Investigatory Voice Biometrics: Interoperability Committee Report," is the second of those four challenge documents and follows the Use Case committee's report in style and spirit. This report reviews current U.S. government and Department of Justice (DOJ) thinking on data interoperability and interchange and discusses various existing and proposed frameworks and approaches currently championed by DOJ. It presents an analysis of existing models for biometric and voice standards and discusses a path forward for developing voice biometric interoperability across the justice domain that supports the current international scope of biometric data exchange involving the FBI.

2. Introduction

The U.S. government Interagency Symposium for Investigatory Voice Biometrics, held March 24–25, 2009, at NIST in Gaithersburg, Md., initiated a multiyear program to develop investigatory voice biometric collection and interoperability standards. The program was directed initially at defining requirements and necessary research to support the development of standards and best practices. NIST held the symposium in response to a request by the FBI Science and Technology Branch BCOE. The wide international participation was indicative of the importance the world places on biometric standards developed by the FBI in partnership with NIST. The symposium focused on four topics: use cases, collection standards, interoperability, and science and technology gaps. The four topics were divided into committees that will explore each topic area and submit a report in the months after the symposium to the Steering Committee. The Interoperability Committee's report discusses interoperability for voice biometric systems across U.S. government and international domains of interest.

The report is intended as a "challenge" document, specifying the current state of knowledge in the area of interoperability and discussing what advances will be necessary to establish voice biometric standards.

2.1 Interoperability Panel

The interoperability case panel at the symposium consisted of the following presenters:

- James L. Wayman, Chair, speaking for the British Standards Institution, London, UK
- Avery Glasser, Agnitio, Spain
- Judith Markowitz, J. Markowitz Consultants, USA
- Homayoon Beigi, Recognition Technologies, USA.

2.2 Interoperability Committee

The Interoperability Committee used the panel presentations, direction from the sponsoring organization, and resultant discussions to define and document the goals and requirements for voice biometric data interoperability across a Community of Interest within the U.S. government. The Interoperability Committee consists of:

- James Wayman, Chair, BRTRC, USA
- Judith Markowitz, member, J. Markowitz Consultants, USA
- Avery Glasser, member, Agnitio, Spain
- Homayoon Beigi, member, Recognition Technologies, USA
- Bradford J. Wing, member, NIST, USA
- Peter T. Higgins, BRTRC, USA
- Mike McCabe, ID Technology Partners, USA
- Joe Campbell, Massachusetts Institute of Technology/Lincoln Laboratory, USA

3. The Concept of Interoperability

This paper concerns the interoperability of investigatory voice biometrics. In the Use Case report, the first in this series of four challenge documents, the basic concepts and issues of investigatory voice biometrics were discussed. This paper inherited the framework developed in the Use Case report. For this paper, the concept of interoperability implies coordination and cooperation among various groups, and even within a single group, to perform tasks of interest. Within the U.S., those groups coordinating and cooperating with the FBI are federal agencies and state, local, and tribal governments. Even from the earliest Bureau of Identification days preceding the current FBI's establishment, biometric data interoperability also meant international coordination and cooperation. This international aspect places additional requirements on the development of interoperability standards for investigatory voice biometrics. This section is concerned with the concept of voice biometric data interoperability for the broad range of the FBI's domestic and international investigatory activities.

3.1 Definitions

The symposium's title places voice data in the context of biometrics. As in the Use Case report, biometrics refers to "the automated recognition of individuals based on their biological and behavioral traits." [1]. In accordance with this definition, voice biometrics implies the automated use of voice data for recognizing individuals. Implicit in this definition is the concept that the voice data will be "personally identifiable." Its collection, storage, and dissemination will require consideration of privacy and security issues.

The field of interest and application of voice biometrics within this study is law enforcement, where law enforcement entails forensic and investigatory uses. Interoperability, in the law enforcement context, means sharing voice data, metadata, and decisions based on data across systems, applications, agencies, jurisdictions, and time in support of forensic and investigatory applications. In other words, interoperability means using data within a single agency for multiple current and future applications on one or more systems and sharing data across agencies for applications that may not be predictable by the collecting agency. "Forensic" is specifically included to indicate that the sharing of this data must be done in such a way to meet all regular procedural legal requirements. Any interoperability standard must be created within the varying and generally non-communicating cultures comprising the operational, legal, scientific, standards, privacy, and data interchange communities and must be applicable at an international level.

This report will accept as standard the additional definitions given in the "Use Case" Committee Report's Appendix A.

3.2 Voice Data Interchange Standards

Interoperability between or within agencies implies the existence of data interchange standards. As the name suggests, data interchange standards are designed to enable agencies to exchange data and, once exchanged, to understand the data and its uses. These standards have two primary components: voice signal data and headers. The voice signal that is exchanged could potentially be original data (unprocessed beyond the immediate requirements for digitization), partially processed data (segmented acoustic data or extracted features, such as short term Fourier spectra or Cepstrum), or fully processed models.

While there is some consensus on how voice signals are to be digitized, there is no consensus on what distinguishing characteristics (also called "features"), should be extracted from those signals and how those characteristics should be used to create "models" for known speakers. This implies voice data interchange can only take place at the level of digitized acoustic data. Methods for digitizing acoustic data, while numerous, are already standardized, so the digital representation of voice signals is not this report's focus.

The headers contain the "metadata" that describes the voice signal contained in the interchange and the conditions of its collection, storage, and dissemination. That metadata will describe the acoustic data, channel, and device used to capture and transmit the speech data, the audio format used to store them, speaker(s) — to the extent known — and other factors that enable the recipient to process and use the data effectively.

All of the data, both voice signal and metadata, must be wrapped in a package that can be understood by the recipients. This report will focus on establishing requirements for both the metadata and the packaging required for voice biometric interoperability.

3.3 Special Challenges of Voice Data Interchange

The nature and wide variety of potential applications across systems for voice data has several challenges that must be considered. Unlike other personally identifiable biometric information, such as fingerprints or iris, voice data can carry semantic content and secondary information, such as language and dialect. The semantic content may entail privacy and security considerations not encountered with other biometric characteristics.

Speech generally takes place within a social context, such as a conversation between two or more individuals. Consequently, voice data may contain multiple speakers, some of whom are not the voice recognition systems' target. If the speech data is not acquired conversationally but rather through prompting or reading, there may be legal restrictions on the speech's semantic content (see Section 7).

In forensic applications, the voice data may be accompanied by other audio information of investigative or forensic interest, such as background speakers, machine noise, or gunshots. In other applications, separating and labeling speech segments by speaker, a process called "segmentation" in the speech community, may be a simple matter, but, in other applications, speech collision may make clear segmentation impossible.

Recorded speech data may inevitably contain personally identifiable information from multiple persons, some of whom are of no interest to the law enforcement community. In this respect, processing voice data for automated human recognition may be more akin to latent fingerprint processing than iris recognition, where data collection systems are optimized with the specific intention of identifying a single person. Additional audio information may be embedded with the voice in the data that must be preserved in the process of labeling and storing the signal.

If interoperability implies the use of voice data by systems and applications other than the application or system of original collection, and if voice data can be accompanied by important non-speech audio data, then anticipating future users' data and metadata needs while meeting information privacy and security requirements will be extremely challenging. Segmenting, formatting, and storing voice data in anticipation of those needs will also be difficult. An interoperability standard must consider all of these issues.

4. Current Data Interoperability Environment Within the U.S. Government

Data interoperability and interchange between U.S. government agencies has received special interest since Sept. 11, 2001. Several important Congressional and agency initiatives creating frameworks for data exchange among federal agencies and supporting data exchange with state, local, and tribal governments have been launched in the last five years. These new frameworks are not always fully compatible with each other or legacy operational data exchange systems, some of which have considerable entrenchment across all levels of government (domestically and internationally) based on substantial previous investment. Laying new frameworks upon the various existing single agency, cross-agency, and international data interchange systems has led to a complex landscape of interrelated paradigms for data exchange within the federal government.

Finding a path forward over this complex landscape will be a challenge when developing an investigatory voice biometric interoperability standard. This section will give an overview of the data interoperability frameworks within the federal government in general and the DOJ in particular that will impact voice biometric interoperability.

4.1 Data Interoperability Within the Federal Government

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the establishment of an Information Sharing Environment (ISE) "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[2]. IRTPA established a Program Manager (PM) ISE to be "responsible for information sharing across the federal government" and to oversee the implementation of and manage the ISE, as well as an interagency advisory body called the Information Sharing Council. One of PM ISE's responsibilities is "assisting, monitoring, and assessing the implementation of the ISE by federal departments and agencies to ensure adequate progress, technological consistency and report findings to Congress." [2] The ISE[1] was established in 2007 and specifically includes consideration of voice data exchange within its framework. [3]

The ISE adopts both the National Information Exchange Model (NIEM), described at length below, and the Department of Defense (DOD) and Intelligence Community (IC) Universal Core (UCore) standards. The DOD/IC UCore is developed and controlled by the Senior Enterprise Services Governance Group, an advisory body to the Director, Information Policy, Office of the DOD Chief Information Officer (CIO), and the Deputy Associate Director of National Intelligence for IC Enterprise Architecture, Office of the Associate Director of National Intelligence CIO. Also, the ISE acknowledges the

[1] Although the importance of international information sharing in terrorism prevention is clear in IRTPA's language, international data sharing standards are outside of the ISE;s scope. Consequently, the ISE is not directly applicable to the international sharing of biometric information tradition to the FBI.

coexistence of multiple information sharing frameworks within the U.S. government as a whole.

According to the NIEM newsletter, "UCore is an interagency information sharing initiative being developed by DOD, DOJ, the Department of Homeland Security (DHS), and the IC." [5] There is a belief within the DOD biometrics standards community that this non-NIEM-compliant solution could be mandated for DOD in the very near future. However, UCore would not generally be considered relevant to developing a standard for use by international law enforcement agencies, so is not discussed further in this report.

4.2 Data Interoperability Within the Justice Domain

Although created before the ISE, DOJ's response to the need for wider data interoperability was the "Law Enforcement Information Sharing Program (LEISP)," discussed in Section 4.2.4 below [4] In addition to the LEISP, DOJ currently supports multiple frameworks and formats for data exchange between law enforcement information systems, domestically and internationally. Frameworks and formats relevant to voice biometric data interoperability are summarized below.

"DOJ Information Technology Strategic Plan 2008–2013" gives DOJ's perspective on the importance of interoperability. It states:

> Because of the importance of the central role in facilitating information sharing among these key entities, implementing interoperable and integrated technology to support these mission processes is the most critical role of the DOJ CIO. To accomplish this, the DOJ CIO needs to lead the effort to both standardize and consolidate key infrastructure to allow intra-agency and cross-agency sharing of data, information, and applications and to leverage the use of existing, and the creation of new, enterprise solutions that will dramatically improve mission results. [7]

One of this report's tasks is to determine how various DOJ frameworks for domestic data sharing do or do not impact the development of a voice biometric interoperability standard that requires an international scope with the goal of making recommendations for the future. This subsection traces the development of FBI biometric data exchange standards over the last 25 years and discusses the various framework options that now exist.

4.2.1 Current American National Standards Institute (ANSI)/NIST Data Format Standards

The earliest automated and semiautomated methods for human recognition used by the FBI involved fingerprints. Consequently, the first interoperability standards were for fingerprints. The development, and subsequent international success, of the FBI fingerprint interchange standards provides an interesting historical model for voice

biometrics. The current exchange format presents an important framework for potential use with voice biometrics.

Before 1985, no work had begun on electronically exchanging fingerprint data between criminal justice agencies or between similar/dissimilar Automated Fingerprint Identification Systems (AFIS). At that time, the FBI operated the largest AFIS, but systems for the Royal Canadian Mounted Police, St. Paul Police Department, and San Francisco Police Department were becoming operational. Other larger state systems were in development, and a different vendor manufactured each system. Despite that the matchers for each AFIS were based on processed data known as minutiae, it was not possible to electronically exchange truly meaningful data between any of these systems.

To search multiple AFIS without physically exchanging fingerprint cards, an interoperable method to electronically exchange fingerprint data was needed. In 1985, NIST, FBI, vendors, state and local users, and other interested parties developed the first ANSI standard for electronically exchanging fingerprint information. Standards approved by ANSI are recognized as having been developed in an open and consensual manner, obtaining user support. Due to bandwidth and time limitations, this standard was based on minutiae, even though images are preferable for enhanced matching. The standard was never instantiated in an operational system or tested for commonality of implementations or impact on matcher accuracy.

However, by the early 1990s, the transmission of fingerprint images had become more commonplace as communication technology improved. At the same time, the FBI was updating its operation into an image-based environment. As a result, NIST, the FBI, and its stakeholders updated the original standard to an image-based standard. This standard, ANSI/NIST-Computer Systems Laboratory 1-1993, served as an essential building block for the FBI's Integrated AFIS (IAFIS) program. The standard provides a common representation for exchanging fingerprint and biographic data among systems in an interoperable manner. The Immigration and Naturalization Service Automated Biometric Identification System (IDENT) used for the border-checking application also was based on this standard.

The standard was updated again in 1997 to allow data exchange for facial images and scars, marks, and tattoos (SMT). Additional revisions to the standard took place in 2000 and 2007, introducing additional enhancements to the standard and including palm, iris, and other types of biometric information. This standard is extremely open, allowing "domains of interest" to determine the specifics of their own implementations. For example, the FBI and its partners implement the ANSI/NIST standard using the Electronic Biometric Transmission Specification (EBTS), which contains a description of operational concepts, descriptors, field edit specifications, image quality specifications, and other information related to IAFIS services. Other domains can establish their own exchange agreements with their cultural specifics — for example, specifying the metric measurement system. Consequently, the ANSI/NIST standard has become the de facto international standard for exchanging fingerprint, face, and SMT data. INTERPOL (The International Criminal Police Organization) uses this system when sending or receiving

fingerprints from any of its 187 member countries, and national AFIS across Europe use it.

In 2008, an eXtensible Markup Language (XML) version of the ANSI/NIST- Information Technology Laboratory (ITL) 1-2007 standard was released as ANSI/NIST-ITL 2-2008. [7] The current 2007 standard and its XML equivalent define the content, format, and units of measurement for exchanging fingerprint, palm print, facial, SMT, iris, and other biometric sample information that may be used for identifying and verifying a subject. [8] Neither the FBI nor any U.S. federal government agency has yet implemented the XML format for biometric data exchange.

An ANSI/NIST transaction consists of several types of logical records, each devoted to a specific representation of information. A properly formed ANSI/NIST transaction can contain all the relative information pertinent to a single subject. Such a record may include the subject's physical characteristics, identification information, fingerprints, facial image, palm images, iris images, descriptions, SMT images, and past criminal history. Voice data is not included in the format.

The ANSI/NISTITL-12007 standard (called "Part 1" in this report) was developed as a binary transmission format with some American Standard Code for Information Interchange (ASCII) fields and records. The ANSI/NIST standard's content was agreed upon by consensus in accordance with ANSI/NIST procedures. A special XML work group was formed to develop the 2007 standard's XML version (called "Part 2" in this report). The goal was to describe a one-to-one correspondence of XML elements to the numerically tagged conventional elements described in Part 1.

Another goal of the Part 2 work group was to define an XML representation that conforms to NIEM. The Part 1 conventional standard defines three logical records for exchanging ASCII textual information fields, six logical records for exchanging binary information, and seven tagged-field record types for exchanging a combination of ASCII and image data within a single logical record structure. For Part 2, the distinction between ASCII and binary information is gone. All records are ASCII with ASCII XML element tags. All binary image data is converted to ASCII using Base64 encoding and contained within a <nv:BinaryBase64Object> element. Part 2's Annex F is an example XML instance document file containing all logical record types and illustrating the use of every data element.

Parts 1 and 2 will be updated and released simultaneously. This will require XML experts to define the elements carefully and coordinate efforts with NIEM. In addition, the International Organization for Standardization (ISO) has formed a group in Standards Committee 37 to develop naming conventions for XML versions of its standards. One goal is to harmonize these efforts to ensure maximum interoperability. A major thrust of next year's update will be including DNA and voice data, and correcting any flaws in the standard's current binary and XML versions. Updating the ANSI/NIST standard will necessitate modifications to the current EBTS exchange agreement. Current plans for updating the ANSI/NIST standards include a stakeholder's conference in late July 2010.

4.2.2 NIEM

In accordance with "DOJ Information Technology Strategic Plan 2008–2013," the Criminal Justice Information Services Division (CJIS) and the FBI's Next Generation Identification (NGI) system are committed to the NIEM, although CJIS and the FBI will continue to accept and respond to the currently used ANSI/NIST ITL-1 2007 compatible-transactions indefinitely.

In February 2005, DHS and DOJ entered into an agreement to support a joint NIEM for exchanging data within their domains, including justice, person screening, and intelligence information. The DOJ Office of the CIO has "adopted NIEM as the standard for documenting information exchanges." [6] NIEM is written within the linguistic culture of XML, but it is incorrect to think that semantically correct XML is equivalent to NIEM conformance. NIEM designates a collection of "name spaces" (discussed below) defining recognized existing element structures and implementation constraints on XML structures. NIEM conformance requires semantic integrity and consistency across all NIEM documents with active reuse of existing NIEM elements whenever possible. Specifically:

> Semantic Integrity — NIEM information exchange standards: (a) are reflected in the model in a coherent and consistent manner; (b) use the model and governance constructs in a consistent manner; and (c) are documented in a complete and actionable manner. The result is a model that ensures semantic integrity by guaranteeing that data content reflects allowable values. [9]

It is DOJ policy that:

> The information model for a service generally should be built from components in one or more domain vocabularies to promote semantic interoperability. In the justice domain, the information model for services should be built from components in the NIEM when NIEM components exist that satisfy the semantic requirements of the model. [10]

For these reasons, NIEM-complaint documents cannot be created from existing data exchange formats through simple, machine-style translation of syntax even if preserving semantic content. NIEM-conformance must be built into the document during its initial specification, as this report will explain.

NIEM is strictly a U.S. national standard with no international equivalent. Although the ANSI/NIST ITL-1 2007 standard has been translated into a NIEM format and a new ANSI-NIST name space has been created for the document's existing elements, knowledge of the NIEM approach has not yet filtered into speaker recognition or international standards communities. Existing voice data exchange protocols within the NIST/National Security Agency (NSA) community for supporting the NIST Speaker

Recognition Evaluation (SRE) program are not compatible with NIEM. [11] Further, no biometric standard has ever been initially written within the NIEM framework.

Central to the NIEM culture is "evangelism," "enthusiasm building," and ensuring "consistent and articulate messaging regarding the goals, benefits, and operations of NIEM." [9] It is not clear that this committee has that responsibility. Rather, this committee's responsibility is to outline a path forward for at least the CJIS portion of the speaker recognition community. The committee will also promote interoperability consistent with the installed base of criminal justice information exchange systems at the federal, state, local, and tribal level; the domestic NIEM culture; and the broader international community, who are not stakeholders in the NIEM process.

4.2.2.1 NIEM Name Spaces

NIEM uses XML to express its constructs. For XML documents from different sources to be interoperable, there needs to be agreement on the meaning of element names or at least agreement that different documents may use different element names or the same names with different meanings. For these reasons, XML documents refer to name spaces that list and define elements. XML documents begin by referencing the relevant name spaces in the document. In XML, eXtensible means elements in the referenced name spaces can be modified within a document to meet document-specific requirements.

NIEM has defined multiple name spaces, including a "core" name space and additional name spaces for justice, (human) screening, and intelligence applications. These various name spaces have elements related to biometrics. In converting the ANSI/NIST ITL-1 2007 standard to NIEM, an ANSI-NIST name space was created. [12].

4.2.2.2 Biometric Elements Currently Within NIEM

Table 1 lists some existing biometric elements within NIEM. Some pertain directly to voice data but all, even those within the justice and ANSI-NIST name spaces, appear unsuitable for reuse by the voice biometrics community, as those elements are outside of the voice conceptual framework. Consequently, using XML for voice biometric data interchange will require creating a voice name space within the NIEM environment.

Table 1: Existing Biometric Elements Within NIEM

NIEM Name Space	Element	Definition
NIEM Core	BiometricAccuracyDescriptionText	A description of the believed accuracy of the biometric type
NIEM Core	BiometricStatus	The status of a biometric sample. Example, tested/scheduled
NIEM Core	BiometricEncodingMethodText	Method used to encode a biometric
NIEM Core	BiometricTestDescriptionText	A description of how a

NIEM Name Space	Element	Definition
		biometric sample was tested
NIEM Core	BiometricValueText	A textual representation of the value of a biometric
NIEM Core	PersonCircumcisionIndicator	
Justice	PersonSpeechPattern	A representation or an encoding of the identifying characteristics of a person's speech pattern
Justice	PersonAccentText	A pattern of speech with which a person speaks
Screening	BiometricSource	The system of record that captured the PERSON BIOMETRIC
Screening	QualityConfidenceLevelText	The quality score of the accuracy and readability of the recorded PERSON BIOMETRIC
Screening	QualityThresholdText	The acceptance level of the accuracy and readability of the recorded PERSON BIOMETRIC
ANSI-NIST	CaptureDeviceModelText	The model of the image capture device
ANSI-NIST	CaptureDescriptionText	Type of human monitoring used to capture an image
ANSI-NIST	CaptureSourceText	Source of an image
ANSI-NIST	CaptureResolution	A minimum or native resolution indicator
ANSI-NIST	QualityValue	Predicted matching performance

4.2.2.3 NIEM Information Exchange Package Documentation (IEPD) Development

Developing a NIEM-compliant standard requires developing an IEPD. The developer must determine metadata requirements and create a graphical model of the content to be exchanged within the "exchange model." This required content must be mapped into components into existing elements in the various NIEM name spaces. NIEM develops and provides the Subset Schema Generation Tool, an online tool to assist in reducing NIEM to just the subset of data objects needed in any specific business case.

The developer may find some required elements already available within the appropriate name spaces, but other requirements may not match, or only partially match, elements already within NIEM. A component-mapping template in the form of a spreadsheet is available from http://niem.gtri.gatech.edu/niemtools/home.iepd.

In this process of mapping requirements to existing elements, the NIEM golden rule is: "Don't corrupt the semantic integrity of the NIEM model." This means avoid mapping NIEM objects to application requirements because they are "kind of close." Consequently, developers must be well acquainted with existing NIEM objects in the NIEM core and relevant (i.e., intelligence and justice) domains. However, NIEM training materials warn that NIEM can be inconsistent on conceptual mappings within NIEM and across domains. Consequently, each project team must have someone with knowledge of all relevant NIEM objects' full semantic meaning.

NIEM was constructed within a limited cultural context, and NIEM objects may not be structured in the same way as data objects in the data exchange model of the application of interest. An example is person, which does not have a name, but contains a personName object. A personName object contains first, middle, and last names. Persons are assumed to have only one first name, middle name, and last name. With the exception of an extension for "Iberian" names (having two last names), there is no accommodation for persons with multiple or hyphenated first names, with no last name, or with multiple or multiple word last names. These naming conventions require NIEM extensions. Consequently, the NIEM core or interest domains are not expected to contain elements closely linked to the requirements of human recognition using voice signals in an international domain. A significant extension of existing NIEM elements will be required to deal with the requirements of voice biometrics.

4.2.3 The Justice Reference Architecture (JRA) and Justice Information Exchange Model (JIEM)

To augment NIEM, DOJ is creating a JRA in its Global Justice Information Sharing Initiative (GLOBAL). [10] Key GLOBAL documents make no, or only marginal, mention of NIEM. [13, 14] One GLOBAL document indicates flexibility within the JRA messaging system regarding NIEM conformance. [15]

The National Consortium for Justice Information and Statistics, previously the System for the Electronic Analysis and Retrieval of Criminal Histories (SEARCH), a nongovernmental organization partnered with CJIS and DHS, created a JIEM to support data exchanges within the JRA and seems to be the bridge from JRA to NIEM. [16] JIEM "addresses the full range of information sharing use cases … (and) provides a comprehensive blueprint for implementing interoperable data sharing services and capabilities." JIEM allows "users to leverage content defined in XML-based standards, such as the NIEM." This seems to indicate that JIEM is not restricted to using only NIEM elements, which would allow JIEM documents to bring in other name spaces, such as the future ISO/International Electrotechnical Commission (IEC) Joint Technical Committee

1 (JTC1) SC37 work. JRA and JIEM documents do not reference ANSI/NIST ITL Parts 1 or 2, so the relationship between JRA, JIEM, and current CJIS biometric information exchange formats is not clear.

4.2.4 LEISP

Prior to IRTPA's mandated creation of the ISE, DOJ defined the "LEISP," which is a "program" and not an information system. [4] The program creates a forum for collaboration on information sharing within the multijurisdictional law enforcement domain. DOJ established an LEISP Coordinating Committee to oversee this work. LEISP creates a "National Information Sharing System" that has two components: the National Law Enforcement Data Exchange (N-DEx) and OneDOJ, formerly the regional data exchange. Both N-DEx and OneDOJ are Justice Information Services, as are IAFIS and NGI. Within LEISP is the Intra-DOJ Information Exchange Architecture Infrastructure, based on NIEM XML exchanges, as outlined in the LEISP Exchange Specification (LEXS) described below, for providing data to N-DEx and OneDOJ. LEISP is concerned with the exchange of audio and video content within N-DEx and OneDOJ, but it is not clear from LEISP documentation whether IAFIS and NGI are specifically excluded from LEISP considerations.

4.2.4.1 N-DEx

The FBI's Law Enforcement N-DEx is a system that provides information sharing for law enforcement investigators. It provides access to incident and case reports, booking and incarceration data, and parole/probation information uploaded by federal, state, local, and tribal law enforcement agencies. Currently, there are more than 50 million records available, with approximately 60 percent loaded by the State of Texas Department of Public Safety. N-DEx provides link analysis tools that support and enhance basic searches. The tool set is intended to expose previously unknown links among seemingly isolated criminal events or suspicious events that occur in disparate jurisdictions. Search results can include geographical links displayed on a map, bar graphs showing frequency of events, etc.

The N-DEx program developed a Law Enforcement N-DEx IEPD v. 1.0.1. It was based on version 1.0 of the NIEM. This system's IEPD is based on the NIEM IEPD Template Requirements document and contains written documentation, schemas, instance documents, a style sheet, a mapping spreadsheet, and additional documentation. User access is typically via the Law Enforcement On-line system or CJIS Wide Access Network. The files can include facial images, fingerprint images, and textual data.

4.2.4.2 OneDOJ

OneDOJ is DOJ's repository for sharing criminal law enforcement information, such as open and closed case documents and investigative reports. It is not clear whether OneDOJ will interface directly with NGI to allow biometric data sharing. Interconnection

with OneDOJ is accomplished through an open, XML-based, NIEM-compliant standard called LEXS-Search and Retrieval.

4.2.5 LEXS

LEXS is a data exchange model within DOJ that supports N-DEx and OneDOJ. There is some disagreement within DOJ as to what the acronym stands for. The DOJ Office of the CIO gives the name as "Law Enforcement Exchange Standard," while other DOJ documents use the terms "Logical Entity Exchange Specification" and "LEISP Exchange Specifications" [6, 16, 17]. We believe that all uses of the term "LEXS" refer to the same specification. LEXS is a NIEM-based framework that specifies an approach to IEPD development but goes beyond NIEM to allow creation of "partner exchange systems" (stovepipes and mission-oriented domains) between two or more entities. The clear advantage of such partner exchange systems is that each partner can query the other's system without creating a common database. Thus, each partner "owns" its data. Under current policy, DOJ "continues to expand on the integration of LEXS and NIEM across the DOJ … and will work with its federal and (state, local, and tribal) partners for opportunities in reusing the NIEM and ISE standards." [6]

LEXS specifically provides support for "rich media attachments (e.g., photos, audio recordings, video footage.)" [17] LEXS could form the basis of a NIEM-compliant voice biometric exchange protocol.

Several other criminal justice communities (e.g., the European Union) are developing similar IEPD exchange domains. They are mostly incompatible with one another as they are appropriately inwardly focused. This limits LEXS' usefulness for the international exchange of voice biometric data.

5. Existing Standard Formats for Voice Data Storage and Transfer

Below are current and developing standards for voice data storage and transmission that may be relevant to this project.

5.1 International Committee on Information Technology Standards (INCITS) 456

Despite its name, the INCITS is a U.S.-focused committee operating under the rules of the American National Standards Association. INCITS develops Information and Communication Technology standards for use primarily in the U.S. The INCITS 456 standard is based on the approach used by the Common Biometric Exchange Format Framework (CBEFF) although use of the CBEFF header is optional. INCITS 456 has reached the public-comment stage via M1, the ANSI INCITS biometrics committee. Some of INCITS 456's characteristics that support law-enforcement use cases are:

1. Supports any spoken input — INCITS 456 supports text-independent, freeform, and constrained speech. The ability to exchange freeform speech is essential for core FBI and law-enforcement use cases, such as forensic analysis, surveillance, and intelligence gathering.
2. Allows constrained audio formats — The draft standard allows raw data interchange. Because raw data can potentially be stored using any of hundreds of audio formats, restricting supported audio formats is essential for effective data interchange. Many audio formats — including the most popular ones (e.g., MP3) — are proprietary. The popular .wav format and the NIST Speech File Manipulation Software (SPHERE) format are shells that allow variations that may not be supported by agencies sharing the data. The .wav format in particular has more than 100 variations.
3. Identifies language and dialect — The draft standard identifies language and dialect used in the spoken data (based on ISO 639, a geography-based coding). These features are useful for the FBI and other sophisticated agencies that can use the information to improve speaker identification and verification (SIV) engines. This information can facilitate higher-level analysis that may be needed to enhance the confidence of automated, semiautomated, or manual data analysis.

These are only a sample of the interoperability support INCITS 456 provides law enforcement. That support can be enhanced through direct modifications of the draft standard and formulation of application-specific data interchange formats that are sometimes called "application profiles" or "domains."

5.2 ISO/IEC 19794-13

In 2004, the international standards committee on biometrics, ISO/IEC JTC1 SC37, proposed the development of a voice data format standard. That standard is currently at the working draft stage and has been divided into three parts: common introductory material, a binary implementation compatible with other biometric data format standards developed by SC37, and an XML version. Work has begun on developing an SC37 name

space for the XML version, as well as for other SC37 documents migrating toward the XML framework. Because this is an international standard and NIEM is a U.S. information exchange model, the XML version is not anticipated to be NIEM-compliant, or even acknowledge NIEM's existence.

ISO/IEC 19794-13 will not be within the DOJ Office of the CIO mandates to use NIEM elements. Nonetheless, some work by SC37 on metadata requirements may be applicable to this project, so the progress of ISO/IEC 19794-13 should be monitored.

5.3 SPHERE

The data developed at the Linguistic Data Consortium for use in the NIST/NSA SRE program is distributed in the SPHERE format. Because SRE participation is international, the standard is recognized throughout the international voice biometric community. Its ASCII text header begins with a label of the form NISTxx, where xx is a version code followed by the number of bytes in the header. [18] The remainder of the header is shown in Table 2.

Table 2: SPHERE Header Data

sample_rate	Sample rate in Hertz
sample_n_bytes	Number of bytes in each sample
sample_count	Number of samples in the file
sample_byte_format	Byte order
sample_coding	Speech coding (e.g., pulse code modulation, mu-law, shortpack)
Channels_interleaved	Indicator for two-channel data

5.4 Biometric Identity Assurance Services (BIAS)

The Organization for the Advancement of Structured Information Standards (OASIS) is an international, not-for-profit consortium that drives the development of commercial standards. They have produced biometric XML standards such as OASIS XML Common Biometric Format (XCBF) . Their current effort in the biometrics arena is an initiative they call INCITS project 1823-D, BIAS for biometric exchange (including voice) under XML. Both DOD Biometrics Task Force and DHS contractors participate in this effort.

According to the OASIS Web site, the OASIS BIAS Integration Technical Committee complements INCITS' efforts to provide the biometrics and security industries with a documented, open framework for deploying and invoking identity assurance capabilities that can be readily accessed as services. The OASIS BIAS Integration TC defines and describes methods and bindings by which the INCITS BIAS framework can be used within XML-based transactional Web services and service-oriented architectures (SOA). It is not known whether this effort will mature in time to be considered within our project. [19]

6. Metadata Requirements Discovered by Use Case Committee

One of the most important tasks that must be tackled in developing a voice interoperability framework and standard is to determine the metadata that will accompany the voice signal. This metadata may be of two kinds: mandatory and optional. The Use Case Committee's report includes a listing of the kinds of metadata needed by typical use cases. That list can serve as a guide to developing metadata requirements for interoperability standards and is repeated here.

6.1 Audio Session Information

1. Sensor type (e.g., cell phone, wireline telephone, telephone intercept/tap, internal tape-recorder microphone (mic), internal digital-voice recorder mic, separate microphone, body/wire mic, covert room mic, laser vibrometer, accelerometer, fiber-optic stethoscope, or unknown).
2. Sensor placement (e.g., handset held close to mouth, desktop microphone 18 inches from lips, or unknown).
3. Channel type and bandwidth (e.g., narrowband telephone, wideband broadcast television (TV), narrowband high-fidelity radio, cassette tape, digital audio tape, minidisc, microcassette, or solid-state digital voice recorder).
4. Channel conditions (e.g., clean, noisy, echo, dropouts, or fading).
5. Data: (a) file-based recordings (e.g., Resource Interchange File Format, .wav, headerless, or streaming audio); (b) stream-based media, audio, or audio/video (e.g., RealNetworks' RealAudio, streaming MP3, Macromedia's Flash and Director Shockwave, Macromedia/Adobe Flash Video H.263/H.264 VP6/ High-efficiency Advanced Audio Coding (AAC), Microsoft's Windows Media Audio/Active Streaming Format, and Apple's QuickTime); (c) stream-based telephony Voice over Internet Protocol (IP) (VOIP) (e.g., IP Phone, Session Initiation Protocol (SIP) Phone, Skype, America Online Voice Chat); and (d) Digital circuit switched (e.g., T1, T3, optical carrier (OC) 3, OC-12).
6. Coding/compression (e.g., G.711 μ-law, G.711 A-law, Global System for Mobile Communications Enhanced Full Rate cellular voice coder, Code Excited Linear Production (CELP) voice coder, algebraic CELP voice coder, G.726 Adaptive Differential Pulse-code Modulation (ADPCM), G.722 split-band wideband ADPCM, MP2, MP3, AAC, MP4).
7. Single channel (all talkers recorded on the same monaural channel) or multichannel (e.g., two talkers on separate stereo channels).
8. Acoustic conditions (background noise and sounds, such as radio/TV/music, wind noise, background talkers, reverberation).
9. Environment (e.g., home, office, car, outdoors, subway station, restaurant, booking station, interrogation room).
10. Number and durations of known samples and questioned samples.
11. Time span between samples and range.
12. Additional information: note any mismatches between questioned and known samples' audio session information.

6.2 Speaker Session Information

1. Style (e.g., spontaneous, conversational, telephone speech, face-to-face conversation, commands, read speech (what material was read?), question answering, broadcast speech, orated speech).
2. Language(s)/dialects(s) spoken
3. Speaker state (e.g., stress, emotion, mentally impaired, intoxicated, medicated).
4. Cooperative or uncooperative.
5. Witting or unwitting.
6. Session data useful for processing this use case (e.g., date and time, telephone number, IP address, geographic location).
7. Pointers to other sources that are typically linked to this kind of use case.
8. Additional information: Note any mismatches between questioned and known samples' speaker session information.

6.3 Speaker Information

1. Speaker characteristics (e.g., name(s), sex, age/birth date, occupation, place of birth, place raised, race, ethnicity, years of education, native language/dialect, other language(s)/dialect(s), speech impairments/pathologies, social network).
2. Additional information

7. Privacy

An oft-heard expression within the privacy literature is that "privacy must be built in, not added on." Consequently, privacy considerations must be considered early in the process of creating a voice biometric interoperability standard. According to DOJ:

> Privacy Impact Assessments (PIAs) are required by Section 208 of the E-Government Act for all federal government agencies that develop or procure new technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing technology for managing information in identifiable form. [20]

The FBI filed a PIA for the national security enhancements required for IAFIS. Prior to fielding any government voice biometrics system within the U.S., the government will be required to create and file a PIA. [21]

Voice biometric information must be personally identifiable or it is not biometric information. Therefore, it must be treated in accordance with restrictions on personally identifiable information. Some nongovernment agencies, such as the National Criminal Justice Association, have developed useful guidance for developing privacy policies for justice information systems containing personally identifiable data. The National Criminal Justice Association states:

> Organizations must clearly identify and document the purposes for collecting personal information. System design must ensure that the system's outcome is limited to the purposes for which the personal information was lawfully collected and disclosed. We must pay attention during the design stage in all instances where personal information is disclosed regularly to one or more parts of the justice system. We must also pay attention to the building of a technology that easily enforces access restrictions to personal information available to parties outside the justice system. [22]

There may be subtleties in the proposed collection effort that require specific consideration. For example, there may be different privacy implications between read and conversational speech. Prompted speech might raise legal difficulties depending upon the status of the person being prompted (i.e., criminal) and the content of the prompt. There are also basic privacy issues in reuse of speech collected for one purpose but used for another, such as using calls to 911 data centers for identifying persons.

Creation of a voice biometric interoperability standard will require careful considerations of privacy implications and, perhaps, the creation of a privacy policy specifically for collected speech.

8. Options Moving Forward

One of the Symposium on Investigatory Voice Biometrics' fundamental goals was to initiate a multiyear program to develop investigatory voice biometric collection and interoperability standards. Initiating development of interoperability standards will require some decision making about a preliminary direction. The committee sees two potential paths forward: to build a record type for the existing ANSI/NIST ITL-1 "Data Format for the Interchange of Fingerprint, Facial, and SMT Information" format or to move directly to an LEISP-mandated LEXS NIEM-compliant format. Both options are discussed below.

8.1 Building an ANSI/NIST ITL-1 Compliant Data Format

As indicated in Section 4.2.1, the ANSI/NIST standard (Part 1 and 2) have undergone revisions to include new face, palm, and iris biometric modalities. A voice record can also be developed for inclusion if the basic principles of openness and consensus are followed. Anyone with a direct or material interest in developing any record type will be able to participate by submitting comments, suggestions, or modifications. NIST will properly evaluate all submissions. Once a proposed record type has been developed, it must attain a consensus approval before becoming part of the standard. NIST is responsible for ensuring all ANSI-mandated procedures are properly followed.

To initiate the development of a voice record type, a champion for such a record should first identify the stakeholders, including major vendors. Opinions regarding the style and content of the record should be solicited from each stakeholder if possible.[2]

Where differences of opinion exist, efforts should be made to obtain agreement or compromise on any conflicting issues or opinions. Once all of this information has been gathered, an initial draft of a proposed record should be written and circulated to all identified stakeholders for comment. Multiple cycles of updating the draft and recirculation may be necessary. Public workshops are an excellent way to gain insight into material for inclusion, discuss points of contention, and are mandated by the ANSI process. Such a workshop may be used to discuss one or more topics associated with an update to the standard. Once content for the new record type appears stable and objections have been addressed, it should be turned over to NIST to officially process the update via the ANSI approved processes.

The inclusion of a speech record in the ANSI/NIST ITL-1 standard is not tied to any particular schedule. It is possible to update the standard whenever a contribution is ready,

[2] Note that voice could be handled as a separate, new record type or included in Record Type 99 by directly incorporating the INCITS 456 standard with a CBEFF header. Using Record Type 99 would mean that revisions to the content of the voice record would also have to go through the INCITS/M1 approval process.

and it can be placed before the community for a vote. After the ANSI/NIST ITL-1 2007 version has been updated, likely in 2011 given the July 2010 initial public meeting at NIST, the process of approving an XML version can begin.

The advantage of this approach is that almost 100 percent of arrest cycles around the world use some implementation of the ANSI/NIST ITL-1 standard for exchanging booking data. By 2015 the FBI and others envision collecting the majority of their reference files at time of booking. Progressing a voice data standard though ANSI/NIST ITL-1 may be the approach least disruptive to the installed database and the substantial investments to date by federal, state, local, and tribal criminal justice agencies.

8.2 Building a LEISP-Compliant Data Format

As indicated in Section 4.2.4, it is not clear whether LEISP is intended to apply to biometric data sharing with such programs as IAFIS and NGI. However, LEISP clearly applies the LEXS to the exchange of audio data on a national (N-DEx) and regional (OneDOJ) level. Therefore, one path forward for voice biometric interoperability would be to consider the LEXS-NIEM approach. This approach, as explained in Section 4.2.2, is much more involved than simply writing a data exchange standard in the XML language or translating an existing standard into XML. LEXS-NIEM conformance requires adherence to a process that produces "semantic integrity by guaranteeing that data content reflects allowable values." [9] Consequently, a decision regarding use of the LEXS-NIEM approach must be made at the beginning, so conformance can be built into the standard from the ground up. LEXS can directly incorporate an ANSI/NIST-ITL XML implementation.

8.2.1 Conformance Difficulties with NIEM

The NIEM philosophy, which is supported by "DOJ Information Technology Strategic Plan 2008–2013," is that existing NIEM components be reused if possible rather than creating local elements or extensions. The NIEM culture also values semantic consistency, using NIEM components in accordance with their adopted definitions.

Current NIEM biometric and voice components, even within the justice and ANSI-NIST name spaces, may not be appropriate in content or appropriately named. One challenge presented in attempting to create a NIEM-compliant data format will be to reconcile requirements with the current concept system already embedded within NIEM name spaces. One approach could be to develop a new name space, say "Voice," to hold elements consistent with the concept system in place within the voice community.[3] This

[3] ANSI/NIST ITL-2 work group is currently examining establishing a biometrics domain that would be outside of NIEM core and could include terms needed for the voice records. Such a domain could be referenced by groups not directly incorporating NIEM into their implementations but using an ANSI/NIST-ITL structure.

would allow bypassing incoherent elements in the various NIEM domains even if similarly named.

A second approach would be to work with the NIEM Program Management Office to modify the existing components to better reflect the scientific conceptual systems of the voice and greater biometrics community. This second approach would allow conformance with the NIEM goal of semantic integrity and consistency across all NIEM applications, but it would require working with other communities that support paradigms incommensurate with those of our community. Further, if an investigative voice biometric interoperability is to extend internationally for transmission of data to and from the FBI, embedding U.S.-based NIEM conformance into the standard may find little traction with international partners.[4]

[4] The ISO/IEC SC37 is examining how best to develop an XML implementation of the biometric standards developed in SC37. The current concept is to maintain as much consistency with ANSI/NIST-ITL as possible without incorporating NIEM schemas or name spaces, since NIEM is a U.S.-based and -maintained construct. The establishment of a biometrics domain outside of NIEM core but consistent with NIEM naming practices may assist in this interoperability.

9. Conclusions

As a result of the symposium, the committee recommends the following:

1. Examine the various options presented in Section 8 in greater detail. The examination is to determine: (a) the viability of each; (b) the utility of each for voice; and (c) the impact on interoperability of voice with other biometrics.
2. Further investigate what would be required to establish a privacy policy/standard that supports the needed interoperability.
3. Investigate the utility of adopting or adapting ANSI and ISO interoperability standards to investigatory interoperability needs. This recommendation is to save time and effort and to minimize potential errors by learning and using existing standards.
4. Adopt a more proactive role in developing ISO/IEC standards to influence their direction. Although these standards are not being developed within the context of existing FBI and DOJ biometric data format standards and interoperability mandates, they are currently in process and do address investigatory needs. Consequently, greater FBI involvement in the development of these standards could produce a standard more quickly than some other directions suggested by this report.

10. Appendix

This appendix discusses some additional voice standard development activities.

10.1 Voice XML

The Voice XML Forum is an international standards body serving the speech-processing industry. It was formed in 1999 by AT&T, IBM, Lucent, and Motorola with a mission to establish a standard language for speech-processing technology that would support communication between telephone and Internet channels. The Voice XML Forum released Voice XML version 1.0 in 1999, and the Forum established a partnership with the World Wide Web Consortium (W3C) in 2000 to co-develop standards for speech-processing technologies that would enable them to operate on the Internet and interoperate with other Internet standards.

Today, the Voice XML Forum has approximately 400 members and participants from the following countries: Australia, Belgium, Canada, Finland, France, Germany, Israel, Italy, Korea, Mexico, South Africa, Spain, the United Kingdom, and the United States. Voice XML Forum members and others have produced more than 10,000 deployments of applications that use the Voice XML standard. The Voice XML Forum's Speaker Biometrics Committee (SBC), established in 2005, has a mission to extend the Voice XML language to include speaker recognition. Among its responsibilities is to establish requirements for adding speaker recognition to Voice XML, create a glossary of terms, develop informational and educational materials related to speaker recognition technology and deployments, and collaborate with M1 to create a data exchange format for speaker recognition.

In April 2009, INCITS released a draft version of a speaker data exchange format known as INCITS 456. This work is the product of collaboration between the SBC of the Voice XML Forum, a liaison member of M1, and ANSI/INCITS/M1 (biometrics). It defines a method for characterizing speech produced by an end user for biometric enrollment, verification, or identification predicated on the concept of a session and turns within the session. It supports transmission of raw speech data with an optional extension for proprietary data. It defines the attributes needed to generate a voice model from the session and turns, and it includes a use case example and a sample XML schema. This document constitutes the considered opinion of representatives from SIV vendor, integrator, and consulting organizations.

10.2 Media Resources Control Protocol (MRCP)

The first version of MRCP (MRCP V1) is a widely used standard developed jointly by Cisco Systems, Inc., Nuance Communications, and SpeechWorks Inc. [23] It was created to manage the use of voice-related resources and support transport of speech data in SOA and interactive voice-response environments. It is typically used for real-time interactions.

MRCP mediates between the servers that house the speech resources, called media processing resources, and the applications or other entities on the network, called clients, that need to communicate with them. An interaction between a client and a media resource server is called a session. MRCP specifies the messages that may be sent between the client and a resource server, how the resources are to be used, and how these messages are to be carried over a transport layer.

10.2.1 MRCP V2

MRCP V1 does not explicitly include voice biometrics. Support for voice biometrics and other security-related resources was one of the drivers for developing MRCP V2, which is in the final stages of development. [24] Unlike MRCP V1, MRCP V2 is created by a speech-industry consortium within the Internet Engineering Technology Forum (IETF). It also differs from MRCP V1 in that it utilizes SIP, Transmission Control Protocol, and Real-Time Transport Protocol in its operations. As with MRCP V1, MRCP V2 is generally used for real-time operations.

The client uses SIP to start and end sessions and to establish an MRCP control channel with the media server so the client can use the server's media processing resources. Once accomplished, MRCP-compliant commands and functions, called messages, may be sent between client and server. These messages enable the client to control the operation within a session. They include commands to start and end sessions, verify, identify, and get intermediate-level results.

Multiple resources may be managed within a single session or separate sessions may be created for each resource. For example, there may be a single session for a speech-recognition resource and a voice-biometrics resource that allows both resources to operate on the same utterances. Also, separate sessions may be created for both resources to enhance their ability to operate on different utterances. The same approaches, single or multiple sessions, may be employed with two or more voice-biometrics resources.

11. References

[1] ISO. "Text of Working Document Standing Document 2, Version 11 (SD 2), Harmonized Biometric Vocabulary, ISO/International Electrotechnical Commission Joint Technical Committee 1/Special Committee 37 Number 3068, Working Draft 2009-02-28." Available online at <http://isotc.iso.org/livelink/livelink?func=ll&objId=2299739>.

[2] IRTPA of 2004. Pub. L. 108-458. 17 Dec. 2004. S. 2845. Available online at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.pdf>.

[3] Program Manager, ISE, Office of the Director of National Intelligence. "ISE Enterprise Architecture Framework Version 1.0." ISE Enterprise Architecture Framework. August 2007. Available online at <http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf>.

[4] U.S. DOJ, OneDOJ. "LEISP: United States Department of Justice Law Enforcement Information Sharing Program." October 2005. Available online at <http://www.usdoj.gov/jmd/ocio/onedoj_strategy.pdf>.

[5] NIEM. "NIEM Gets a Uniform and Takes to the Seas." NIEM Newsletter. February 2009. Available online at <http://www.niem.gov/newsletter200902.php>.

[6] U.S. DOJ. "DOJ Information Technology Strategic Plan 2008–2013." Feb. 28, 2008. Available online at <http://www.usdoj.gov/jmd/ocio/2008itplan/08it-strategic-plan.pdf>.

[7] NIST and the U.S. Department of Commerce. "Information Technology: American National Standard for Information Systems — Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information — Part 2: XML Version." NIST Special Publication 500-275. Eds. E. Newton, G. Coleman, and P.Yuh. August 2008. Gaithersburg, MD: NIST, 2008. Available online at <http://fingerprint.nist.gov/standard/Approved-XML-Std-20080828.pdf>.

[8] NIST and the U.S. Department of Commerce. "Information Technology: American National Standard for Information Systems — Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information – Part 1." NIST Special Publication 500-271. Eds. R. Michael McCabe and Elaine M. Newton. May 2007. Gaithersburg, MD: NIST, 2007. Available online at <http://www.itl.nist.gov/ANSIASD/Approved-Std-20070427%20(2).pdf>.

[9] NIEM Program Management Office. "National Information Exchange Model Concept of Operations Version 0.5." Jan. 9, 2007. Available online at <http://www.niem.gov/files/NIEM_Concept_of_Operations.pdf>.

[10] The Global Infrastructure/Standards Working Group. U.S. DOJ's Global JRA Specification Version 1.7. March 2009. Available online at <http://it.ojp.gov/docdownloader.aspx?ddid=1072>.

[11] NIST. "The NIST Year 2008 Speaker Recognition Evaluation Plan." April 3, 2008. Available online at <http://www.itl.nist.gov/iad/mig//tests/sre/2008/sre08_evalplan_release4.pdf>.

[12] NIEM. NIEM http://niem.gov/niem/ansi-nist/2.0. Available online at <http://niem.gov/niem/ansi-nist/2.0>.

[13] The Global Infrastructure/Standards Working Group. Globa lJRA Guidelines for Identifying and Designing Services Version 1.0. March 2009. Available online at <http://www.it.ojp.gov/docdownloader.aspx?ddid=1070>.

[14] The Global Infrastructure/Standards Working Group. Global JRA Execution Context Guidelines Version 1.0. March 2009. Available online at <http://www.it.ojp.gov/docdownloader.aspx?ddid=1071>.

[15] The Global Infrastructure/Standards Working Group. Global JRA ebXML Messaging Services Version 1.0. March 2009. Available online at <http://it.ojp.gov/docdownloader.aspx?ddid=1073>.

[16] U.S. DOJ. Logical Entity Exchange Specification 3.1, Revision 8. Jan. 15, 2009.

[17] U.S. DOJ. LEISP Exchange Specification 3.0, LEXS 3.0 User Guide Revision 9. Aug. 8, 2007.

[18] Laboratory for the Recognition and Organization of Speech and Audio at Columbia University. 5.8.4 NIST File Format. Available online at <http://labrosa.ee.columbia.edu/doc/HTKBook21/node64.html>.

[19] OASIS. OASIS Biometric Identity Assurance Services (BIAS) Integration TC. OASIS 1993-2009. Available online at <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bias>.

[20] Privacy and Civil Liberties Office, Office of the Deputy Attorney General. Privacy Impact Assessments: Official Guidance Revised Aug. 7, 2006. Available online at <http://www.usdoj.gov/opcl/pia_manual.pdf>.

[21] FBI. FBI – Electronic Questionnaire for Investigations Processing. 2009. Available online at <http://foia.fbi.gov/iafis.htm>.

[22] National Criminal Justice Association. "Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems." Justice Information Privacy Guideline. September 2002. Available online at

1054 <http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformation
1055 PrivacyGuideline/privacyguideline.pdf>.
1056
1057 [23] S. Shanmugham, P. Monaco, and B. Eberman. “A Media Resource Control Protocol
1058 (MRCP) Developed by Cisco, Nuance, and Speechworks.” Internet Informational
1059 Request for Comment 4463. The Internet Society. April 2006. Available online at
1060 <http://www.ietf.org/rfc/rfc4463.txt>.
1061
1062 [24] S. Shanmugham and D. Burnett. “Media Resource Control Protocol Version 2.”
1063 Internet Informational Request for Comment 4463. The Internet Society. August
1064 2009. *This is draft 20. As of August 2009, it was the current draft. Upon final*
1065 *approval, a stable IETF Internet Informational RFC reference number will be*
1066 *assigned.* Available online at <ftp://ftp.ietf.org/internet-drafts/draft-ietf-speechsc-
1067 mrcpv2-20.txt>.