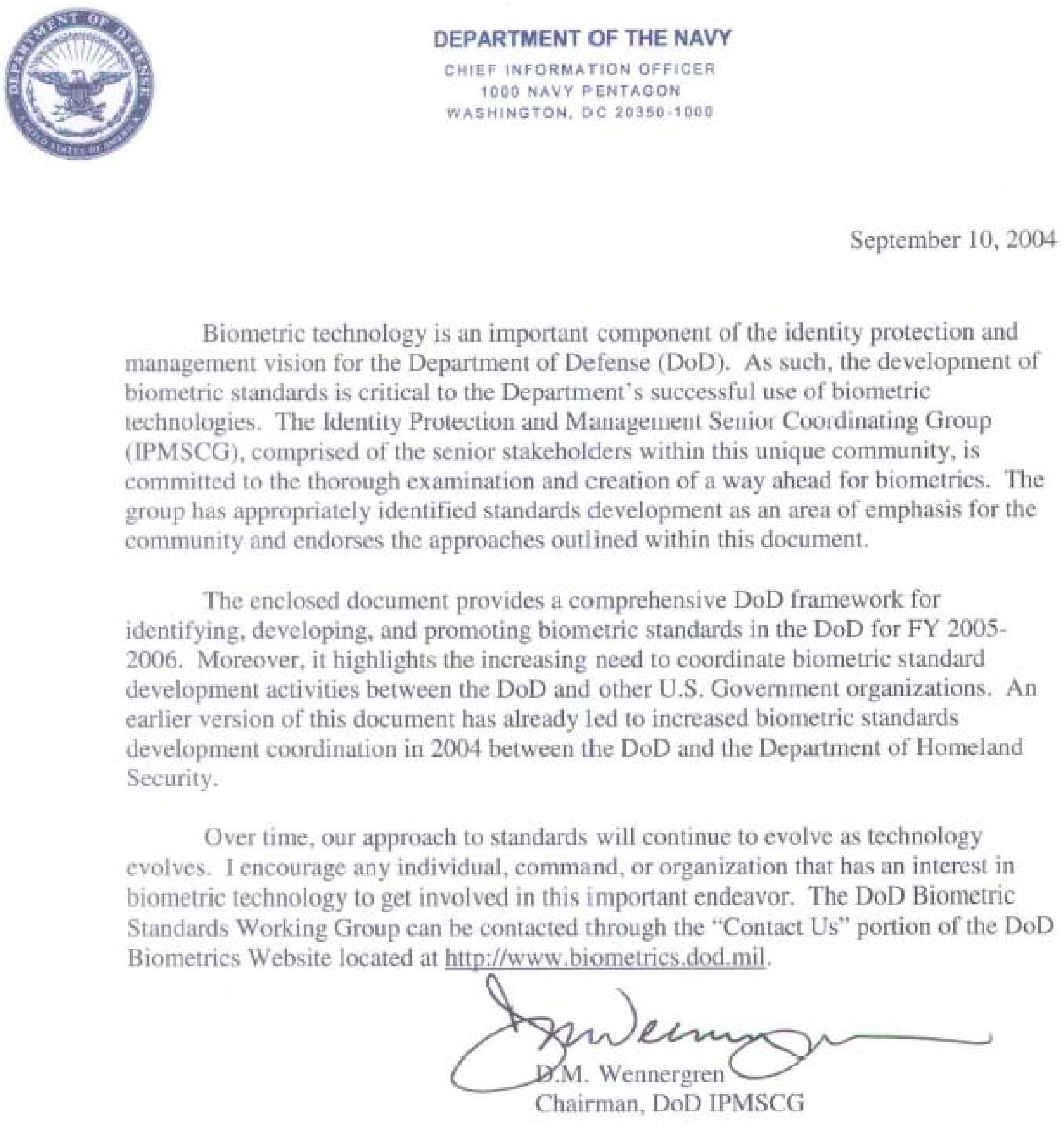
BIOMETRICS
DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE BIOMETRIC STANDARDS DEVELOPMENT RECOMMENDED APPROACH

John D Woodward, Jr.
Director,
Department of Defense
Biometrics Management Office

Arlington, Virginia ● September 10, 2004

Department of Defense Biometrics
Biometrics Management Office
Biometrics Fusion Center
www.biometrics.dod.mil
☎ (703) 602-5427



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

September 10, 2004

Biometric technology is an important component of the identity protection and management vision for the Department of Defense (DoD). As such, the development of biometric standards is critical to the Department's successful use of biometric technologies. The Identity Protection and Management Senior Coordinating Group (IPMSCG), comprised of the senior stakeholders within this unique community, is committed to the thorough examination and creation of a way ahead for biometrics. The group has appropriately identified standards development as an area of emphasis for the community and endorses the approaches outlined within this document.

The enclosed document provides a comprehensive DoD framework for identifying, developing, and promoting biometric standards in the DoD for FY 2005-2006. Moreover, it highlights the increasing need to coordinate biometric standard development activities between the DoD and other U.S. Government organizations. An earlier version of this document has already led to increased biometric standards development coordination in 2004 between the DoD and the Department of Homeland Security.

Over time, our approach to standards will continue to evolve as technology evolves. I encourage any individual, command, or organization that has an interest in biometric technology to get involved in this important endeavor. The DoD Biometric Standards Working Group can be contacted through the "Contact Us" portion of the DoD Biometrics Website located at http://www.biometrics.dod.mil.

D.M. Wennergren
Chairman, DoD IPMSCG

Changes in the September 2004 Version

This document is an augmented and revised version of the *DoD Biometrics Standards Development Recommended Approach* originally developed by the DoD Biometrics Management Office (BMO) in October 2003. The original document outlined the current status of biometric standards and identified areas where the BMO could contribute towards advancing these standards. The document was initially reviewed by the DoD Biometrics Standards Working Group, and then was formally staffed for review by the DoD Biometrics Senior Coordinating Group (BSCG). Overall, 22 DoD organizations provided a total of more than 200 comments on the document.

In January 2004, the BMO released an updated version of the 2003 document, which incorporated comments from the two rounds of reviews. This July 2004 version of the document includes the following changes:

- A discussion of the role of biometric technology and biometric standards in supporting U.S. efforts in the Global War on Terrorism
- A listing of significant BMO standards development accomplishments completed in the first half of 2004
- DoD biometric policy updates approved by DoD senior management in the first half of 2004
- A description of the Person Data Exchange Standard (PDES), a standard developed by the intelligence community for representing biographical information about persons of interest
- Updates to the descriptions and status of several biometric standards based on the progress that took place between January and June 2004

EXECUTIVE SUMMARY

The challenges facing the United States and its coalition partners in the Global War on Terrorism have created an urgent need for the U.S. Government to improve information sharing between organizations and leverage information technology to the greatest extent possible. *Standards* are an essential component for enabling information sharing and technology interoperability.

Biometric technologies have the unique capability of identifying who a person *actually is*, as opposed to who a person *claims to be*. Nowhere is this capability more important to the Department of Defense (DoD) than in fighting the Global War on Terrorism. The Department has undertaken the task of collecting fingerprints and other biometric data from Enemy Prisoners of War (EPW), detainees, civilian internees, and persons of interest with respect to national security, collectively referred to as *Red Force* personnel.

The purposes for collecting and sharing biometric data from Red Force personnel are to:

- Identify potential national security threats
- Link a current person of interest to:
    - Past activities (e.g., match a latent fingerprint left at a terrorist incident to a detainee’s fingerprint)
    - Previously-used identity/identities
- Provide evidence in the prosecution of terrorists
- Fix or freeze identities
- Vet foreign nationals in positions of trust

Collecting Red Force biometric data in an interoperable manner, so that it may be shared between DoD components and between the DoD and other U.S. Government organizations, is of the utmost importance in winning the Global War on Terrorism. *Biometric standards* are the linchpin for achieving this interoperability. This document addresses biometric standards in detail, and explains the relevance and applicability of the standards to the DoD.

On 25 August 2003, Deputy Secretary of Defense Dr. Wolfowitz signed a memorandum titled “Department of Defense Biometrics Enterprise Vision.” In this memorandum Dr. Wolfowitz stated, “By 2010, biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for physical and logical access control.” To support this vision, he directed the DoD Biometrics Management Office (BMO) to perform the following two actions: (1) “ensure that a scalable biometrics component of the Global Information Grid (GIG) infrastructure is in place” and (2) “**ensure that the appropriate standards, interoperability tools, testing frameworks, and approved product validations are available to the DoD community**.”

On February 2, 2004, the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) signed a Memorandum titled, "Department of Defense (DoD) Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from 'Red Force' Personnel." This memorandum directs that electronic fingerprint systems used by DoD components to collect Red Force fingerprint data must (1) conform with the Electronic Fingerprint Transmission Specification (EFTS) that is based on the American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000 and (2) be certified to be interoperable with the FBI's Integrated Automated Fingerprint Identification System. Systems currently in use that do not meet these criteria must either be upgraded or replaced by December 31, 2004. This memorandum does not apply to electronic systems used to collect fingerprint data from U.S. military, civilian, and contract personnel. Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics to ensure that materials, products, processes, and services are fit for their purpose. As such, standards are important and powerful tools for effective information technology systems development, and ultimately support the Global War on Terrorism.

Table ES-1 summarizes the DoD BMO Standards Working Group recommendations regarding adoption of relevant biometrics standards:

Table ES-1. BMO Standards Working Group Recommendations

#	Recommendation	Where Discussed in This Document
1	DoD should use the established Biometrics Application Programming Interface (BioAPI) and Common Biometric Exchange Formats Framework (CBEFF) standards in all DoD implementations of biometric technology.	Section 3.3 Section 3.4
2	DoD should continue its lead role in the development of one or more national DoD biometrics application profile standards.	Section 5.2
3	DoD should continue its lead role in the development of national and international biometrics conformance testing standards.	Section 5.3
4	DoD should assume a lead role in the development of a BioAPI conformance test suite/testing framework.	Section 5.3
5	DoD should assume a contributor role by developing specific technical contributions in the development of national and international biometrics performance testing standards. Responsibilities for this role include tracking progress of the standards, reviewing and providing comments on working drafts, and reporting progress on the standards to DoD stakeholders.	Section 5.4

#	Recommendation	Where Discussed in This Document
6	DoD should assume a contributor role in the development of national and international biometrics data interchange (e.g., template) standards. Responsibilities for this role include tracking progress of the standards, reviewing and providing comments on working drafts, and reporting progress on the standards to DoD stakeholders.	Section 5.5
7	BMO should actively participate in appropriate national and international standards bodies to exert DoD influence on the development and adoption of standards important to DoD.	Section 1.5

Note: This table summarizes the principal recommendations provided in this document.

These seven principal recommendations represent the actions that the BMO believes will have the greatest impact on the development of biometric standards for DoD. Other recommendations also appear throughout this document; however, these are of lesser significance than those listed above.

DoD has the greatest need for biometric standards development in the areas of DoD-specific application profiles and conformance testing standards. The BMO is focusing on developing draft standards to fill existing gaps in these areas, as discussed in Sections 2, 4, and 5.

This document contains five main sections:

- Section 1 identifies the driving factors and current efforts that support development of biometric standards in the DoD. Driving factors discussed include the unique capabilities that biometric technologies provide in supporting the Global War on Terrorism, DoD policy direction on the use of standards, and key interoperability benefits that standards provide the DoD.
- Section 2 provides a deficiency or gap analysis of biometric standards and explains why DoD participation in the development of biometric standards is necessary to overcome shortcomings in the coverage provided by existing biometric standards
- Section 3 provides in-depth discussion of existing biometric standards and their applicability to DoD
- Section 4 covers the biometric standards under development by standards bodies
- Section 5 provides details on the recommended DoD role in advancing biometric standards development in the areas that are of greatest importance to DoD.

The initial (October 2003) version of this document served as a starting point for coordinating the development and advancement of biometric standards within the DoD and among the DoD and other U.S. Government organizations. The document was well received, and led to an inter-agency U.S. Government Workshop on "Biometric Standards in Support of the Global War on Terrorism" in May 2004. The workshop has generated a tremendous level of cooperation between the DoD, the Department of Homeland Security, the National Institute of Standards and Technology (NIST), and other organizations.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION: BIOMETRICS AND THE GLOBAL WAR ON TERRORISM

This section identifies the driving factors and current efforts that support development of biometric standards in the Department of Defense (DoD). The section begins with a brief discussion of the unique capabilities that biometric technologies provide to support the Global War on Terrorism. It describes the key interoperability benefits that standards provide to the DoD, and discusses current standards deficiencies in the commercial biometrics marketplace. The section also explains why DoD participation in national and international standards bodies is necessary to achieve DoD standards objectives.

1.1 The Role of Biometric Standards in the Global War on Terrorism

The importance of biometric technology in fighting the Global War on Terrorism has grown significantly in the past three years. In addition to the conventional capability of verifying a claimed identity for access control purposes, biometric technologies have the unique capability of verifying that an individual *is not* a member of a particular population (e.g., a terrorist watchlist). Biometric technology also facilitates *positive identification*, i.e. identifying who an individual actually *is* as opposed to who the individual *claims to be*. The goal of creating an identity dominance capability, where our forces have the distinct ability to separate “friend or foe,” is paramount to winning the Global War on Terrorism. The enemy has employed sophisticated methods to exploit flaws in current identity management systems in carrying out past terrorist attacks, and we must strive to blunt and eventually eliminate this capability. The need for technologies that can provide for better border security, force protection, and counter-terrorism measures has never been greater.

The effectiveness of this ability to identify adversaries will ultimately depend upon collection and maintenance of data in interoperable formats that can be shared among U.S. Government organizations, as well as with partner governments through appropriate agreements, when the need arises. Biometric data collected from persons of interest will include physical characteristics and traits that can be used to identify an individual included in the system. To ensure this data is accessible and usable to the fullest extent possible, the systems that utilize biometric data must leverage appropriate standards wherever possible.

1.2 DoD Leadership Direction on Biometric Standards

On 25 August 2003, Deputy Secretary of Defense Dr. Wolfowitz signed a memorandum titled “Department of Defense (DoD) Biometrics Enterprise Vision.” In this memorandum Dr. Wolfowitz stated, “By 2010, biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for logical and physical access control.” To support this vision, he directed the DoD Biometrics Management Office (BMO) to perform the following two actions: (1) “ensure that a scalable biometrics component of the Global Information Grid (GIG) infrastructure is in place” and (2) **ensure “that the appropriate standards, interoperability tools, testing frameworks, and approved product validations are available to assist the DoD Components in using this technology**.”

Additionally, on 02 February 2004 the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)), and the DoD Chief Information Officer, signed a memorandum which directs that all DoD organizations must collect Red Force fingerprint data using biometric data formats described in the ANSI/NIST ITL 1-2000 standard (discussed in detail in Section 3.1). Red Force personnel are collectively known as Enemy Prisoners of War (EPWs), detainees, civilian internees, and other persons of interest with respect to national security.

The ANSI/NIST ITL 1-2000 standard specifies the biometric data formats operationally used by the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) and other U.S. Government and foreign fingerprint systems. DoD support for the ANSI/NIST ITL 1-2000 standard is key for achieving future interoperability with the FBI IAFIS system and fingerprint systems of other U.S. Government organizations.

The BMO sponsored an inter-agency government workshop titled “Biometric Standards in Support of the Global War on Terrorism (GWOT)” on 25 May 2004. The keynote speaker for this workshop was Ms. Priscilla Guthrie, Deputy Assistant Secretary of Defense, Deputy Chief Information Officer. Ms. Guthrie’s keynote address emphasized that standards are critical for the effective sharing of information.

The consensus of the attendees at the 25 May 2004 workshop was that there are three key areas necessary to enable better use of biometrics in the Global War on Terrorism: The establishment of policy by DoD and other U.S. Government organizations to facilitate the sharing of biometric data taken from Red Force personnel; the identification and use of biometric standards that will provide for interoperability and the exchange of information; and ultimately, a standards-based system that supports the storage, use, and processing of biometric data.

1.3 Coordination with Other U.S. Government Organizations

The original (2003) version of this document recommended closer coordination among the DoD and other U.S. Government organizations in biometric standards development to foster inter-agency sharing of information and reduce possible duplications of effort. Those recommendations have led to actions by the BMO to work more closely with the Department of Homeland Security (DHS), the intelligence community, the Department of State, the Justice Department, the FBI, and other U.S. Government organizations in the coordination of biometric standards development activities.

The 25 May 2004 workshop “Biometric Standards in Support of the Global War on Terrorism (GWOT)” referred to above in Section 1.2 brought together more than 70 representatives from 28 organizations inside and outside of the DoD. During this conference NIST, DHS, and the BMO gave presentations on U.S. Government biometric standards initiatives. Presentations by DHS included the use of biometric standards in the U.S. Visitor and Immigrant Status Indicator Technology (US VISIT) program, and the development of biometric testing standards by the Transportation Security Administration. Presentations by NIST included a summary of recent progress by biometrics standards bodies, and an overview of U.S. Government conformity assessment activities.

Participants in the workshop viewed it as an overwhelming success, and open discussions on standards collaboration at the workshop have created an impetus for organizations to continue to work together in developing biometric standards.

1.4 Standards and Interoperability

Information technology (IT) literature has differing and often incompatible definitions of the term "standards." The International Organization for Standardization (ISO) defines the term as follows:

> Documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes, and services are fit for their purpose.

Standards provide a level of consistency that makes them the cornerstone for interoperability. DoD continues to stress the need for better interoperability in support of the joint warfighter. This needed interoperability has been the theme of such DoD enterprise planning documents as Joint Vision 2010 and Joint Vision 2020. For example, Joint Vision 2020 states that joint missions are "dependent on interoperability between organizations, processes, and technologies." DoD Directive 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, states the need for interoperability unambiguously, with a special emphasis on testing:

> IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.

In accordance with this directive and the 25 August 2003 memorandum from the Deputy Secretary of Defense, the BMO's biometric standards development work includes a strong emphasis on testing.

1.5 Current State of Biometric Industry/Biometric Standards, and Impact on DoD

The biometric industry is currently in a nascent, evolving state. Problems affecting the industry at this stage of development include:

- **Fact # 1.** The biometric record formats (known as "templates") used in many current (2004) biometric products are proprietary and do not work with biometric equipment sold by competing vendors. That is, the templates are not interoperable.

Impact: The lack of interoperability in biometric template formats results in biometric "vendor lock-in," necessitating purchase of all biometric readers and software for a biometric system from a single vendor.[1] The following example illustrates the potential consequences of this lock-in.

Suppose that a DoD organization has purchased biometric readers and software from Vendor A. If Vendor A discontinues support for these products because of bankruptcy or some other cause, DoD might completely lose its investment and require costly replacement of technology. In addition, if another vendor developed a superior product, DoD may be unable to take advantage of the superior product because changing products in midcourse would be prohibitively expensive.

- **Fact # 2.** There are currently no approved national or international standards for measuring the accuracy of biometric products.

  Impact: The lack of established scientific standards for comparing the accuracy of different biometric products (known in the biometric industry as "performance testing standards") results in marketplace confusion and makes the job of comparing biometric products extremely difficult. Currently, it is essentially impossible to scientifically compare the accuracy of different biometric products in a repeatable manner. Biometric product consumers, including DoD, currently have no scientifically developed, agreed-upon methods[2] to determine how well the biometric products they buy actually work.

  In April 2003, the M1.5 Task Group on Biometric Performance Testing and Reporting began development of a four-part draft standard for biometric performance testing and reporting. Development of biometric performance testing and reporting standards is still at an early stage and will likely progress more slowly than development of biometric data format standards because of the complex mathematical nature of biometric performance testing. (Section 4.4 describes performance testing in more detail.)

- **Fact # 3.** There are currently no approved national or international standards for evaluating whether a product that claims to support a biometric standard actually conforms to the standard.

  Impact: The lack of established conformance testing standards results in an inability to verify that a commercial product conforms to a standard, such as BioAPI (American National Standards Institute [ANSI]/International Committee for Information Technology Standards [INCITS] 358-2002) and thus makes it impossible to guarantee the interoperability of the product with other biometric products or system components.

[1] An immediately available workaround to this problem is to require the use of "full images" of biometric data using a standard such as the ANSI/NIST ITL 1-2000 standard described in Section 3.5. The discussion in this paragraph, however, concerns the proprietary *template* formats that are used by default in many commercial biometric products.

[2] There are some "best practices" sources for biometric testing, such as the Facial Recognition Vendor Test (FRVT) described at http://www.frvt.org and the fingerprint tests described at http://bias.csr.unibo.it/fvc2002 and http://fpvte.nist.gov. However, details of these methodologies have not yet been incorporated into national and international biometric performance testing *standards*.

> To mitigate this fact, the BMO is developing a BioAPI conformance testing methodology standard and a test suite implementing this methodology that will enable the user to definitively determine whether a product conforms to BioAPI. This development effort is making significant contributions at the national and international levels of standards development. Additionally, this conformance test suite will support the Deputy Secretary of Defense's direction to "ensure that the appropriate standards, interoperability tools, testing frameworks, and approved product validations" are available to the DoD community. (Section 5.3 expands on this discussion.)

To ensure that standards are developed, DoD participates in the development of commercial standards through national and international standards bodies. These development efforts will yield robust standards that DoD will eventually adopt.

DoD has long encouraged the use of commercial standards to ensure that it can meet its mission objectives.[3] For example, in his 29 June 1994 memorandum, "Specifications and Standards—A New Way of Doing Business," Secretary of Defense William Perry states, "Greater use of performance and commercial specifications and standards is one of the most important actions that DoD must take to ensure we are able to meet our military, economic, and policy objectives in the future." In a 14 October 1999 memorandum titled "Participation on Non-Government Standards Committees," the Under Secretary of Defense for Acquisition, Technology and Logistics stated, "It is essential that we participate on appropriate non-Government standards committees to ensure that the standards meet our needs."

To support the adoption of standards, DoD chartered the Defense Standardization Program in DoD Instruction 4120.24. This directive states that it is DoD policy to "promote standardization of materiel, facilities, and engineering practices to improve military operational readiness, reduce total ownership costs, and reduce acquisition cycle time." It also defines one of the objectives of the Defense Standardization Program to "support the development and use of interoperability standards for national and international use." This important objective highlights DoD's shift away from development and use of government standards (better known as Military Specifications [MILSPECs]) toward development and use of commercial and government-wide standards. However, in some cases, commercial standards are not feasible and developmental items are necessary.

1.6 Participation in Standards Organizations

DoD is required by law to implement the National Technology Transfer and Advancement Act (NTTAA) of 1995 (Public Law 104-113 [1996]). This law not only encourages participation in, and use of, commercial standards, but also requires federal organizations and departments to explain failures to use commercial standards when such standards meet their needs. The act directs the National Institute of Standards and Technology (NIST) to bring together federal organizations, and state and local governments, to achieve greater reliance on commercial

[3] Commercial standards are also commonly referred to as national and/or international standards, non-government standards, voluntary standards, and third-party standards. Cited standards are *national* or *international* unless otherwise specified.

standards and decreased dependence on DoD-internal standards (e.g., MILSPECs). The act requires federal organizations to adopt commercial standards, particularly those developed by standards development organizations, wherever possible, in lieu of creating proprietary, non-consensus standards.

On 15 March 2000, in his testimony before the House Committee on Science's Subcommittee on Technology, Gregory E. Saunders, Director, Defense Standardization Program Office, stated, with reference to DoD implementation of the NTTAA:

> The DoD has a proud tradition of being at the forefront of standards development for the kinds of advanced technology products and processes that are vital to our national defense and ultimately to U.S. industrial competitiveness. Being an engaged and educated customer facilitates development of the standards necessary to support such DoD goals as interoperability and coalition warfighting capability. Virtually every major user of standards has learned that participation makes knowledgeable application possible, keeps engineers and scientists current, and is the only effective way of communicating requirements to those who write the standards. Where it is important to DoD's mission to be involved in standards development, we must do so with the same resolve and energy that has paid off so richly in the past.
>
> Interoperability among the Services is a cornerstone vision to future warfighting capability. The Joint Technical Architecture and Open Systems are two major efforts to ensure interoperability among systems of U.S. Military Services, and among those of our Allies; and to allow for rapid insertion of new technology. The success of these initiatives largely depends on the availability of suitable voluntary standards. We must continue to participate with voluntary standards development, to stay engaged in efforts to identify future needs and keep apprised of cutting edge industry directions.

To ensure the development of commercial standards that meet DoD's needs, DoD must participate in national and international commercial standards bodies. The premier U.S. commercial national standards organization is the International Committee for Information Technology Standards (INCITS). INCITS is accredited by, and operates under rules approved by, the American National Standards Institute (ANSI). Its international counterpart is the Joint Technical Committee 1 (JTC 1), a joint technical committee of the ISO and the International Electrotechnical Commission (IEC). Each organization (ANSI and ISO) has an established committee that deals with development of biometric standards. Section 4 provides more detail on these committees.

To oversee biometric standards work currently under development by JTC 1 and INCITS, several DoD and federal organizations actively participate in both organizations. Ensuring the development of standards for DoD and other federal organizations has been a combined effort. The General Services Administration (GSA), Defense Information Systems Agency (DISA), NIST, the National Security Agency (NSA), the State Department, the Department of Homeland Security (DHS), the Department of Justice, and the BMO have made a concerted effort to participate in the development of biometric standards. In addition, the BMO coordinates its standards efforts through the BMO Standards Working Group, which includes members from DISA, NSA, NIST, Air Force, Army, Navy, and the Biometrics Fusion Center (BFC). The BMO is working to expand the Standards Working Group's membership. Through the members of the BMO Standards Working Group, information regarding standards development and adoption is communicated throughout the DoD. The BMO also coordinates the development of the required policy regarding the adoption of biometric standards.

2. DOD BIOMETRICS AND BIOMETRIC STANDARDS

This section describes the applicability and relevance of existing biometric standards to DoD. The section summarizes the building blocks of biometric standards, and illustrates how these building blocks can map to any biometric architecture. Table 18 (in Section 5.1) provides a summary of the DoD biometric standards development priorities that the BMO has identified.

2.1 Types of Standards

This document categorizes biometric standards in the following manner:

- **International Standards.** Standards formally approved and recognized by the ISO or the IEC. The acronyms ISO and/or IEC appear in the titles of these standards. One example of these standards is ISO Standard 15408, the Common Criteria, an internationally recognized IT standard.

- **U.S. National Standards.** Standards formally approved and recognized by ANSI, the official U.S. representative to the ISO and IEC organizations mentioned above. The titles of these standards include the acronym ANSI. One example of these standards is ANSI/NIST–Information Technology Laboratory (ITL) 1-2000, Standard Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo, an ANSI-approved standard, which is discussed in Section 3.

- **U.S. Government-Wide Standards.** NIST, a U.S. Department of Commerce agency, is the organization chartered to establish government-wide IT standards for U.S. federal departments and organizations. U.S. Government standards documents published by NIST include Federal Information Processing Standards (FIPS), NIST Interagency Reports (NISTIR), and NIST Special Publications. Section 3 discusses two examples of these standards, Common Biometric Exchange Formats Framework (CBEFF): NISTIR 6529-A and Government Smart Card Interoperability Specification (GSC-IS), NISTIR 6887.

- **Draft (ANSI or ISO) Standards.** ISO and ANSI follow rigorous procedural rules for the review of draft specifications before the specifications advance to the status of draft standards. A draft standard is a document that has undergone several rounds of technical reviews and is in the final rounds of approval balloting (i.e., voting) to decide whether it will become an approved standard.

- **Third-Party Standards.** For the purposes of this document, third-party standards are standards documents (per the ISO definition of standards provided above) developed by industry consortia or other organizations outside of the U.S. Government and the formal organizational structures of ISO/IEC or ANSI. Examples of third-party standards are standards developed by the Organization for the Advancement of Structured Information Standards (OASIS) and similar industry consortia.

- **DoD Internal Standards.** Organizations, such as DoD organizations, may choose to develop internal standards documents that are specific to the organization. The BMO generally does not recommend use of internal standards for DoD biometric deployments, except in cases in which the recommended types of standards mentioned above do not address the standards issues in question. Use of ISO standards, ANSI standards, and NIST standards are the preferred methods of applying standards to DoD biometric programs.

2.2 Biometric Standards Building Blocks

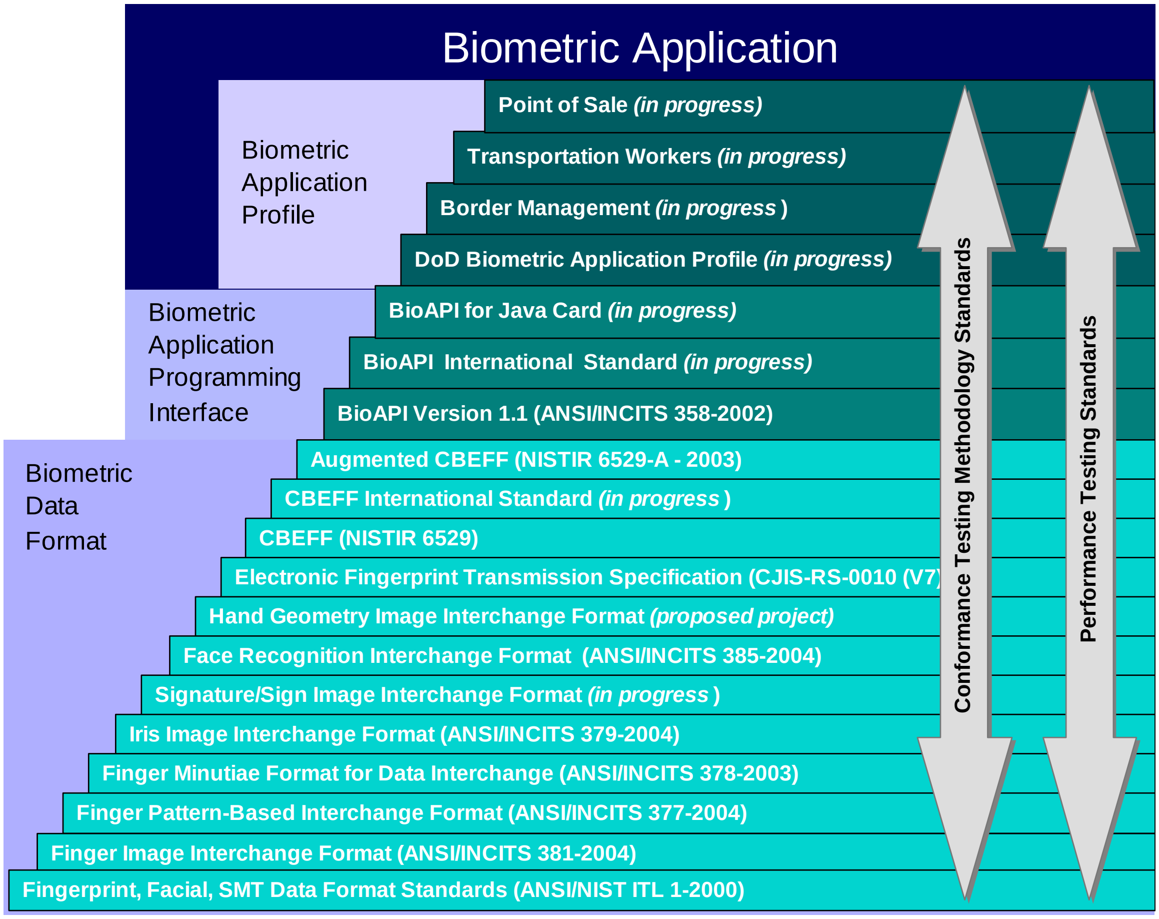
This section introduces a conceptual building block model that clarifies where biometric standards currently exist and which standards are under development. As shown in Figure 1, the major components of the biometric standards building blocks model are as follows:

- Image standards
- Template standards
- File format standards
- Interface standards
- Application profiles
- Performance testing standards
- Conformance testing standards

The above set of standards serves as a base collection of biometric standards. The consolidated set of standards (conforming subsets or combinations of base standards) that constitute the infrastructure for building biometric systems that meet the particular needs of an industry or group of applications is known as a "biometric application profile."

Figure 1 shows the status of various biometric standards (at the national level except where otherwise indicated).

Figure 1. Biometric Standards Building Blocks


Biometric Application
Biometric Application Profile
Point of Sale (in progress)
Transportation Workers (in progress)
Border Management (in progress)
DoD Biometric Application Profile (in progress)
Biometric Application Programming Interface
BioAPI for Java Card (in progress)
BioAPI International Standard (in progress)
BioAPI Version 1.1 (ANSI/INCITS 358-2002)
Biometric Data Format
Augmented CBEFF (NISTIR 6529-A - 2003)
CBEFF International Standard (in progress)
CBEFF (NISTIR 6529)
Electronic Fingerprint Transmission Specification (CJIS-RS-0010 (V7)
Hand Geometry Image Interchange Format (proposed project)
Face Recognition Interchange Format (ANSI/INCITS 385-2004)
Signature/Sign Image Interchange Format (in progress)
Iris Image Interchange Format (ANSI/INCITS 379-2004)
Finger Minutiae Format for Data Interchange (ANSI/INCITS 378-2003)
Finger Pattern-Based Interchange Format (ANSI/INCITS 377-2004)
Finger Image Interchange Format (ANSI/INCITS 381-2004)
Fingerprint, Facial, SMT Data Format Standards (ANSI/NIST ITL 1-2000)
Conformance Testing Methodology Standards
Performance Testing Standards

2.3 Biometric Standards Deficiencies

As Section 1.4 notes, there are many gaps in current biometric standards. The most critical areas for DoD to apply its resources to accelerate biometric standards development are:

- Conformance testing standards
- Performance testing standards
- Biometric data interchange (e.g., template) standards
- Biometric application profiles
- National Information Assurance Partnership (NIAP) protection profiles (PP)

The following paragraphs discuss each of these areas in turn.

Conformance Testing Standards: Conformance testing is the process of testing a technology implementation that claims to support a standard to determine if the implementation adheres to the standard. Conformance testing *standards* specify the manner in which conformance testing should be performed and recorded. Although other IT industries have established standards for conducting conformance tests, this area remains underdeveloped in the biometric industry. (Conformance testing standards are described in more detail in Section 3.)

DoD must have consistent methodologies for evaluating biometric products to determine how well the biometric products conform to established standards. This is an area in which progress in the standards community has been slow. As a result, the BMO is providing contributions to national and international standards bodies to accelerate development of biometric conformance testing standards. Section 5.3 provides additional information on BMO standards development activities in this area.

Performance Testing Standards: Biometric performance testing standards are intended to provide uniform, repeatable methods for measuring the accuracy, speed, durability, reliability, and security of biometric systems. DoD will utilize national and international standards when possible, but will also have to develop unique performance testing standards for certain applications. To understand what biometric performance testing entails, consider the metrics described in the table below. In simplistic terms, this table below shows the four possible outcomes when subjects (e.g., personnel) attempt to authenticate to a system using biometric technology.

Table 1. Metrics for Estimating Performance of a Biometric System

Authentication Situation	Metric for Recording Outcome of Authentication Situation
An authorized subject presents his or her biometric and is granted access.	Correct (or *Genuine*) Match Rate
An unauthorized subject presents his or her biometric and is granted access.	False Match (or *False Acceptance*) Rate
An unauthorized subject presents his or her biometric and is denied access.	Correct (or *Impostor*) Non Match Rate
An authorized subject presents his or her biometric and is denied access.	False Non-Match (or *False Rejection*) Rate

False match rate (FMR) and the false non-match rate (FNMR) statistics provide an estimate of the accuracy, or performance of a biometric system. Failure-to-enroll (FTE) rate statistics are the expected proportion of the population for whom the system is unable to generate repeatable templates (for example, a small percentage of the population is not able to provide fingerprints because of inadequate ridge patterns). The FMR, FNMR, and FTE estimates are expressed as a percentage (e.g., 0.005%) or decimal between 0 and 1. The genuine match rate is calculated as 1-FMR, and the imposter non-match rate is calculated as 1-FNMR.[4] The equal error rate (EER) is the point on a FMR vs. FNMR graph where the FMR and FNMR have equal values.[5]

[4] False rejection rate can be expressed arithmetically as FRR = (# of rejections of an authorized user)/(total # of attempts by the user). The UK Best Practices paper described in Section 4.4 states "'False match rate' and 'false non-match rate' are not generally synonymous with 'false accept rate' and 'false reject rate'. False match/non-match rates are calculated over the number of comparisons, but false accept/reject rates are calculated over transactions." Differences in terminology among biometric experts are one area of difficulty in the biometric standards development process.

[5] FMR and FNMR statistics by themselves are only partially useful. To compare the performance of biometric technologies, use of mathematical graphing techniques such as cumulative match curves or receiver operating curves

FMR and FNMR are not useful indicators by themselves since any biometric system can be made to accomplish either end of the spectrum. A more meaningful metric is required to allow the user to select a required FMR or FNMR. The problem with all of these metrics is that there are no established national or international standards that describe how the metrics should be collected and reported.[6] For example, how many biometric samples does one need for a biometric system to verify a vendor claim of a false match rate of 1/100,000? Are 200,000 samples statistically sufficient, or is the required number of samples much larger (such as 1 million or 5 million)? Is the required number of samples technology dependent? This is an area in which a significant amount of standards development work must occur. Biometric performance testing standards are under development in both national and international biometric standards bodies, as discussed in Section 4.

Data Interchange/Template Format Standards: The area of biometric data interchange format specifications is the area in which biometric standards development progress is occurring most rapidly. The BMO is supporting NIST activities to further the development of standards in this area. Table 2 summarizes the status of biometric data interchange format specifications. Section 4 discusses each of the draft specifications, as well as the M1 national biometric standards body, in more detail.

is necessary. Discussion of these details is beyond the scope of this document, and will be addressed by the performance testing standards reports described in Section 5.4.

[6] There are fundamental disagreements among international biometric experts over the exact definitions of the terms discussed in this section. Disagreements about terminology have hampered the standards development process in the past.

Table 2. Status of Biometric Data Interchange Specifications

Type of Biometric Interchange Format	Status of Data Interchange Specification	Expected Completion Date (US/SC 37)	Is a Performance Testing Standard Available?	Is a Conformance Testing Standard Available?
Finger Minutiae	US: Approved ANSI Standard SC37: Final Committee Draft	2004/2005	No	No[7]
Finger Pattern	US: Approved ANSI Standard SC37: Committee Draft	2004/2005	No	No
Finger Image	US: Approved ANSI Standard SC37: Final Committee Draft	2004/2005	No	No[8]
Iris Recognition	US: Approved ANSI Standard SC37: Final Committee Draft	2004/2005	No	No[9]
Face Recognition	US: Approved ANSI Standard SC37: Final Committee Draft	2004/2005	No	No
Signature Recognition	US: Draft SC37: Working Draft	2004/2005	No	No
Hand Geometry	US: Draft SC37: New Project	2005/2006	No	No
Vascular Image	US: N/A (none) SC37: New project	(N/A)/2007	No	No
Other Biometrics (e.g., voice recognition, palm print, gait, ear, retina)	N/A (none)	N/A	No	No

Biometric Application Profiles: These standards provide logical groupings of subsets of other biometric standards (e.g., data format standards, performance testing standards, and conformance testing standards) to provide a consolidated collection of requirements for use in biometric acquisition and system integration. Currently, there are no approved national or international standards in this area. Section 4.3 discusses four draft biometric application profile specifications under development by the M1 national biometric standards development body.

NIAP Protection Profiles: Protection profiles provide a comprehensive list of security requirements for biometric products. Section 4.5 discusses NIAP PPs in more detail.

2.4 DoD Biometrics Management Office and Biometrics Fusion Center

The U.S. Congress publicly endorsed the importance of biometric technologies by inserting the following statement in Section 112 of the Emergency Supplemental Act, 2000, Public Law 106-246:

[7] BMO submitted a new project proposal to the M1 standards body in May 2004 to initiate the development of a conformance testing methodology standard for the Finger Minutiae Data Interchange Format Standard.

[8] BMO submitted a new project proposal to the M1 standards body in May 2004 to initiate the development of a conformance testing methodology standard for the Finger Image Data Interchange Format Standard.

[9] Iridian submitted a new project proposal for a conformance testing standard for the Iris Data Interchange Format to the M1 standards body in June 2004.

> To ensure the availability of biometrics technologies in the Department of Defense, the Secretary of the Army shall be the Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs of the Department of Defense.

On 27 December 2000, Mr. De Leon, Deputy Secretary of Defense, issued a memorandum, *Executive Agent for the Department of Defense (DoD) Biometrics Project*, that acknowledged the Army as the DoD's Executive Agent for developing and implementing biometric technology. Additionally, this memorandum documents that the Army will create the BMO and BFC to execute its roles as Executive Agent. The memorandum "consolidates oversight and management for all biometrics technology for DoD under the DoD BMO," while it establishes the BFC "to acquire, test, evaluate and integrate biometrics, and to develop and implement storage methods for biometric templates."

2.5 DoD Biometrics Standards Working Group

The BMO established a DoD Biometric Standards Working Group in 2003 to participate in biometric standards development at national and international levels; advocate DoD interests through this participation; and build a consensus on standards development, evaluation, and implementation issues.

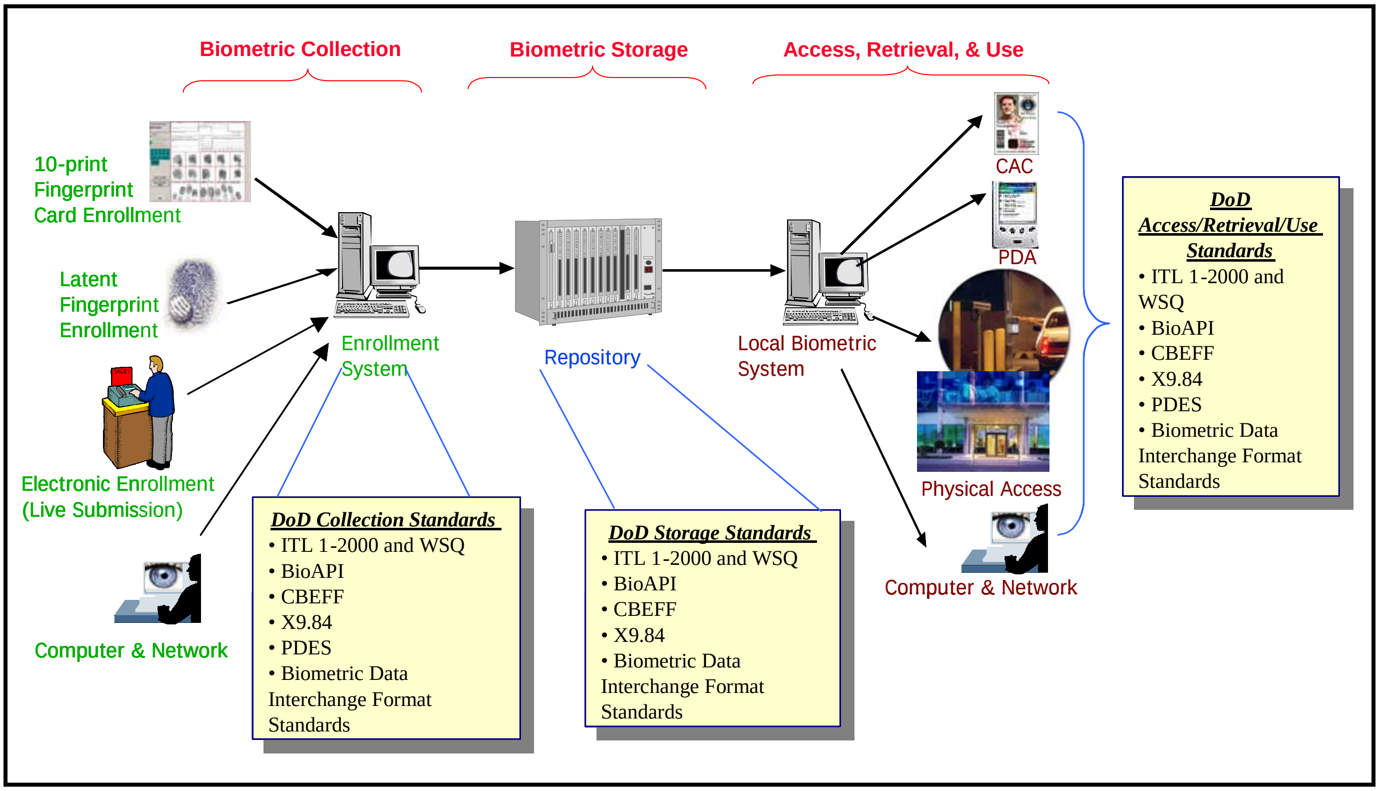
Several DoD organizations actively participate in the DoD Biometric Standards Working Group. Members of this working group include:

- Army Product Manager, Secure Electronic Transactions Devices (PM SET-D)
- Biometrics Fusion Center (BFC)
- BMO
- Defense Information Systems Agency (DISA)
- Defense Manpower Data Center (DMDC)
- Department of the Air Force
- Department of the Army
- Department of the Navy
- National Security Agency (NSA)
- National Biometric Security Project (NBSP)
- National Institute of Standards and Technology (NIST)

2.6 Applying Standards to DoD Biometrics Deployments

Figure 2 shows how biometric standards would apply to a generic, notional biometric architecture.

Figure 2. Standards Applicable to a Generic Biometric Architecture



DoD Collection Standards
- ITL 1-2000 and WSQ
- BioAPI
- CBEFF
- X9.84
- PDES
- Biometric Data Interchange Format Standards

DoD Storage Standards
- ITL 1-2000 and WSQ
- BioAPI
- CBEFF
- X9.84
- Biometric Data Interchange Format Standards

DoD Access/Retrieval/Use Standards
- ITL 1-2000 and WSQ
- BioAPI
- CBEFF
- X9.84
- PDES
- Biometric Data Interchange Format Standards

As Figure 2 illustrates, typical deployments of biometric systems provide three main capabilities:

- **Collection.** Processes and technology used to capture biometric samples from the subjects (i.e., personnel), and perform binding of the biometric data with identity information.
- **Storage/Repository System.** Infrastructure that supports the storage and processing of biometric and related data, and facilitates the exchange of biometric data with other authorized repositories.
- **Access, Retrieval, and Use.** Technology that provides the ability to access and retrieve a biometric from a repository within the DoD or another federal agency and subsequently make a “match” decision to identify a subject.

Figure 2 illustrates the concept of a high-level biometrics architecture. The components of such an architecture provide the three basic capabilities listed above, and can be scaled in size to support large databases of biometric information. A system of this type that supports the collection, storage, and use of fingerprint biometric data is known as an automated fingerprint identification system (AFIS). The notional architecture depicted above can also be designed to support additional biometric *modalities* (i.e., types of biometric data) other than fingerprints, such as face, iris, or hand geometry data. The standards listed in the shaded boxes are examples of standards that would apply to the various components of such an architecture. Each of the standards listed in Figure 2 are discussed in detail in Sections 3 and 4.

2.7 DEVELOPING DOD-CRITICAL BIOMETRIC STANDARDS

As noted previously, the areas of biometric standards development that are most important to DoD are:

- Conformance testing standards
- Performance testing standards
- Biometric data interchange (e.g., template) standards
- Biometric application profiles

The BMO is providing contributions to biometric standards bodies in each of these areas, as described in detail in Section 5. In particular, the BMO provides editors to lead the development of standards in the areas of conformance testing and application profiles.

In the first half of 2004, the BMO has accomplished the following standards development activities:

- Distributed the original (2003) version of this document to 22 DoD organizations for staff review. The BMO received more than 200 comments on the document during two rounds of staffing.

- Submitted new project proposals and assumed editor responsibilities for two national and two international biometric standards development projects (discussed in Section 5).

- Developed first working drafts of standards for conformance testing and application profile standards, and submitted those drafts to standards bodies (discussed in Section 5).

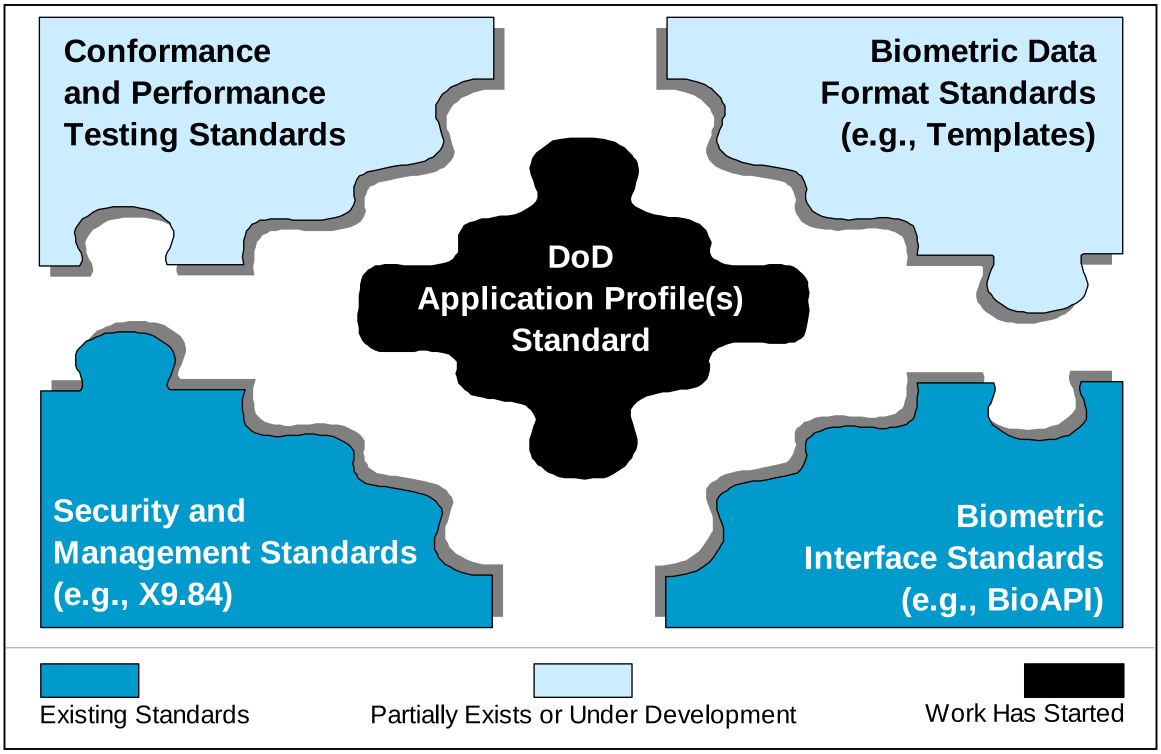
- Expanded membership and participation in the DoD Biometric Standards Working Group, an advisory group which reports to the BMO Director (discussed in Section 2.5).

- Conducted outreach and biometric standards information sharing activities with the Department of Homeland Security, Department of Justice, State Department, the U.S intelligence community, and several DoD organizations.

- Conducted an inter-agency U.S. Government workshop on “Biometric Standards in Support of the Global War on Terrorism.” More than 70 participants from 28 organizations participated in the workshop. The workshop served as an impetus for closer coordination between U.S. Government organizations in biometric standards development activities.

As Figure 3 illustrates, the DoD application profiles serve as the cornerstone for mapping biometric standards to the specific functionality provided in DoD biometric technology deployments. A biometric application profile consolidates the technical requirements described in standards documentation. Section 5.2 provides a more detailed discussion of the DoD biometric application profile standard.

Figure 3. Integration of Biometric Standards Into a DoD Biometric Application Profile


Conformance and Performance Testing Standards
Biometric Data Format Standards (e.g., Templates)
DoD Application Profile(s) Standard
Security and Management Standards (e.g., X9.84)
Biometric Interface Standards (e.g., BioAPI)
Existing Standards
Partially Exists or Under Development
Work Has Started

2.8 Proprietary Biometric Technologies

The biometric industry is in an evolving state, as explained in Section 1.4. Users of biometric products, such as DoD organizations, face a business risk of acquiring biometric products from commercial vendors that do not interoperate with similar biometric products from competing vendors.

> DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), dated 11 January 2002, states in Section 4.1:
>
> It is DoD policy that…IT and NSS interoperability and supportability are essential to joint, combined and coalition forces working together seamlessly to enhance operational effectiveness… Achieving and sustaining interoperability and supportability is a DoD enterprise-wide responsibility that must be woven into the thread of organizational roles, responsibilities, processes, and resources.

In most areas of information technology, initial generations of commercial products tend to use proprietary technologies, as is currently true of the biometric industry. Going forward, it is important that DoD organizations use standards-based biometric products to meet the interoperability goals mandated by DoD Directive 4630.5 and related DoD policies identified in Appendices A and E. Commercial vendors of biometrically-enabled products may offer seemingly compelling arguments that “enhancements” in their products offer benefits not provided by standards defined by standards organizations described in Section 4.1. Such claims should be viewed skeptically, and adherence to DoD policies and product testing processes should be observed. Note that commercial product vendors often use the loosely defined term “industry standard” in marketing literature, and use of this term should be disregarded if the “standard” in question has not been developed by a neutral standards body as described in Section 4.1.

A major consequence of using technologies that are not compliant with standards established by standards bodies is that the products in question will most likely not interoperate with the products of competing vendors. DoD organizations have to take a longer-term view of this situation to understand its importance to local operational effectiveness. For example, a small office of workstations or a single access gate to a military installation may presently use biometrics on a small scale. In such situations, there may be a future requirement or mandate from the chain of command to integrate those resources (e.g., workstations or gates) into a larger regional system. If the products in question are not standards-based, then integrating local systems into a larger regional system at a later date will likely require a costly and operationally disruptive replacement of technology.

2.9 Biometrics and Security

Biometric products are often touted as having “better” security features than the security features provided by password-based authentication products. For example, users often forget their passwords, which necessitates help desk intervention that is disruptive to the user and is operationally costly to the organization. Users sometimes share passwords with coworkers or write down passwords as a convenience, even if these practices are forbidden by policy. The use of biometrics in an organization can reduce some of these common vulnerabilities that exist in password-based authentication environments. However, biometric products are not a panacea, and can have vulnerabilities of their own.

Information assurance and information security are complicated subjects, and go beyond the scope of this document. It is important to note for the purposes of this document that the primary DoD policy regarding the security of information systems is DoD Directive 8500.1, *Information Assurance*, dated 24 October 2002.

DoD Directive 8500.1 includes the following two paragraphs that affect DoD IT systems using biometric technologies in particular:

> 4.13 All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation

> Process (DITSCAP). This instruction implements policy, assigns responsibilities, and prescribes procedures for certification and accreditation of information technology, including automated information systems, networks, and sites in the Department of Defense.
>
> 4.17. All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 [see Section 3.13.4]. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program.

The impact of paragraph 4.13 is that large scale DoD biometric systems must go through traditional certification and accreditation (C&A) processes, just as other DoD IT systems do. Security-related C&A activities for a DoD biometric system would typically include a risk assessment or threat assessment, where security vulnerabilities of a biometric system are discussed.

The impact of paragraph 4.17 is biometric products used in DoD information systems are subject to NIAP evaluation as a condition for acquisition. The subject of NIAP protection profiles for biometrics is discussed in Section 4.5. The protection profiles provide detailed security requirements that affect the security of biometric implementations.

One of the technical subjects discussed in DoD biometric protection profiles is the concept of *strength of function*. The strength of function is an estimate of the effort required by an attacker to defeat a security feature in a product under NIAP evaluation. Additional information about strength of function metrics can be obtained from the Common Criteria standard (ISO/IEC Standard 14508, Part 1) and the protection profile documents discussed in Section 4.5.

3. EXISTING BIOMETRIC STANDARDS

This section discusses the following established biometric standards:

- Standard Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo standard, ANSI/NIST-ITL 1-2000
- Electronic Fingerprint Transmission Specification (EFTS), CJIS-RS-0010 (V7)
- BioAPI standard, ANSI/INCITS 358-2002
- Common Biometric Exchange Formats Framework (CBEFF) standard, NISTIR 6529-A
- ANSI X9.84 Biometric Information Management and Security for the Financial Services Industry standard
- Finger Pattern Based Interchange Format standard, ANSI/INCITS 377-2004
- Finger Minutiae Format for Data Interchange standard, ANSI/INCITS 378-2004
- Finger Image-Based Data Interchange Format standard, ANSI/INCITS 381-2004
- Face Recognition Format for Data Interchange
- Iris Image Interchange Format
- Extensible Markup Language (XML) Common Biometric Format (XCBF) standard

3.1 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo Information, ANSI/NIST-ITL 1-2000

3.1.1 Description

The ANSI/NIST-ITL 1-2000 standard, Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, defines the content, format, and units of measurement for exchange of fingerprint, palm print, facial/mug shot, and SMT full-image information that may be useful in identifying a subject.

Use of the ANSI/NIST-ITL 1-2000 standard and the FBI Electronic Fingerprint Transmission Specification (EFTS) is mandated for all DoD organizations that collect Red Force fingerprint data pursuant to an ASD (NII) Memorandum on “DoD Compliance with the Internationally Accepted Standard for the Electronic Transmission and Storage of Fingerprint Data from ‘Red Force’ Personnel” promulgated 02 February 2004.

The standard consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images. Criminal justice organizations that rely on automated fingerprint and/or palm print identification systems or use facial/mug shot or SMT data for identification purposes, such as police departments, use this standard for data exchange.

The ANSI/NIST-ITL 1-2000 standard defines 16 *logical record types*, which are used by Automated Fingerprint Identification Systems (AFISs) to exchange text and image data between systems. The 16 logical record types defined in the ANSI/NIST-ITL 1-2000 standard are as follows:

1.) Transaction Information
2.) User Defined Descriptive Text
3.) Low-resolution FP Grayscale Image Data
4.) High-resolution FP Grayscale Image Data
5.) Low-resolution FP Binary Image Data
6.) High-resolution FP Binary Image Data
7.) User-defined Image Data
8.) Signature Image Data
9.) Minutiae Data
10.) Facial and SMT (Scar, Mark, Tattoo) Image Data
11.) (Reserved for future use)
12.) (Reserved for future use)
13.) Latent Image Data (variable resolution)
14.) Ten-Print Fingerprint Impressions (variable resolution)
15.) Palm Print Image Data (variable resolution)
16.) User Defined Testing Image Data (variable resolution)

3.1.2 Current Status

The ANSI/NIST-ITL 1-2000 standard is a U.S. national standard endorsed by ANSI. There are currently no international standardization activities associated with this standard.

ANSI standards require renewal, updates, or cancellation every five years after their publication. The ANSI/NIST-ITL 1-2000 was published in the year 2000, and thus must either be renewed (i.e., re-approved without changes) or updated in the year 2005.

3.1.3 Applicability to DoD

Table 3 provides a synopsis of the ANSI/NIST-ITL 1-2000 standard.

Table 3. Synopsis of ANSI/NIST ITL 1-2000 Standard

ANSI/NIST ITL 1-2000 Standard	Status
Recommended for future DoD use?	Yes
Currently mandated in DoD policies?	Yes
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	No
Widely implemented in currently available COTS products?	Yes

DoD support of the fingerprint portions of the ANSI/NIST-ITL 1-2000 standard is necessary for those DoD biometric systems that need to exchange data with the FBI Integrated Automated Fingerprint Identification System (IAFIS). DoD systems that store or process Red Force biometric data have a requirement to interoperate with the FBI IAFIS for identification purposes. DoD organizations that have military law enforcement responsibilities, such as the Army

Criminal Investigation Command (CID[10]) and its counterparts in the Departments of the Navy and Air Force, also must interface with the FBI IAFIS.

DoD must also leverage ANSI/NIST-ITL 1-2000 to vet Blue Force personnel through IAFIS. Blue Force personnel are individuals that are explicitly trusted, such as DoD personnel. However, there is no current policy that requires DoD to leverage ANSI/NIST-ITL 1-2000 for non-Red Force personnel.

3.1.4 Advantages and Disadvantages

Use of the ANSI/NIST-ITL 1-2000 standard is required by policy for use in DoD systems that collect Red Force fingerprint data, as explained in Section 3.1.1.

ANSI/NIST-ITL 1-2000 is a well-established and mature standard used by vendors that supply biometric technologies to the FBI IAFIS, and more than 100 biometric products have been certified for use via FBI conformance testing procedures defined in the EFTS standard.

3.2 Electronic Fingerprint Transmission Specification

3.2.1 Description

The Electronic Fingerprint Transmission Specification (EFTS) is the FBI's specification for transmitting fingerprint information across computer and telecommunications networks. EFTS can be thought of as a biometric "*application software standard,*" since it specifies data fields, commands, and transaction codes necessary for interoperating with the FBI's IAFIS. EFTS is broader in scope than being just a biometric standard, since it also specifies data fields for biographical and arrest record data.

DoD biometric systems involved in Red Force biometric data collection are required to support the EFTS, as described in Section 3.1.1 above. DoD organizations that have military law enforcement responsibilities, and therefore interface with the FBI IAFIS, are also required to support the EFTS..

3.2.2 Current Status

The FBI's Criminal Justice Information Services (CJIS) Division published version 7 of the EFTS in 1999. EFTS version 7 serves as the primary technical reference document for law enforcement and other government organizations that communicate electronically with the FBI IAFIS. There are no known efforts underway to develop the EFTS into a formal national (ANSI) or international (ISO/IEC) standard.

[10] The Army Criminal Investigation Command retains the seemingly incongruous abbreviation, CID, from its earlier incarnation as the Criminal Investigation Division in order to prevent confusion and maintain tradition.

3.2.3 Applicability to DoD

Table 4 provides a synopsis of the EFTS standard:

Table 4. Synopsis of EFTS Standard

EFTS Standard	Status
Recommended for future DoD use?	Yes
Currently mandated in DoD policies?	Yes
Approved ANSI standard?	No
In development to become an International (ISO) standard?	No
Widely implemented in currently available COTS products?	Yes

3.2.4 Advantages and Disadvantages

Use of the EFTS is required by policy for use in DoD systems that collect Red Force fingerprint data, as explained in Section 3.1.1 above.

Support for the EFTS is necessary in IT systems that communicate electronically with the FBI IAFIS, which includes DoD Red Force biometric systems and may also include some Blue Force systems. For example, a DoD Blue Force human resources application that has requirements to perform automated background checks may interface with the FBI IAFIS. The EFTS would be used to facilitate communications between the DoD systems in question and the FBI IAFIS.

One disadvantage of the EFTS is that it was created prior to the development of other biometric standards described in this document, such as the Common Biometric Exchange Formats Framework (CBEFF) standard described in Section 3.4. EFTS does not include support for standards such as CBEFF, because EFTS was developed before CBEFF and most of the other biometric standards described in this document existed.

The EFTS supports a very large-scale legacy application (the FBI IAFIS) having thousands of remote connected nodes. As such, maintaining backwards compatibility with existing EFTS functionality is absolutely necessary, and the possibility of making changes to EFTS is operationally difficult.

3.3 BioAPI Specification Version 1.1, ANSI/INCITS 358-2002

3.3.1 Description

ANSI/INCITS 358-2002, the BioAPI Specification Version 1.1, is a standard for a general application programming interface (API) that can work with any type of biometric technology.[11] BioAPI is currently in development to become a two-part international standard, as described in Section 3.3.2 below.

Benefits provided by the BioAPI standard include:

- Ability to rapidly develop and use application software that is independent of the technological details of specific biometric technologies (e.g., finger, face, iris). BioAPI provides a vendor- and technology-neutral middle layer between biometric devices and software applications.
- Ease of use for software application developers. Programmers can develop interoperable software by building on top of existing functionality in the BioAPI.
- Access to a free, open source reference implementation of software source code that lowers the barriers to entry for new biometric vendors.[12]

3.3.2 Current Status

The BioAPI standard gained ANSI approval as a U.S. national standard in 2002.

The BioAPI standard is under development in ISO/IEC JTC 1 SC 37, the international standards body for biometrics, and is in the process of being adopted as a two international standard titled ISO/IEC 19784 –1 (Information Technology – BioAPI Biometric Application Programming Interface: Part 1: BioAPI Specification) and ISO/IEC 19784 –2 (Information Technology – BioAPI Biometric Application Programming Interface: Part 2: Biometric Archive Module Interface). Section 4.1 provides further discussion of the SC 37 international standards body.

The BMO began development of a conformance testing methodology standard for the international version of BioAPI in early 2004. This work is still underway. The BMO also is contributing to a national BioAPI conformance testing methodology project along with other participants in the M1 standards body (such as NIST and NBSP). The BMO has initiated development of conformance testing tools for BioAPI, as described in Section 5.3.

3.3.3 Applicability to DoD

Table 5 provides a synopsis of the BioAPI standard.

[11] The sponsoring organization for the BioAPI standard is the BioAPI Consortium. The consortium was founded in 1998 and has more than 128 members, including U.S. Government organizations and private industry representatives.

[12] The BioAPI reference implementation is available for free download from http://www.bioapi.org.

Table 5. Synopsis of the BioAPI Standard

BioAPI Standard	Status
Recommended for future DoD use?	Yes
Currently mandated in DoD Information Technology Standards Registry (DISR)[13]?	Yes
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available commercial off-the-shelf (COTS) products?	Yes

The BMO Standards Working Group strongly recommends that BioAPI-compliant products be used throughout DoD wherever biometric products and solutions are deployed.

Failure to use the BioAPI in DoD deployments of biometric products virtually guarantees a lack of interoperability between the biometric products used by DoD-selected vendors and competing biometric products sold by other vendors.

The BioAPI specification has been listed in the DoD Joint Technical Architecture (JTA) as a mandated DoD-wide standard since JTA Version 5.0 in January 2003. The BioAPI standard continues to be mandated in the successor to the JTA, the Defense Information Technology Standards Registry (DISR).

3.3.4 Advantages and Disadvantages

At least 128 organizations, including biometric vendor companies and U.S. Government organizations, support the BioAPI standard.[14] The major advantage of the standard is that it is designed to be suited for any form of biometric technology. BMO Standards Working Group members have seen live demonstrations of BioAPI-based application software that works seamlessly with a fingerprint reader, a thumbprint reader, and a camera system using both iris recognition and facial recognition software.[15] In short, the BioAPI standard works. The BMO Standards Working Group believes the BioAPI standard is currently DoD's best hope for achieving biometric product interoperability.

There are few, if any, disadvantages to mandating and using the BioAPI standard in DoD systems. One possible disadvantage of this standard, as well as of the other existing biometric standards discussed in this document, is the current lack of explicit support from certain large commercial software vendors. However, lack of certain built-in support for the standard in

[13] The DoD Information Technology Standards Registry (DISR) replaced the DoD Joint Technical Architecture (JTA) as the authoritative listing of DoD-wide technology standards in May 2004.
[14] See the BioAPI Consortium Website at http://www.bioapi.org.
[15] See Section 1.1 of the BioAPI Specification, version 1.1, available at http://www.bioapi.org.

certain commercial operating system products is not a “showstopper” for BioAPI. Biometric equipment vendors (e.g., fingerprint reader vendors) can simply provide BioAPI-compliant application software along with their hardware products to provide BioAPI functionality.

3.4 CBEFF, NISTIR 6529-A

3.4.1 Description

The Common Biometric Exchange Formats Framework (CBEFF) defines a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by enabling biometric data exchange. CBEFF describes a set of required and optional data fields, a domain of use, and CBEFF patron (i.e., supported) formats that use some combination of these standard elements. The common set of data elements described in CBEFF can exist in a single file record, or data object, used to exchange biometric information between different system components. Different biometric technologies, or different data instantiations in a single technology, can leverage the CBEFF nested structure specified in NISTIR 6529-A to exchange biometric data.

3.4.2 Current Status

The CBEFF is a U.S. Government standard published by NIST. NIST initially published the specification as NISTIR 6529 in January 2001 and released an augmented version of the specification (CBEFF NISTIR 6529-A) in April 2004. CBEFF is currently undergoing development as an international standard within ISO/IEC JTC 1 SC 37.

3.4.3 Applicability to DoD

Table 6 provides a synopsis of the CBEFF standard.

Table 6. Synopsis of CBEFF Standard

CBEFF Standard	Status
Recommended for future DoD use?	Yes
Currently mandated in DoD Information Technology Standards Registry (DISR)?	Yes
Approved ANSI standard?	No
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	Yes (some)

To promote interoperability, **the BMO Standards Working Group strongly recommends use of CBEFF data structures in all DoD biometric deployments**. The CBEFF standard has been listed in the DoD Joint Technical Architecture (JTA) as a mandated DoD-wide standard since JTA Version 5.0 in January 2003. The CBEFF standard continues to be mandated in the successor to the JTA, the Defense Information Technology Standards Registry (DISR)[16]. CBEFF compliance is a requirement in all data interchange format standards and application profile standards under development in the M1 and SC 37 standards bodies described in Section 4.

3.4.4 Advantages and Disadvantages

CBEFF's purpose is to "define a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange."[17] To this end, CBEFF provides valuable and necessary support for biometric data interoperability at a systems (as opposed to a device) level. BioAPI is defined in the CBEFF standard as a patron format, meaning that all current BioAPI implementations are notionally CBEFF compliant. However, there appear to be technical incompatibilities between CBEFF and X9.84 that are currently being analyzed by the SC37 international standards body [see Section 3.5.3]. The SC37 standards body is described in Sections 4.1 and 4.6.

CBEFF compliance has been part of the requirements for all the data interchange format standards under development in the M1 and SC 37 standards bodies. CBEFF data structures "wrap" or enclose biometric data in a consistent manner, providing a higher degree of interoperability than the interchange format standards provide alone.

3.5 Biometric Information Management and Security for the Financial Services Industry, ANSI X9.84-2003

3.5.1 Description

The ANSI X9.84-2003 standard provides biometric management and security requirements for the following areas:

- Security of collection, distribution, and processing of biometric data
- Management of biometric data across its life cycle (consisting of enrollment, transmission and storage, verification, and termination processes)
- Application of biometric technology for logical and physical access
- Encapsulation of biometric data
- Techniques for secure transmission and storage of biometric data
- Techniques for integrity and privacy protection of biometric data

Through use of the X9.84-2003 standard, a biometric system can ensure the integrity of biometric data by using public key infrastructure (PKI) digital signatures and PKI-based or symmetric encryption. The security features described in X9.84-2003 leverage well established,

[16] The DoD Information Technology Standards Registry (DISR) replaced the DoD Joint Technical Architecture (JTA) as the authoritative listing of DoD-wide technology standards in May 2004.
[17] Section 2 NISTIR 6529 (CBEFF standard), 3 January 2001.

well-tested information security technologies such as those described in the ANSI X9.73-2002 standard titled *Cryptographic Message Syntax (CMS).* The bulk of the X9.84-2003 standard specifies record formats in Abstract Syntax Notation 1 (ASN.1) for encoding biometric data. The standard also has excellent informative appendices describing the security controls that should be present in any IT system that processes sensitive information.

3.5.2 Current Status

The X9.84 specification became an approved U.S. national standard in 2001, identified as ANSI X9.84-2001. An update to this standard, ANSI X9.84-2003, was published in 2003.

ISO 19092 is the international counterpart to the ANSI X9.84-2003 standard and is under development by ISO Technical Committee (TC) 68, Financial Services. ISO 19092 is being developed as a two-part standard, whose titles are ISO 19092-1 (Financial Services - Biometrics - Part 1: Security Framework) and ISO 19092-2 (Financial Services - Biometrics- Part 2: Cryptographic Requirements).

3.5.3 Applicability to DoD

Table 7 provides a synopsis of the ANSI X9.84-2003 standard.

Table 7. Synopsis of ANSI X9.84-2003 Standard

ANSI X9.84-2003 Standard	Status
Recommended for future DoD use?	Yes – Tentatively
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved U.S. (ANSI) standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	No

The X9.84-2003 standard is the most complete existing standard addressing the security of biometric data. However, some members of the M1 standards body have noted incompatibilities between X9.84-2003 data formats that use encryption and the CBEFF standard described in Section 3.3. The TC68 and SC37 international standards bodies are currently investigating this issue. The BMO Standards Working Group recommendation on DoD-wide adoption of X9.84 is awaiting resolution of this issue.

BMO Standards Working Group research on the X9.84-2003 standard indicates that the standard is very thorough in its description of security controls. The portions of the X9.84-2003 standard that are normative (i.e., mandatory) relate to the encoding rules used to represent X9.84-2003 data. There are also several non-mandatory annexes to the standard that describe issues such as biometric enrollment criteria, types of testing that can be performed, management of encryption keys to protect the integrity of biometric data, and other security controls that affect a biometric system. The annexes are potentially of greatest interest to DoD because they may address security requirements of DoD IT systems. (The exact security requirements of DoD IT systems vary by organization, and are documented through the Certification and Accreditation processes mentioned in Section 2.9.) DoD is mandating use of annexes (i.e., appendices) in X9.84-2003 that do not conflict with the CBEFF standard through the DoD Application Profile standard described in Section 5.2. Section 4.3 provides background information on biometric application profile standards.

3.5.4 Advantages and Disadvantages

The X9.84 standard is very thorough and well designed, and leverages well-established IT security standards, such as the ANSI X9.73-2002 Cryptographic Message Syntax standard. X9.84 also applies the best practices in existing security standards to biometric implementations.

A significant issue with the 2003 version of X9.84 is a technical incompatibility with the CBEFF standard, specifically with respect to header encryption in X9.84-2003. The TC68 and SC37 international standards bodies are currently analyzing this issue. Another disadvantage of mandating the X9.84 standard at present is the current dearth of commercially available X9.84-compliant software. Only two relatively small companies are known to sell X9.84 software development tools, and neither of these companies sell complete (i.e., ready to operate) commercial off-the-shelf (COTS) X9.84 applications that can operate an AFIS. These are serious marketplace disadvantages of X9.84 technology. If DoD mandated use of X9.84 in large-scale uses of DoD biometrics, it would probably need to have an integrator develop government off-the-shelf (GOTS) software to meet X9.84 technical requirements. Nevertheless, although investing in development of GOTS X9.84 software would increase the costs of a DoD biometrics deployment (compared with implementation of a purely COTS solution), such an investment will probably be necessary (and desirable) to attain the long-term benefits of secure and reliable biometric data protection, which may be necessary to meet the security requirements of the applications involved. (See Section 2.9 for a brief discussion of biometric security issues.)

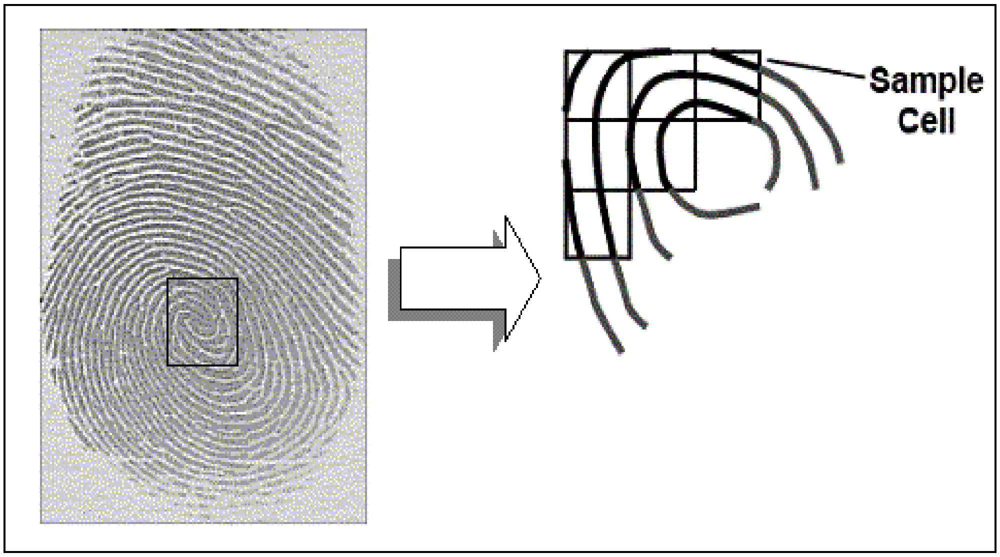
3.6 Finger Pattern Based Interchange Format

3.6.1 Description

The Finger Pattern Based Interchange Format (ANSI/INCITS 377-2004) standard specifies a method of creating biometric templates of fingerprint biometric information using ridge pattern measurements found in fingerprints.

Figure 4 illustrates the concept of dividing a fingerprint image into a grid of “sample cells,” which are then analyzed to determine the angular differences between the ridges within each cell. The Finger Pattern Based Interchange Format specification describes a number of parameters used to generate data records, such as size of finger pattern in the X and Y directions, resolution of the pattern in the X and Y directions, number of cells in each direction, and so on. Note that this technique of representing biometric data is different from that assumed by the finger minutiae interchange specification. Whereas the Finger Minutiae Format for Data Interchange (described in Section 3.7) stores minutiae points from a fingerprint, the Finger Pattern Based Interchange Format stores angular orientation information about the ridges in the fingerprint. The Finger Pattern Based Interchange Format cites the BioAPI standard, the CBEFF standard, and the ANSI/NIST-ITL 1-2000 standard as normative (i.e., mandatory prerequisite) references.

Figure 4. Finger Pattern-Based Biometric Processing



3.6.2 Current Status

This specification was approved as an ANSI standard in February 2004. An international version of this specification is under development in the ISO/JTC/SC37 standards body, as discussed in Section 4.6. The international version of the specification is in the Committee Draft stage of processing.

3.6.3 Applicability to DoD

Table 8 provides a synopsis of the Finger Pattern Data Interchange Format, ANSI/INCITS 377-2004.

Table 8. Synopsis of the ANSI/INCITS 377-2004 Standard

ANSI/INCITS 377-2004	Status
Recommended for future DoD use?	Yes (in limited cases)
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes

ANSI/INCITS 377-2004	Status
Widely implemented in currently available COTS products?	No (new standard)

3.6.4 Advantages and Disadvantages

This standard is useful in situations where a relatively small sized *template* of fingerprint biometric information is desired for storage efficiency reasons.

This standard is not applicable or appropriate for use in biometric applications where a full fingerprint image is necessary, such as Red Force biometric applications where support for forensic capabilities are required.

ANSI approved this standard in 2004. Since this standard is new, commercial biometric products that implement this standard will not likely be available until 2005 or 2006. Initial biometric products that implement this standard (e.g., in 2005) will most likely only be available from the vendor that provided an editor for the standard, and implementations from competing vendors might not be available until 2006 or later.

3.7 Finger Minutiae Format for Data Interchange

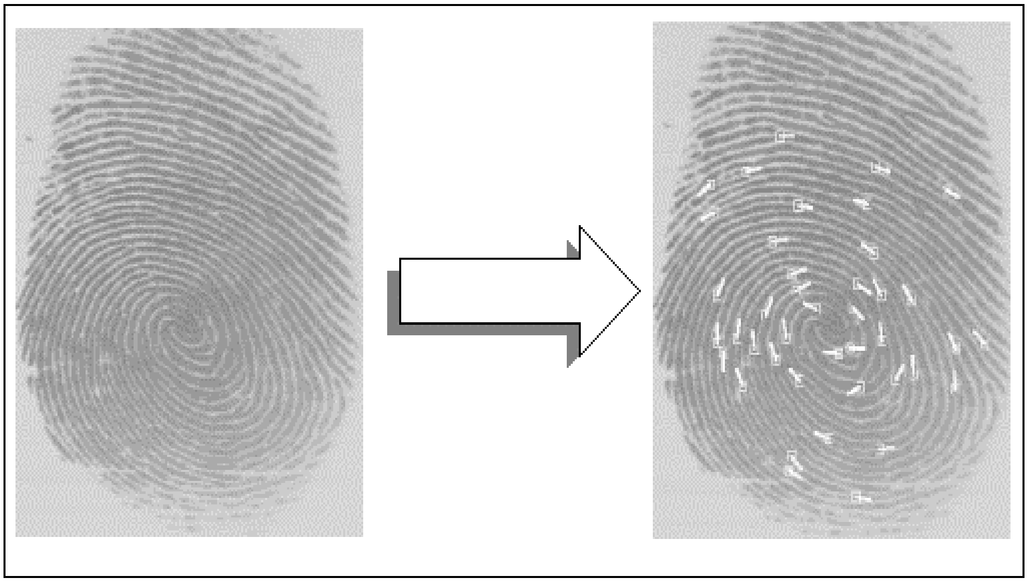
3.7.1 Description

The Finger Minutiae Format for Data Interchange (ANSI/INCITS 378-2003) specifies a method of creating biometric templates of fingerprint minutiae, such as ridge endings and bifurcations.[18]

Figure 5 shows the types of minutiae that the specification discusses. The specification provides values for finger position codes, finger impression-type codes (plain up/down, or rolled), ridge counts, “core” (approximate center of a fingerprint image area) and “delta” (point of divergence of a ridge) values, etc. It cites the BioAPI standard, the CBEFF standard, and the ANSI/NIST-ITL 1-2000 standard as normative (i.e., mandatory prerequisite) references.

[18] A ridge ending is the point at which a fingerprint ridge terminates. A bifurcation is the point at which one ridge splits into two ridges.

Figure 5. Finger Minutiae-Based Biometric Matching



3.7.2 Current Status

This specification was approved as an ANSI standard in February 2004.

An international version of this specification is under development in the ISO/JTC/SC37 standards body, as discussed in Section 4.6. The international version of the specification is in the Final Committee Draft stage of processing.

3.7.3 Applicability to DoD

Table 9 provides a synopsis of the Finger Minutiae Format for Data Interchange standard, ANSI/INCITS 378-2004.

Table 9. Synopsis of the ANSI/INCITS 378-2004 Standard

ANSI/INCITS 378-2004	Status
Recommended for future DoD use?	Yes (in limited cases)
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	No (new standard)

3.7.4 Advantages and Disadvantages

This standard is useful in situations where a relatively small sized *template* of fingerprint biometric data is desired for storage efficiency reasons.

This standard is not applicable or appropriate for use in biometric applications where a full fingerprint image is necessary, such as Red Force biometric applications where support for forensic capabilities are required.

ANSI approved this standard in 2004. Since this standard is new, commercial biometric products that implement this standard will not likely be available until 2005 or 2006. Initial biometric products that implement this standard (e.g., in 2005) will most likely only be available from the vendor that provided an editor for the standard, and implementations from competing vendors might not be available until 2006 or later.

3.8 Finger Image Based Recognition Data Interchange Format

3.8.1 Description

The Finger Image-Based Interchange Format (ANSI/INCITS 381-2004) is applicable to biometric applications requiring exchange of raw or processed fingerprint images that may not be limited by the amount of resources required for data storage or transmission time. This standard supports the exchange of scanned fingerprints containing detailed image pixel information or for the exchange of processed fingerprint image data containing considerably fewer pixels per inch and/or a lesser number of grayscale levels. This specification is in contrast to the standard formats used for exchanging lists of fingerprint characteristics such as minutiae, patterns, or other variants. These formats require considerably less storage than does a fingerprint image. However, information recorded in one standard format is not interoperable with information recorded in an alternative standard format. In other words, minutiae data cannot be used by pattern matching algorithms, and pattern data cannot be used by minutiae matching algorithms.

The Finger Image-Based Interchange Format cites WSQ, EFTS, ANSI/NIST-ITL 1-2000, JPEG, JPEG 2000, BioAPI, and CBEFF standards as normative (i.e., mandatory prerequisite) references.

3.8.2 Current Status

This specification was approved as an ANSI standard in May 2004.

An international version of this specification is under development in the ISO/JTC/SC37 standards body, as discussed in Section 4.6. The international version of the specification is in the Final Committee Draft stage of processing.

The BMO submitted a new project proposal to the M1 standards body in May 2004 to begin development of a conformance testing methodology standard for the ANSI/INCITS 381-2004 standard. M1 approved the project proposal, and the BMO has since begun development of this conformance testing methodology standard. Conformance testing standards are further discussed in Section 5.3.

3.8.3 Applicability to DoD

Table 10 provides a synopsis of the Finger Image-Based Interchange Format standard, ANSI/INCITS 381-2004.

Table 10. Synopsis of the ANSI/INCITS 381-2004 Standard

ANSI/INCITS 381-2004	Status
Recommended for future DoD use?	Yes (in limited cases)
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	No (new standard)

3.8.4 Advantages and Disadvantages

This standard specifies use of full images of fingerprint biometric data, as opposed to the template approaches of the finger pattern and finger minutiae data interchange formats. The use of full images of fingerprint data supports capabilities such as latent fingerprint analysis, and the availability of full images allows fingerprint data to be converted to multiple template-based representations in an automated manner.

This data format is technically very similar to the Type-4 *high-resolution grayscale fingerprint image* logical record type defined in the ANSI/NIST-ITL 1-2000 standard. Conversion between ANSI/NIST-ITL 1-2000 Type-4 records and finger image interchange files is feasible using relatively simple transcoding software, given the similarities between the two specifications.

The drawbacks with this standard are: (1) It, like the finger pattern and finger minutiae data interchange formats, is a new 2004 standard and thus may not be supported in commercial biometric products until 2005 or 2006; and (2) The use of full images imposes larger storage capacity requirements than do template-based biometric systems.

3.9 Face Recognition Format for Data Interchange

3.9.1 Description

The Face Recognition Format for Data Interchange (ANSI/INCITS 385-2004) specifies a method of creating biometric images of facial characteristics. Topics addressed by this specification include image dimensions (e.g., position of eyes and relative length of the head in an image), lighting used in the image capture process, image resolution and focus, image colors, and the digital representation of all of these characteristics (e.g., pixels, gray scales, byte order, data structures, etc). Two types of image outputs are described by the specification: A "full" color image suitable for both human examination and computer face recognition, and a "canonical" image that minimizes storage requirements for computer face recognition tasks. The specification calls for the use of JPEG 2000 to compress images produced using this standard

3.9.2 Current Status

This specification was approved as an ANSI standard in May 2004.

An international version of this specification is under development in the ISO/JTC/SC37 standards body, as discussed in Section 4.6. The international version of the specification is in the Final Committee Draft stage of processing.

3.9.3 Applicability to DoD

Table 11 provides a synopsis of the Face Recognition Format for Data Interchange standard, ANSI/INCITS 385-2004.

Table 11. Synopsis of the ANSI/INCITS 385-2004 Standard

ANSI/INCITS 385-2004	Status
Recommended for future DoD use?	Yes (in limited cases)
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	No (new standard)

3.9.4 Advantages and Disadvantages

The ANSI/INCITS 385-2004 standard provides a standard data format that can be used in face recognition biometric applications. Face recognition biometric systems provide important capabilities that are planned for future use in U.S. Government biometric systems such as the U.S. Visitor and Immigrant Status Indicator Technology (US VISIT) program of the Department of Homeland Security.

The face recognition data interchange format, like the finger pattern and finger minutiae standards mentioned previously, is a new 2004 standard that (as of this writing) has not yet been implemented in commercially available products from multiple vendors. Use of this standard will likely become more important over a two to three year time frame as multiple face recognition biometric vendors release commercial products that implement the standard.

Face recognition biometric technology, in general, is a less established form of technology than fingerprint-based biometric technologies. The ANSI/INCITS 385-2004 standard requires several user behavioral actions at biometric enrolment (e.g., a frontal pose, a neutral facial expression, a centering of the head in the image area, etc) that may limit the operational effectiveness of biometric applications that use this standard. In situations where the enrolment assumptions listed in the standard are not met (e.g., situations where the pose of the subject may not be a fully frontal pose, but rather may be at an angle), the operational effectiveness of the technology is likely to be degraded.

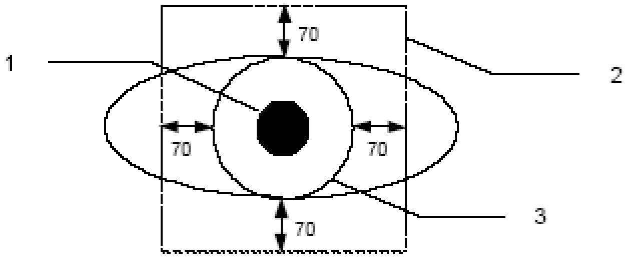
3.10 Iris Image Interchange Format

3.10.1 Description

The Iris Image Data Interchange Format (ANSI/INCITS 379-2004) standard specifies a method of creating an image of iris biometric information. This specification addresses such topics as image compression, image preprocessing, image data packet formats, and image header format.

Figure 6 illustrates the key features of an iris image described in the ANSI/INCITS 379-2003 specification. Three “points of interest” in an iris image are identified in the figure: 1) The pupil boundary, 2) The image border, and 3) The iris boundary. The number “70” denotes that 70 pixels of image data is required by the specification to center the iris data from the image border.

Figure 6. Key Features of an Iris Image



3.10.2 Current Status

This specification was approved as an ANSI standard in May 2004.

An international version of this specification is under development in the ISO/JTC/SC37 standards body, as discussed in Section 4.6. The international version of the specification is in the Final Committee Draft stage of processing.

3.10.3 Applicability to DoD

Table 12 provides a synopsis of the Iris Image Data Interchange Format, ANSI/INCITS 379-2004.

Table 12. Synopsis of the ANSI/INCITS 379-2004 Standard

ANSI/INCITS 379-2004	Status
Recommended for future DoD use?	Yes (in limited cases)
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Yes
In development to become an International (ISO) standard?	Yes
Widely implemented in currently available COTS products?	No (only one U.S. vendor for this technology)

3.10.4 Advantages and Disadvantages

Iris recognition technology, when appropriately used, is reputed to have excellent performance characteristics, i.e. extremely low false acceptance rates and low false rejection rates. The ANSI/INCITS 379-2004 standard provides a standard data format that can be used in iris recognition biometric applications.

ANSI approved this standard in May 2004. Since this standard is new, commercial biometric products that implement this standard will not likely be available until 2005 or 2006. Initial biometric products that implement this standard (e.g., in 2005) will most likely only be available from the vendor that provided an editor for the standard, and implementations from competing vendors might not be available until 2006 or later.

3.11 XML Common Biometric Format

3.11.1 Description

The XML Common Biometric Format (XCBF) is a common set of secure XML encodings defined by the XCBF Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS) for the data formats specified in the X9.84 standard (described in Section 3.5). XCBF is based on XML, a highly flexible text markup language used to create, structure, store, and send information. XCBF provides security for biometric data through its support of the X9.96 XML Cryptographic Message Syntax (XCMS) standard.

3.11.2 Current Status

The XCBF Version 1.1 specification was approved as an OASIS standard on 31 August 2003. The technical content contained in XCBF is currently included in X9.84-2003 and is progressing through the ISO standardization process as a part of ISO/TC68 project 19092. The XCBF specification has ceased further development as a stand-alone standard.

3.11.3 Applicability to DoD

Table 13 provides a synopsis of the XCBF standard.

Table 13. Synopsis of OASIS XCBF Standard

OASIS XCBF Standard	Status
Recommended for future DoD use?	No
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	No
In development to become an International (ISO) standard?	Yes (indirectly)
Widely implemented in currently available COTS products?	No

3.11.4 Advantages and Disadvantages

XCBF, in its current form, is no longer recommended for DoD use.

XCBF Version 1.1 was originally recommended for future DoD use in the initial (2003) version of the *DoD Biometrics Standards Development Recommended Approach* document. The BMO Standards Working Group, after researching XCBF further and monitoring the rate of industry adoption of this standard, determined in 2004 that the DoD should *not* adopt the XCBF standard in its current form.

As noted in Section 3.11.2 above, the technical content of the XCBF specification is included in the X9.84-2003 standard and it is being reviewed and modified as it moves through the ISO standardization process as ISO/TC68 project 19092. The XCBF specification itself, however, has ceased development. As ISO/TC68 project 19092 proceeds with making modifications to its technical content, the content of XCBF Version 1.1 will become un-maintained and obsolete.

3.12 Wavelet Scalar Quantization Algorithm

3.12.1 Description

The Wavelet Scalar Quantization (WSQ) algorithm is the FBI-specified compression standard used for the exchange of fingerprint images within the criminal justice community. The WSQ specification is a publicly available specification for representing biometric image data in a compressed image format.

3.12.2 Current Status

The WSQ algorithm is published in FBI publication IAFIS-IC-0110, and is cited as normative (i.e., mandatory) reference in the ANSI/NIST ITL 1-2000 standard discussed in Section 3.1.

WSQ can be considered a "standard" by virtue of its inclusion in the ANSI/NIST ITL 1-2000 standard.

3.12.3 Applicability to DoD

Table 14 provides a synopsis of the WSQ standard.

Table 14. Synopsis of the WSQ Standard

WSQ Standard	Status
Recommended for future DoD use?	Yes
Currently mandated in DoD Information Technology Standards Registry (DISR)?	No
Approved ANSI standard?	Used in the ANSI ITL 1-2000 standard (See Section 3.1 above)
In development to become an International (ISO) standard?	No
Widely implemented in currently available COTS products?	Yes

The WSQ specification is a proven, reliable method of compressing fingerprint images used in the world's largest operational biometric system, the FBI IAFIS. DoD biometric systems having a requirement to exchange data with the FBI IAFIS, such as DoD law enforcement organizations, *must* use WSQ for fingerprint image compression for data interoperability purposes. However, WSQ appears to have much broader applicability to DoD biometric systems that collect and store fingerprint image data.

3.12.4 Advantages and Disadvantages

WSQ is an image compression algorithm designed specifically for fingerprint images, and its use is required in both ANSI/NIST ITL 1-2000 (Section 3.1) and the FBI Electronic Fingerprint Transmission Specification (EFTS, Section 3.2). The WSQ specification provides an efficient and proven means of compressing fingerprint images. According to informal review comments provided on this document by NIST,[19] "Fingerprints scanned at 500 pixels per inch (ppi) have been traditionally compressed with WSQ at a compression ratio of approximately 15:1. By comparison, the original baseline JPEG algorithms would only compress fingerprint images to about 5:1 reliably." There is commercially available software for WSQ compression and decompression, and for building and parsing EFTS transactions--on virtually any platform.

[19] Informal review comments on the 2003 edition of this document by R.M. McCabe, Computer Scientist, NIST, 12 Nov 03.

3.13 Other Standards Related to Biometrics

This section describes several standards that are not biometric standards per se but are important standards that DoD organizations should take into account in planning deployments of biometric technologies as part of larger automated information systems. The list presented here is not exhaustive, and many other standards related to IT are identified in the DoD JTA. The BMO discusses the standards identified here because of their direct impact on the acquisition, deployment, and integration of biometric technologies into larger systems.

3.13.1 Person Data Exchange Standard (PDES)

The Person Data Exchange Standard (PDES) is a data format specification developed by the Intelligence Community to facilitate the interchange of terrorist watch list information. PDES establishes a mechanism for the consistent exchange of normalized descriptive data on individuals that may pose a threat to national security. This data may provide the foundation for predictive analysis that leads to actionable intelligence in support of the Global War on Terrorism. PDES uses extensible markup language (XML) to markup biographical data on individuals such as names, aliases, physical descriptions, skills possessed, and location information.

PDES uses the CBEFF standard (described in Section 3.4) to facilitate the exchange of biometric data. Through CBEFF, any modality of biometric data may be encapsulated in a standard structure and shared across U.S. Government organizations, as appropriate.

3.13.2 Government Smart Card Interoperability Specification, NISTIR 6887

The Government Smart Card Interoperability Specification (GSC-IS), NISTIR 6887, is a U.S. Government standard published by NIST. "Smart cards" are credit card-sized cards that contain electronic memory storage and/or microprocessor chips. The GSC-IS defines an API for performing card functions such as accessing an external source for authentication, reading card data, and performing encryption and decryption of card data. NIST released NISTIR 6887-2003 Edition, GSC-IS (v2.1) on 16 July 2003.

One portion of this specification that may be of interest to DoD—specifically to the DoD Common Access Card (CAC) program—is the GSC Data Model (in Appendix C of the specification), which includes a data field in which a 512-byte biometric template can be stored. The use of biometrics is optional in the current GSC-IS. The BMO and Access Card Office (ACO) will address this issue jointly through coordination with relevant DoD CAC stakeholders. A GSC-IS compatible biometric standards proposal has been evaluated by INCITS M1 and is now in draft form at the B10 national standards committee[20]. A BMO representative serves on the B10 committee, and coordinated the development of the B10 position on a key GSC-IS study submitted to B10 by the M1 standards body.

Another item of note in GSC-IS, version 2.1, is the list of normative (mandatory prerequisite) references provided in Appendix A. This list cites ISO/IEC 7816-3, 7816-4, 7816-5, and 7816-8 standards as normative references for the GSC-IS. These standards deal with physical (e.g.,

[20] The B10 standards committee is described in Section 4.1.

electrical) and internal command syntax aspects of smart cards. The GSC-IS does *not* reference of ISO/IEC standard 7816-11, Personal Verification Through Biometric Methods. A future version of the GSC-IS may reference ISO/IEC 7816-11. ISO/IEC 7816-11 was approved as an international standard in 2004.

A modular biometric extension to GSC-IS v2.1 has been proposed as INCITS M1/03-0398, and is entitled Smart Card Interoperability Report. This extension to GSC-IS has been submitted by the M1 committee to the INCITS B10 committee for incorporation into a US national (ANSI) standard. This specification builds on other standards described here to provide a modular extension for store on card and match on card multiple biometrics on the CAC.

3.13.3 Java Card Biometry API

The Java Card Forum is a third-party consortium that promotes the use of the Java programming language in smart cards. A "Java Card" is a smart card that includes a subset of the Java programming language. The Java Card Biometry API21 is a Java application-programming interface that supports smart card storage of biometric templates and on-card matching for biometric verification. The Java Card Biometry API is generally compatible with BioAPI and CBEFF, but only applies to operations on a smart card.

3.13.4 Common Criteria, ISO/IEC 15408:1999

The Common Criteria is a three-part international standard (formally designated ISO/IEC Standard 15408) published in 1999. The Common Criteria provides an internationally standardized set of processes and terminology related to the evaluation of products against functional and assurance requirements. Part 1 of the standard covers terminology and the general Common Criteria model. Part 2 defines security functional components that provide a standard way of expressing security requirements. Part 3 defines a catalog of assurance components (such as life-cycle management controls) that provide a standard way of expressing assurance requirements for IT products.

In the United States, NIAP manages the processes of testing, evaluating, and assessing IT products against the Common Criteria standard. NIAP is a U.S. Government initiative jointly managed by NIST and the NSA. National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11 mandates that in acquiring IA products or IA-enabled products for national security systems, federal departments and organizations acquire only those products validated by NIAP (described in Section 4.5) or the NIST Cryptographic Module Validation Program. Biometric products used within DoD IT systems are subject to NSTISSP 11 requirements.

3.13.5 Federal Information Processing Standards (FIPS) 140-1 and 140-2

NIST FIPS publications 140-1 and 140-2 establish standards for the security features and validation requirements of cryptographic technologies. The NIST CMV Program prescribes a

[21] Technical information on the Java Card Biometry API is available at http://www.javacardforum.org/Documents/Biometry/biometry.html.

standard, repeatable, rigorous process for testing and certifying the cryptographic features of products.

FIPS 140-2, the more recent of the two cryptographic standards (published in May 2001), has replaced the older FIPS 140-1 for all new NIST CMV evaluations of cryptographic technologies. DoD mandates use of FIPS 140-2 in the current version of the JTA for uses of cryptographic modules in DoD environments.[22]

3.13.6 X.509

ISO/IEC 9594-8:2001, Information Technology: ITU-T Recommendation X.509, Open Systems Interconnection—The Directory: Public Key and Attribute Certificate Frameworks, provides a specification for digital certificates that DoD has mandated for use through the JTA.[23] **The BMO strongly recommends the use of X.509 certificates as a means of protecting the integrity of biometric data**. For more information on DoD use of X.509 certificates refer to *X.509 Policy Certificate Policy for the United States Department of Defense*, 11 Dec 2003, Version 8.0. This policy was prepared by the DoD PKI Program Management Office and was approved by ASD (NII).

3.13.7 JPEG and JPEG 2000

The Joint Photographic Experts Group (JPEG) specification is a long-standing common industry data format for compressing general image data. JPEG 2000 resulted from a standardization effort that culminated in publication of International Standard ISO/IEC 15444 Part 1. Specifications for biometric data formats that represent captured biometric samples (e.g., fingerprints, handwriting samples, iris photographs) as images frequently cite JPEG and JPEG 2000 as references. In particular, the draft Face Recognition and Iris Interchange Formats (described in Section 4) reference JPEG 2000. The JPEG and JPEG 2000 standards offer varying degrees of image compression, and one of the technical considerations in image compression is the question of how much compression of an image is allowable without degrading the quality of the original image. Implementations of the JPEG and JPEG 2000 standards must be capable of compressing and decompressing data to the same compression ratios.

3.13.8 International Civil Aviation Organization Machine Readable Travel Documents specification

The International Civil Aviation Organization (ICAO) is discussed in Section 4.1 as a third party organization that influences the development of biometric standards. ICAO, over a number of years since the 1980s, has been incrementally developing a three part series of standards documents known as the ICAO 9303 standards. The ICAO 9303 standards address “Machine Readable Travel Documents”, which include passport and visa documents. ICAO published a

[22] DoD mandates use of FIPS 140-2 in Section 5.3.2.7(a) of version 5 of the DoD JTA.
[23] DoD mandates use of X.509 in Section 5.3.1.2 (for Defense Message System secure messaging) and Section 5.7.1.1(a) (for PKI certificates) of version 5 of the DoD JTA.

technical report[24] in 2003 that calls for the storage of face image template and fingerprint template biometric data in storage chips used in travel documents. The technical report also addresses technologies outside of the scope of biometrics, such as bar codes and contactless integrated circuit cards.

3.14 BMO Standards Working Group Standards Recommendations

Table 15 summarizes the BMO Standards Working Group recommendations regarding existing biometric standards previously discussed in Section 3.

Table 15. Applicability of Existing Biometric Standards to DoD Environments

Standard Name	Section Where Discussed	BMO Standards Working Group Recommendations	DoD Biometric Solution Area of Applicability
ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information	Section 3.1	*This standard should continue to be used in Red Force biometric applications, per the 2 February 04 memorandum titled "DoD Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from "Red Force" Personnel"*	Collection Storage Use
EFTS Electronic Fingerprint Transmission Specification	Section 3.2	*This standard should continue to be used in Red Force biometric applications, per the 2 February 04 memorandum titled "DoD Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from "Red Force" Personnel"*	Access/Retrieval
BioAPI: ANSI INCITS 358-2002 Biometric Application Programming Interface	Section 3.3	*DoD should use the established BioAPI standard in all DoD implementations of biometric technology.*	Collection Storage Use

[24] The title of the report is: *Machine Readable Travel Documents: Development of a Logical Data Structure - LDS - for Optional Capacity Expansion Technologies – First edition, 2003.*

Standard Name	Section Where Discussed	BMO Standards Working Group Recommendations	DoD Biometric Solution Area of Applicability
CBEFF: NISTIR 6529-A Common Biometric Exchange Formats Framework	Section 3.4	*DoD should use the established CBEFF standard in all DoD implementations of biometric technology.*	Collection Storage
ANSI X9.84-2003 Biometric Information Management and Security for the Financial Services Industry	Section 3.5	*Some members of the M1 standards body have stated that there are minor incompatibilities between X9.84 data formats that use encryption and the CBEFF standard. The BMO Standards Working Group recommendation on the adoption of X9.84 is awaiting resolution of these compatibility issues.*	Collection Storage Access/Retrieval
ANSI/INCITS 377-2004 Finger Pattern Based Interchange Format	Section 3.6	*This standard is suitable for use in Blue Force biometric applications where data storage or transmission capacity is limited*	Collection Storage Access/Retrieval
ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange	Section 3.7	*This standard is suitable for use in Blue Force biometric applications where data storage or transmission capacity is limited.*	Collection Storage Access/Retrieval
ANSI/INCITS 381-2004 Finger Image-Based Data Interchange Format	Section 3.8	*This standard is suitable for use in biometric applications where access to full fingerprint images is required or desired.*	Collection Storage Access/Retrieval
ANSI/INCITS 385-2004 Face Recognition Format for Data Interchange	Section 3.9	*This standard is suitable for use in biometric applications where use of face recognition biometric technology is preferred.*	Collection Storage Access/Retrieval

Standard Name	Section Where Discussed	BMO Standards Working Group Recommendations	DoD Biometric Solution Area of Applicability
ANSI/INCITS 379-2004 Iris Image Interchange Format	Section 3.10	*This standard is suitable for use in biometric applications where use of iris recognition biometric technology is preferred.*	Collection Storage Access/Retrieval
OASIS XCBF v1.1 XML Common Biometric Format	Section 3.11	*The BMO Standards Working Group no longer recommends this standard for DoD use in its current form, as it has been subsumed into the X9.84-2003 standard and is no longer being maintained as a stand-alone standard.*	N/A
WSQ Wavelet Scalar Quantization	Section 3.12	*The BMO Standards Working Group recommends use of this standard as the preferred method for compressing fingerprint image data.*	Collection Storage
PDES Person Data Exchange Standard	Section 3.13	*The BMO Standards Working Group recommends use of this standard for the exchange of Red Force biographical data.*	Collection Storage
GSC-IS Government Smart Card Interoperability Specification	Section 3.13	*The BMO Standards Working Group recommends use of this standard for future generations of the DoD Common Access Card (CAC).*	Storage
FIPS 140-2 Federal Information Processing Standards 140-1 and 140-2	Section 3.13	*The BMO Standards Working Group recommends use of FIPS 140-2 approved encryption algorithms to protect biometric data in transit.*	Access/Retrieval
X.509 ISO/IEC 9594-8:2001, Information Technology: ITU-T Recommendation X.509, Open Systems Interconnection—The Directory: Public Key and Attribute Certificate Frameworks	Section 3.13	*The BMO Standards Working Group recommends the use of X.509 certificates as a means of protecting the integrity of biometric data.*	Collection Storage Access/Retrieval

Standard Name	Section Where Discussed	BMO Standards Working Group Recommendations	DoD Biometric Solution Area of Applicability
JPEG 2000: ISO/IEC 15444 Part 1 Joint Photographic Experts Group	Section 3.13	*Preferred format for compressing facial image data.*	Collection Storage

4. BIOMETRIC STANDARDS UNDER DEVELOPMENT

This section provides a status report on the activities of biometric standards bodies and a summary of several draft specifications for biometric standards under development by these standards bodies.[25]

Topics covered in this section include:

- Standards bodies and the standards development process
- Biometric template/data interchange formats
- Biometric application profiles
- Biometric performance testing
- NIAP protection profiles

4.1 Standards Bodies and the Standards Development Process

In the United States, the M1 technical committee is the primary standards body responsible for developing national biometric standards. M1 is technical committee under INCITS, the InterNational Committee for Information Technology Standards. INCITS is the recognized standards development organization for IT within the United States and operates under the rules of ANSI. INCITS does not restrict membership and attracts participants in its technical work from 13 different countries. The M1 technical committee, established in November 2001, is one of several INCITS standards committees that develop U.S. national commercial standards related to biometrics.

Two other INCITS committees, B10 and T4, have involvement in biometric-related issues. The B10 committee covers identification cards and related devices (e.g., issues related to smart cards); the T4 committee covers security techniques, which include a broad range of data security issues such as the security of biometric data. In addition, another ANSI-chartered organization, X9, is responsible for developing, establishing, publishing, maintaining, and promoting standards for the financial services industry. The ANSI X9F committee published the X9.84 Biometric Information Management and Security for the Financial Services Industry standard (discussed in Section 3.5) in 2001.

Figure 7 shows the relationship among the U.S. standards bodies. Each of the U.S. national standards bodies has a corresponding organization at the international level. The counterpart biometric standards body to M1 at the international level is SC 37 of the ISO/IEC Joint Technical Committee. SC 37 is the primary international standards body for biometrics. The international counterpart to the U.S. B10 identification cards committee is SC 17, and the international counterpart of the U.S. T4 security techniques committee is SC27.

[25] The status of the various draft specifications, as described in this section, represents a snapshot view as of August 2004. The status of these draft specifications is expected to change over time as standards bodies continue development of the specifications.

Figure 7. U.S. National Standards Organizations Related to Biometrics

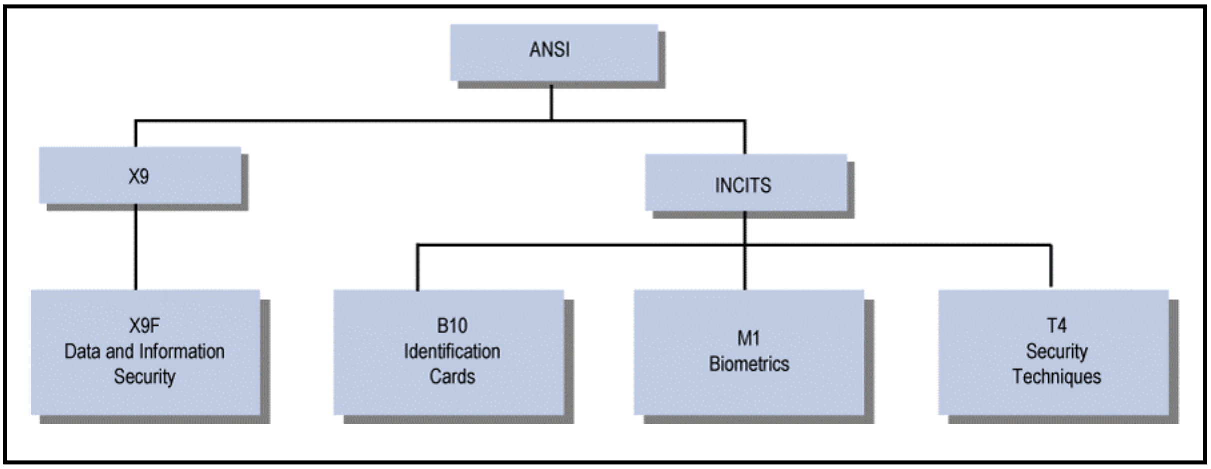
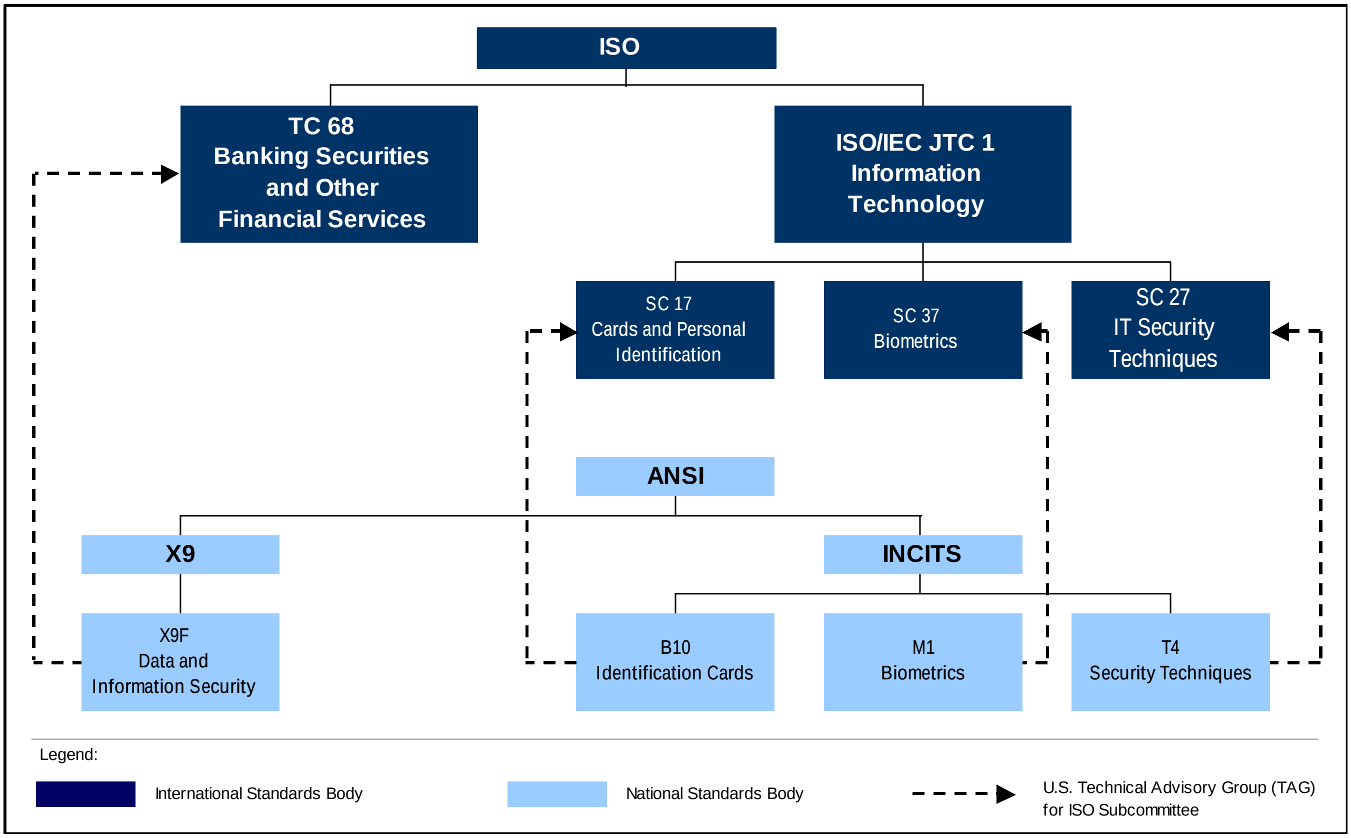


Figure 8 shows the relationship between the U.S. national biometric technology-related standards bodies and their international counterparts.

Figure 8. U.S. National Standards Bodies for Biometrics and Their International Counterparts

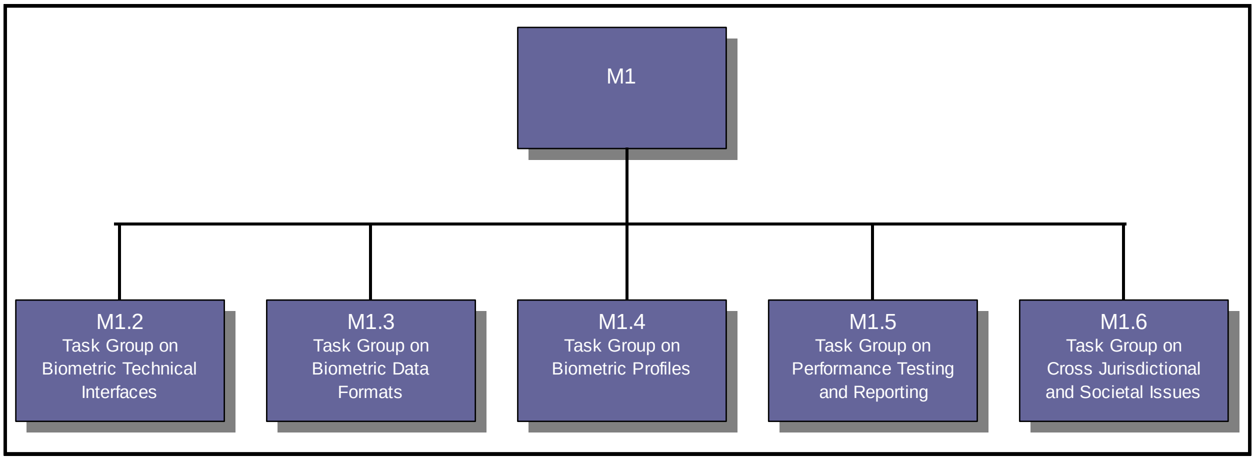


The M1 biometric standards committee consists of five permanent task groups that address specialized topics related to biometric standards development:

- M1.2: Task Group on Biometric Technical Interfaces
- M1.3: Task Group on Biometric Data Formats
- M1.4: Task Group on Biometric Profiles
- M1.5: Task Group on Performance Testing and Reporting
- M1.6: Task Group on Cross Societal and Jurisdictional Issues

Figure 9 provides a graphical depiction of the M1 task groups:

Figure 9. Task Groups of the M1 Biometric Standards Committee


M1
M1.2 Task Group on Biometric Technical Interfaces
M1.3 Task Group on Biometric Data Formats
M1.4 Task Group on Biometric Profiles
M1.5 Task Group on Performance Testing and Reporting
M1.6 Task Group on Cross Jurisdictional and Societal Issues

In addition to these five permanent task groups, M1 periodically establishes temporary ad hoc groups to address specific short-term issues related to its work. Ad hoc groups established by M1 in 2003 and 2004 have included:

- Ad Hoc Group on Harmonization of Vocabulary
- Ad Hoc Group on Biometric Sample Quality
- Ad Hoc Group on Evaluating Multi-Biometric Systems
- Ad Hoc Group on Conformity Assessment

Beyond the work of the M1 and SC 37 formal standards bodies, there are several other third-party organizations that are directly or indirectly involved in the development of biometric standards. These include the following:

- **BioAPI Consortium.** This consortium developed the BioAPI specification.

- **International Civil Aviation Organization (ICAO).** An organization of 188 member countries, ICAO has been active in 2002 and 2003 in defining specifications for use of biometrics in international travel documents such as passports and visas.

- **Organization for the Advancement of Structured Information Standards (OASIS).** This organization is connected to development of biometric standards through its work on the XCBF specification (discussed in Section 3.11).
- **NIST/BC Biometric Interoperability, Performance and Assurance Working Group (NIST/BC WG).** This working group (sponsored by NIST and the Biometric Consortium) is a major biometric standards incubator.
- **Federal Identity Credentialing Committee (FICC).** This is a U.S. Government interagency committee[26] that addresses government identity management topics and facilitates interagency coordination in areas such as public key infrastructure (PKI) planning.
- **General Services Administration Interagency Advisory Board.** This group is a joint effort between GSA and NIST to further smart card development and coordinate smart card deployment. The group is comprised of representatives from industry and federal, civilian, defense, and intelligence communities.

The M1 and SC 37 standards bodies coordinate the work of such organizations through liaison relationships between members of the organizations and the standards bodies.

4.2 Biometric Template/Data Interchange Formats

When a sample of biometric data is obtained from a user at enrollment, that biometric sample must be stored in some form for later use in biometric identification and verification. At this writing, most vendors of biometric products store representations of biometric samples in proprietary, non-interoperable, data formats. To facilitate interoperability of biometric products, the M1.3 Task Group on Biometric Data Interchange Formats has been developing several draft interchange format specifications since late 2002. Several of the biometric data interchange standards described in Section 3, such as the finger pattern, finger minutiae, finger image, iris, and face formats, originated their development in the M1.3 task group.

This section provides an overview of the following draft M1.3 draft biometric data interchange format specifications:

- Signature/Sign Interchange Format
- Hand Geometry Interchange Format.

Note that the technical specifications described in this section are currently only *draft* specifications and are not yet mature enough to be mandated for use within DoD.

[26] The Website for the FICC is http://www.cio.gov/ficc.

4.2.1 Signature/Sign Interchange Format

The draft Signature/Sign Interchange Format specifies a method of creating biometric templates of handwriting signature samples. The specification defines a Signature/Sign Image as "a set of sequentially sampled X, Y points of a digitized signature or sign, including time (T) and pressure (P) values. Positive X is to the 'right.' Positive y is 'up.'" The specification cites the BioAPI and CBEFF standards as normative references.

The specification includes the following statement in an informative (i.e., non-mandatory) section, and is of special note: "Since Signature/Sign biometric verification is essentially a 'behavioural' biometric, an author's template often records some measure of inherent variation and in this case, the biometric template might include mean values as well as their standard deviations for each feature."

The Signature/Sign Interchange Format is the only biometric type based on behavioral biometric measurements currently going through the standardization process. All of the other data interchange formats described in this document are based on physiological biometric measurements.

4.2.2 Hand Geometry Data Interchange Format

The draft Hand Geometry Data Interchange Format specifies a method of recording and storing a digital representation of a hand silhouette within a CBEFF data structure. Topics addressed by this specification include hand orientation during image capture, the use of finger alignment pins by the hand geometry reader, and the values of data header fields for the resulting CBEFF data generated in an image capture operation. The specification cites the CBEFF standard as a normative reference.

4.3 Biometric Application Profiles

A biometric application profile, also known as a "biometric profile," is a biometric standards document that serves as a catalog of the relevant biometric standards required to support a particular industry or a specialized type of biometric application. A biometric profile can:

- Mandate compliance with an existing standard (such as BioAPI or another of the standards discussed in Section 3) in full or in part,
- Waive specific sections of an existing standard and require the rest, or
- Mandate functionality identified as optional in an existing standard.

Five draft biometric application profiles are currently undergoing development in the M1.4 task group within the M1 biometric standards body:

- Biometric Verification and Identification of Transportation Workers
- Biometric-Based Personal Identification for Border Management

- Point-of-Sale Biometric Verification/Identification
- **DoD Application Profile**[27]
- Application Profile for Commercial Biometric Physical Access Control

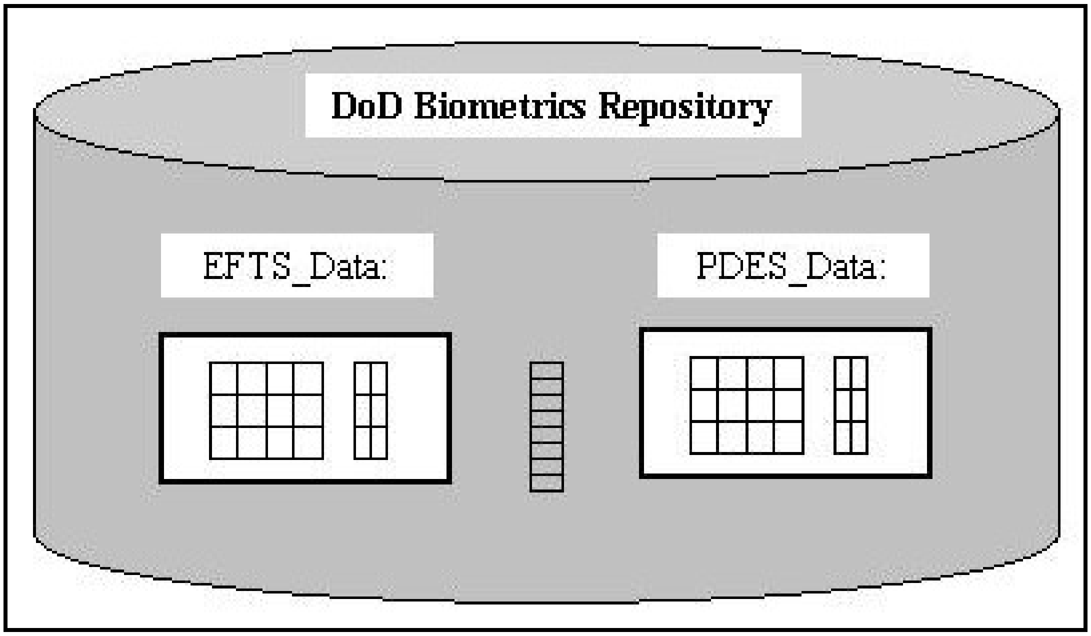
The BMO currently provides a project editor to develop a biometric application profile standard in the M1 standards body. The BMO submitted a project proposal to M1 in December 2003 to request the initiation of a formal standards project to develop a DoD biometric application profile standard. M1 reviewed and endorsed the project proposal for approval in January 2004. INCITS, the authorizing body for M1 standards projects, approved the project proposal for the DoD biometric application profile in early February 2004. The BMO submitted a base document to M1 in April 2004 that was endorsed by the M1.4 task group on biometric profiles as a M1 working draft in May 2004.

The DoD Application Profile provides standards guidance and requirements for both Red Force and Blue Force implementations of DoD biometric systems. Red Force standards requirements cited in the DoD Application Profile include mandatory support for ANSI/NIST ITL 1-2000, EFTS, PDES, and data interchange format standards described in Section 3. Blue Force standards requirements cited in the DoD Application Profile include mandatory support for the BioAPI, X9.84, and data interchange format standards (also described in Section 3).

One concept explained in the DoD Application Profile is the notion of utilizing *both* the “law enforcement community” biometric standards (ANSI/NIST ITL 1-2000 and the EFTS) as well as newer standards such as CBEFF and PDES in the repository of the DoD Automated Biometric Identification System (ABIS). This concept is illustrated in Figure 10.

[27] The formal name of the DoD Application Profile in the M1 standards body is “Biometric Profiles: Interoperability and Data Interchange- DoD Implementations.”

Figure 10. DoD Application Profile Cited Standards for DoD Biometric Repositories



Many more technical details on how the biometric standards described in this document can be applied to DoD Red Force and Blue Force biometric systems can be found in DoD Application Profile.

4.4 Biometric Performance Testing

In April 2002, the M1.5 Task Group on Biometric Performance Testing and Reporting began development of a four-part draft standard for biometric performance testing and reporting. The four parts of this draft standard, which is still in the development stage, are as follows:

- **Part 1:** Framework for Biometric Performance Testing and Reporting
- **Part 2:** Technology Testing and Reporting
- **Part 3:** Scenario Testing and Reporting
- **Part 4:** Operational Testing and Reporting

A.J. Mansfield and J.L. Wayman define the terms "technology," "scenario," and "operational" testing used in these standards as:[28]

- **Technology Testing.** The comparison of competing algorithms within a single technology (e.g., comparing two fingerprint minutiae algorithms)

[28] A. J. Mansfield and J. L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, version 2.01, August 2002, available at http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf.

- **Scenario Testing.** Testing to determine the overall system performance in a prototype or simulated application (e.g., a physical security application that controls access to a vehicle entrance gate)
- **Operational Testing.** Testing to determine the performance of a complete biometric system in a specific application environment with a specific target population (e.g., a biometric system used for network logical access control for the employees of a particular staff organization).

Development of biometric performance testing and reporting standards is still at an early stage and will likely progress more slowly than development of types of biometric standards because of the complex mathematical nature of biometric performance testing.

As of this writing, the M1.5 task group has circulated initial outlines for Parts 3 and 4 of the draft standard for initial member review and comments.

4.5 National Information Assurance Partnership Protection Profiles

NIAP protection profiles are reusable collections of security objectives and requirements that apply to a whole category of IT products. The NIAP Website[29] has existing protection profiles for the general product categories of firewalls, operating systems, tokens, intrusion detection systems, PKI, certificate management, peripheral sharing switches, and biometrics.

Biometric protection profiles conform to the international standard, "Common Criteria" (CC), for evaluating information technology security products, ISO/IEC 15408l and apply to all DoD components. They work closely with the Global Information Grid (GIG) Information Assurance guidance and policy, and the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11.

The Protection Profile (PP) falls under the broad scope of standards as they apply to Information Assurance. In its simplest form, a PP is the *test criteria* for security, against which a device is evaluated. Defining that test criteria is a complex matter. PPs contain a comprehensive collection of required information that allows products to be evaluated against a measurable set of requirements. PPs are the composite of the perceived threats, security policies, security objectives, security requirements and the rationale that links them.

A biometric PP is the minimum acceptable information security level for a given biometric device, technology or system, based on the robustness of probable threat for the environment of intended use. The DoD BMO has approached biometric PPs from the standpoint of user need, environment, functionality, and the current state of technology. As user needs, environments, threats and technologies change, biometric PPs may be added, changed or removed as warranted.

Currently the DoD BMO and NSA are developing five protection profiles for biometric products that meet the "Common Criteria" (CC) international standard for evaluating information

[29] The Website for NIAP is http://niap.nist.gov.

technology security products. The research and development of the PP document is being accomplished through the efforts of a Protection Profile Working Group for biometrics. The working group is made up of technical and security experts from several organizations. In addition to BMO and NSA, representatives from the U.S. Navy, U.S. Air Force and U.S. Army's Product Manager Secure Electronic Transaction Devices (PM SET-D) have contributed in development of the biometric PPs. Development and publication of biometric PPs have begun. At present, three of the five initial PPs are complete or in development. The PPs are being completed in the following order:

1. Medium Robustness Biometric PP for Verification[30] Mode
2. Basic Robustness Biometric PP for Verification Mode
3. Medium Robustness Biometric PP for Identification[31] Mode
4. Basic Robustness Biometric PP for Identification Mode
5. High Robustness Biometric PP

Two example security policy requirements from the first of these profiles, the U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, are listed in Table 16.

Table 16. Example Security Policy Requirements from the U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments

Protection Profile Security Policy Requirement	Requirement Description
P.CRYPTOGRAPHY_ VALIDATED	Where the TOE[32] requires FIPS-approved security functions, only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e., generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e., encryption, decryption, signature, hashing, key distribution, and random number generation services).
P.VULNERABILITY_ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

In the example security policy requirements listed above, "P.CRYPTOGRAPHY_VALIDATED" is an example requirement name, where the "P" denotes

[30] Verification is one-to-one identity authentication.
[31] Identification is one-to-many identity authentication.
[32] A "TOE" is a Target of Evaluation, i.e., the biometric product being evaluated by NIAP.

that it is a security policy requirement. The descriptions of the requirements tend to be technically detailed, and go beyond the scope of what this document discusses.

Biometric PPs are one cornerstone of the DoD acquisition process for biometric products. When biometric products attach to the GIG, they join an environment that has been evaluated against a certain threat level and in turn will need to be certified against an applicable protection profile prior to acquisition and incorporation into that environment.

4.6 International Activities

Most of the information presented in this document is focused on biometric standards either currently in use in the United States (Section 3) or under development within the M1 U.S. biometric standards body. This section gives a brief synopsis of the structure of the international standards body for biometrics, ISO JTC1/SC37.

SC 37 is organized into the following six permanent working groups:

- WG 1, Harmonized Biometric Vocabulary and Definitions
- WG 2, Biometric Technical Interfaces
- WG 3, Biometric Data Interchange Formats
- WG 4, Profiles for Biometric Applications
- WG 5, Biometric Testing and Reporting
- WG 6, Cross Jurisdictional and Societal Aspects

Working group (WG) 1 focuses on internationally standardizing biometric vocabulary, as its name implies. WG2, Biometric Technical Interfaces, is the SC37 working group that develops international versions of the BioAPI and CBEFF standards discussed in Section 3. WG 3, Biometric Data Interchange Formats, develops international versions of the data format specifications described in Sections 3 and 4. WG 5, Biometric Testing and Reporting, began development of a four-part standard for biometric performance testing and reporting in September 2003. WG 6, Cross Jurisdictional and Societal Aspects, is the working group in SC37 that has begun to address privacy concerns and other social concerns related to biometric standards.

Table 17 provides an overview of the international counterparts to U.S. standards under development in SC 37 as of July 2004.

Table 17. Standards Under Development in SC 37

US Standard Name	ISO SC 37 Project
ANSI INCITS 358-2002 BioAPI	**ISO/IEC FCD 19784-1 and WD 19784-2** BioAPI Part 1: BioAPI Specification Part 2: Biometric Archive Function Provider Interface
CBEFF: NISTIR 6529-A	**ISO FCD 19785-1 and WD 19785-2** CBEFF Part 1: Data Element Specification Part 2: Testing methodologies
ANSI X9.84-2003 Biometric Information Management and Security for the Financial Services Industry	**ISO WD 19092** Biometric Information Management and Security for Financial Applications
(No equivalent in M1)	**ISO/IEC CD 19794-1** Biometric data interchange formats -- Part 1: Framework
ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange	**ISO/IEC FCD 19794-2** Biometric data interchange formats -- Part 2: Finger Minutiae Based Interchange Format
ANSI/INCITS 377-2004 Finger Pattern-Based Interchange Format	**ISO/IEC CD 19794-3** Biometric data interchange formats -- Part 3: Finger Pattern Based Interchange Format
ANSI/INCITS 381-2004 Finger Image-Based Interchange Format	**ISO/IEC FCD 19794-4** Biometric data interchange formats -- Part 4: Finger Image Based Interchange Format
ANSI/INCITS 381-2004 Face Recognition Format for Data Interchange	**ISO/IEC FCD 19794-5** Biometric data interchange formats -- Part 5: Face Recognition Format for Data Interchange
ANSI/INCITS 379-2004 Iris Image Data Interchange Format	**ISO/IEC FCD 19794-6** Biometric data interchange formats -- Part 6: Iris Image Format for Data Interchange

US Standard Name	ISO SC 37 Project
Project INCITS 1603-D Signature/Sign Data Interchange Format	**ISO/IEC WD 19794-7** Biometric data interchange formats -- Part 7: Signature/Sign Behavioral Data
(No equivalent in M1)	**ISO/IEC WD 19794-8** Biometric data interchange formats -- Part 8: Finger Pattern Skeletal Data
Project INCITS 1602-D Biometric Performance Testing and Reporting	**ISO/IEC WD 19795-1; 19795-2; 19795-3; 19795-4** Information technology -- Biometric performance testing and reporting Part 1: Test Principles Part 2: Test Methodologies Part 3: Developing Specific Test Methodologies Part 4: Specific Test Methodologies
Project INCITS 1703-D Conformance Testing for BioAPI	**ISO/IEC WD 24701-1; 24709-2** **Conformance Testing for BioAPI –** Part 1: Methods and Procedures Part 2: Test Assertions
Project INCITS 1643-D Hand Geometry Data Interchange Format	New Project Proposal for ISO/IEC 19794-N**,** Hand Geometry Data Interchange Format

4.7 Biometric Security

In addition to the work related to ANSI X9.84 in ISO/IEC TC68 (discussed in Section 3.5), standardization of the security aspects of biometric data and systems is allocated to ISO JTC1/SC 27. Work there is in the preliminary stage and has been assigned to an Ad-hoc Group on Biometric Security Standardization. This Ad-hoc Group has initiated three Study Periods, which are temporary subgroups that analyze and report back to a parent organization on a specific topic of interest:

- Security management and biometrics
- Authentication of biometric data
- Biometric security valuation and testing

SC 27 also has initiated a New Work Item on biometric template protection. This New Work Item may include liaison relationships with TC68 and SC 37 to collaborate on the progression of X9.84 as an international standard.

5. RECOMMENDED DOD PRIORITIZATION FOR BIOMETRIC STANDARDS DEVELOPMENT

This section presents recommendations of actions that DoD can take to accelerate development of biometric standards in areas in which DoD has a critical need for standards. Critical areas of biometric standards discussed in this section are:

- DoD biometric application profiles
- Biometric conformance testing standards
- Biometric performance testing standards
- Biometric data interchange (e.g., template) standards

Each of these standards development areas also needs accompanying *policies* to effectively institute the use of the standards in the DoD. The BMO is developing draft policies for each of these areas for DoD senior leadership to review and approve as the standards involve reach a sufficient state of maturity.

5.1 DoD Biometric Standards Development Priorities

Four biometric standards development areas that are of high priority to DoD are outlined in Table 18. The suggested ranking of these four high-priority development areas is based on DoD's relative ability to significantly influence and advance the standards in question. DoD can have a substantial impact on conformance and performance testing standards over a 1-year period and can then incorporate this work into DoD application profiles. Progress in the area of biometric data interchange standards has been significant in the past year; this area requires continued vigilance and involvement by DoD at current levels.

In reading the recommendations in Table 18, keep in mind that standards bodies such as M1 and SC 37 refer to the primary coordinator of standards documents as "project editors." A project editor leads the development of a specific standard as it goes through the standards body processes, and also coordinates all comment, review, and update activities associated with the standard. A "technical contributor" is a standards body participant who authors a portion, or portions, of a standard or provides comments on a standards document that influence the direction of the standard in question. Technical contributors author all portions of a standards document, while the project editor assembles the contributions. Project editors often serve also as technical contributors.

The BMO's general approach for providing technical contributions is to initially focus on advancing U.S. (that is, M1) national standards projects. In cases where BMO contributions can also simultaneously advance international standards projects, such as BioAPI conformance testing standards, BMO contributions are offered to those projects as well.

Table 18. DoD Biometric Standards Development Priorities, Ranked by Impact

Priority #	Mapping to Executive Summary Recommendations	Biometric Standards Development Area	Recommended DoD BMO Role in Development of the Standards
1	#5	DoD application profiles	**Lead**: Continue providing dedicated editor to author national standards documents, tailoring all DoD biometric standards requirements into one set of standards documentation.
2	#2, #3	Conformance testing standards	**Lead**: Continue providing dedicated editor to author national and international standards documents. Provide majority of the technical contributions to the standards and participate in resolution of comments from standards bodies.
3	#4	Performance testing standards	**Participant**: Develop national and international technical contributions to standards to add content for topics most relevant to DoD. For the specific topics relevant to DoD, assuming a lead role is appropriate.
4	#6	Data interchange (e.g., template) standards	**Contributor**: Track progress of the national and international standards, review and provide comments on working drafts, vote on draft approvals, and report progress on the standards to DoD stakeholders.

Section 2.3 of this document introduced the actions ranked as Priorities #1 and #2 above, namely the development of DoD application profile standards and biometric conformance testing standards. This section provides further detail on the standards development work that DoD must accomplish to accelerate development of standards in these areas. Priority #1, DoD application profiles, can bind all standards requirements defined in multiple standards into a single reference for DoD biometric project managers and systems integrators. Priority #4, biometric data interchange standards, is the area in which standards development is now progressing most successfully. Although this area of work continues to be highly important to DoD, direct DoD intervention is not as critical to the success of this work as it is in the areas of biometric performance testing and conformance testing standards.

5.2 DoD Biometric Application Profiles

The DoD Application Profile serves as a standards focal point for identifying the technical details of biometric standards related to the Global War on Terrorism. The draft DoD Application Profile currently under development in the M1 standards body contains extensive information about Red Force biometrics collection. The Red Force biometrics content in the DoD Application Profile will continue to evolve through 2004 as DoD policies related to Red Force biometrics become further defined.

As explained in Section 2, biometric application profiles provide logical groupings of subsets of other biometric standards (e.g., data format standards, performance testing standards, and conformance testing standards) to serve as a consolidated collection of requirements for use in biometrics acquisition and system integration. **The BMO Standards Working Group recommends that DoD continue efforts initiated in 2004 in developing one or more DoD biometric application profiles.** This will consolidate all standards requirements defined in multiple standards into a single reference for DoD biometric project managers and systems integrators.

Application profiles can provide guidance on the values and options used from applicable standards. The proposed work will start with a single profile that attempts to define universal standards requirements for all DoD biometric applications. However, it is possible that more than one profile may be necessary to accommodate differing or incompatible requirements for different DoD uses of biometrics. For example, a tactical-environment use of biometrics may have radically different requirements for biometric standards than does a logical access (e.g., internal office network) application of biometrics.

The BMO Standards Working Group recommends that development of the first DoD Application Profile standard continue in the M1 standards body, and that inputs from a wider DoD audience be incorporated into the profile.

The BMO Standards Working Group envisions the possibility that more than one DoD biometrics application profile may be necessary to meet the diverse needs of DoD biometric applications. The “split” of the current DoD Application Profile standard, if it occurs, would likely produce one standard for Red Force DoD biometric applications, and a separate standard for Blue Force DoD biometric applications. This issue is currently under review by the BMO.

The approach to developing the first generation of DoD application profiles is iterative, or “spiral” in nature, with each iteration refining the set of capabilities and standards requirements that apply to DoD. This process provides the opportunity for continuous feedback and interaction between DoD users of biometrics and the developers of the profile. The application profile developer refines the requirements listed based on user feedback.

5.3 Conformance Testing Standards

Biometric conformance testing standards are of great importance to DoD and an area in which DoD can make a substantial contribution to advancing the state of standards in 2004 and 2005. Currently, there are no established national or international conformance testing methodology standards that allow a testing organization to measure how well a biometric product conforms to a given standard (for example, the BioAPI standard discussed in Section 3). **The BMO Standards Working Group recommends that DoD continue efforts initiated in 2004 in the development of national and international biometric conformance testing standards and**

the development of a BioAPI conformance test suite/testing framework. These initiatives are crucial to implementing the "standards, interoperability tools, [and] testing frameworks" mandated in the 25 August 2003 Deputy Secretary of Defense DoD Biometrics Enterprise Vision memorandum, discussed in Section 1.2.

Table 19 provides a list of proposed DoD standards contributions that will accelerate the development of national and international biometric conformance testing standards. This list of contributions is only a starting point and will be adjusted as necessary to meet the mission needs and requirements of DoD organizations deploying biometric solutions.

Table 19. DoD Biometric Conformance Testing Standardization Topics

Proposed Conformance Testing Topic	Biometric Conformance Testing Topic Description	Development Time Frame
1	Conformance testing methodology for the BioAPI standard.	FY 2004–FY 2005
2	Conformance test suite/testing framework development for BioAPI conformance testing.	FY 2004–FY 2006
3	Conformance testing methodology for finger image data interchange format. [33]	FY 2004–FY 2005
4	Conformance testing methodology for the CBEFF standard.	FY 2005–FY 2006

One item of special significance in Table 19 is Topic #2, Conformance test suite/testing framework development for BioAPI conformance testing. This item differs from the others listed in that it involves the development of conformance testing *software* as opposed to conformance testing standards documentation. As explained in Section 3.3 of this document, the BioAPI standard is arguably the *most* important biometric standard currently in existence in terms of providing interoperability and interchangeability between biometric vendor products.

However, the BFC, the DoD organization primarily responsible for testing and evaluation of biometric products, has indicated that it cannot adequately evaluate the interoperability of vendor products that claim to support the BioAPI standard because of a complete lack of BioAPI testing tools in the commercial marketplace. Therefore, **the BMO Standards Working Group recommends that DoD continue to develop an initial testing suite/testing framework for BioAPI conformance testing** to enable the BFC, and other organizations, to conduct BioAPI conformance testing as part of its product evaluation testing processes. This conformance test suite will support the Deputy Secretary of Defense's direction, expressed in his 25 August 2003 memorandum, to "ensure that the appropriate standards, interoperability tools, testing frameworks, and approved product validations" are available to the DoD community.

Since the January 2004 version of this document was published, the BMO has made significant progress in the development of BioAPI conformance testing at the national and international

[33] The specific interchange format specification chosen for conformance methodology development would be one of the three fingerprint-related specifications discussed in Section 3.

levels. The SC37 standards body has begun development of a two-part international standard for BioAPI Conformance Testing, where Part 1 establishes the testing framework and Part 2 defines test assertions. A BMO representative has been approved by SC37 to lead the development of international BioAPI conformance testing standards as *editor* of Part 2 of the standard. The BMO is now providing a *co-editor* for Part 1 of this standard, and *lead editor* for Part 2 of the standard. A project proposal to begin a U.S version of conformance testing standards for BioAPI was submitted to the M1 standards body in May 2004. The BMO is a contributor to this project.

The BMO began work in May 2004 to develop a conformance testing methodology standard for the Finger Image data interchange format, ANSI/INCIT 381-2004. The BMO submitted a project proposal to the M1 standards body to obtain approval to initiate a standards development project in this area in April 2004. M1 approved the project proposal submitted by the BMO in May 2004. The BMO believes that it will be important to have conformance testing standards for each of the biometric data interchange format standards that DoD will use in operational systems.

5.4 PERFORMANCE TESTING STANDARDS

In the U.S. Government community, NIST and the Department of Homeland Security (DHS) have assumed leadership roles in the development of biometric performance testing standards contributions. **The BMO Standards Working Group recommends that the BMO augment and support the contributions being provided by NIST and DHS in advancing standards in this area**.

The establishment of biometric performance testing and reporting standards is one of the most technically complex areas in biometric standards development. Many technical and administrative variables affect the manner in which biometric performance testing is performed, and variations in these items produce variations in testing results. Some of the variables that affect biometric performance testing and reporting are the procedures used, the environmental settings (such as temperature, humidity, and lighting) used in the capture and testing processes, the demographic diversity (e.g., age differences, ethnic differences) of the users who provide the biometric samples used in the testing, differences in the biometric hardware and software used during biometric capture and biometric testing, and differences in the education/awareness levels of the users who provide the biometric samples.

In addition to these concerns, there is mathematical complexity involved in properly performing statistical analysis of testing results. An extensive understanding of probability theory and statistics is necessary to interpret testing results. Even when the analysts involved have a sufficient mathematical background, simplifying assumptions (which may or may not be valid for the user population tested) are necessary to estimate FMR or FNMR statistics from a set of biometric testing data.

In April 2003, the performance testing ad hoc group of the M1 standards committee (which became a formal task group in June 2003) agreed to develop the following four-part biometric performance-testing standard:

- Part 1: Framework for Biometric Performance Testing and Reporting
- Part 2: Technology Testing and Reporting
- Part 3: Scenario Testing and Reporting
- Part 4: Operational Testing and Reporting

Development of biometric these performance testing and reporting standards is still at an early stage and will likely progress more slowly than development of types of biometric standards because of the complex mathematical nature of biometric performance testing.

5.5 Data Interchange/Template Standards

The establishment and use of biometric data interchange standards is a high priority for DoD. In particular, establishment of standards for biometric *template* representation is critical to DoD's achievement of interoperability between the biometric devices used by different biometric vendors. Biometric template formats currently are proprietary to each vendor of biometric equipment, which makes achievement of interoperability between biometric equipment vendors impossible at present. Interoperability between vendor equipment will be possible only after multiple biometric vendors implement and use data interchange standards in commercial products. Interagency common biometric template standards will enhance many business processes of the DoD and other federal organizations.

Several draft biometric data interchange formats that were under development in the M1 standards body in 2003 were recently approved as ANSI standards in 2004. These specifications are now in the process of becoming ISO standards, as discussed in Section 4.6.

5.6 Biometric Security Standards

Security standards can address protection of biometric data, management of the security of biometric systems, and assessment of the assurance level of biometric systems. Given the environments in which the DoD is expected to operate biometric systems, the establishment of these security standards is a high priority for the BMO. While the efforts to develop these standards are in their infancy (as discussed in Section 4.7), it is important for the DoD to track their progress and guide their development where necessary.

The recommended future roles of the DoD BMO in this area of biometric standards development are as follows:

- Track the progress of the SC 27 Ad-hoc group on Biometric Security Standardization and the New Work Item on biometric template protection.

- Provide resources to develop the standards that are determined to be required during the three SC 27 Study Periods. Participate via INCITS T4, the U.S. TAG to SC 27.
- Contribute to the New Work Item on biometric template protection (again, via membership in T4).
- Report progress on the standards to DoD stakeholders.
- Review draft standards and execute votes in T4.

5.7 Conclusion

Table 20 outlines the criticality of the BMO's recommendations regarding biometric standards development and the need for additional DoD resources.

Table 20. Criticality of BMO's Recommendations

Recommendation		Criticality to DoD	Need for Continued Commitment of DoD Resources
1	DoD should use the established Biometric Application Programming Interface (BioAPI) and Common Biometric Exchange Formats Framework standards in all DoD implementations of biometric technology.	High	Low
2	DoD should assume a lead role in the development of national and international biometric conformance testing standards.	High	High
3	DoD should assume a lead role in the development of a BioAPI conformance test suite/testing framework.	High	High
4	DoD should assume a contributor role by developing specific technical contributions in the development of national and international biometric performance testing standards. Responsibilities for this role include tracking progress of the standards, reviewing and providing comments on working drafts, and reporting progress on the standards to DoD stakeholders.	High	Medium
5	DoD should assume a lead role, including editorial responsibilities, in the development of one or more national DoD biometric application profile standards.	High	High

Recommendation		Criticality to DoD	Need for Continued Commitment of DoD Resources
6	DoD should assume a contributor role in the development of national and international biometric data interchange (e.g., template) standards. Responsibilities for this role include tracking progress of the standards, reviewing and providing comments on working drafts, and reporting progress on the standards to DoD stakeholders.	High	Low
7	BMO should actively participate in appropriate national and international standards bodies to exert DoD influence on the direction and adoption of standards important to DoD.	High	Medium

A significant amount of work on developing biometric standards is now under way, as this document has outlined, and much of the work is of great importance to DoD. Figure 10 illustrates the areas of standards development that are most critical to DoD and how those development activities relate to the standards activities of national and international standards bodies.

Figure 11 captures, in a simplified fashion, DoD's standards priorities versus the development efforts being pursued by standards bodies. The landscape of current biometric standardization work is broadly divisible into four categories:

- Biometric standards development work that is progressing but is not directly tied to critical DoD biometric standards priorities.
- Biometric standards development work that is progressing and is directly tied to critical DoD biometric standards priorities.
- Critical biometric standards development work that is of strategic importance to DoD and is currently lacking in resources.
- Biometrics as a significant tool to assist the DoD to become interoperable with other federal organizations in new and emerging mission areas like homeland defense and maritime awareness.

Figure 11. DoD Standards Priorities Compared With Development Activities of Standards Bodies

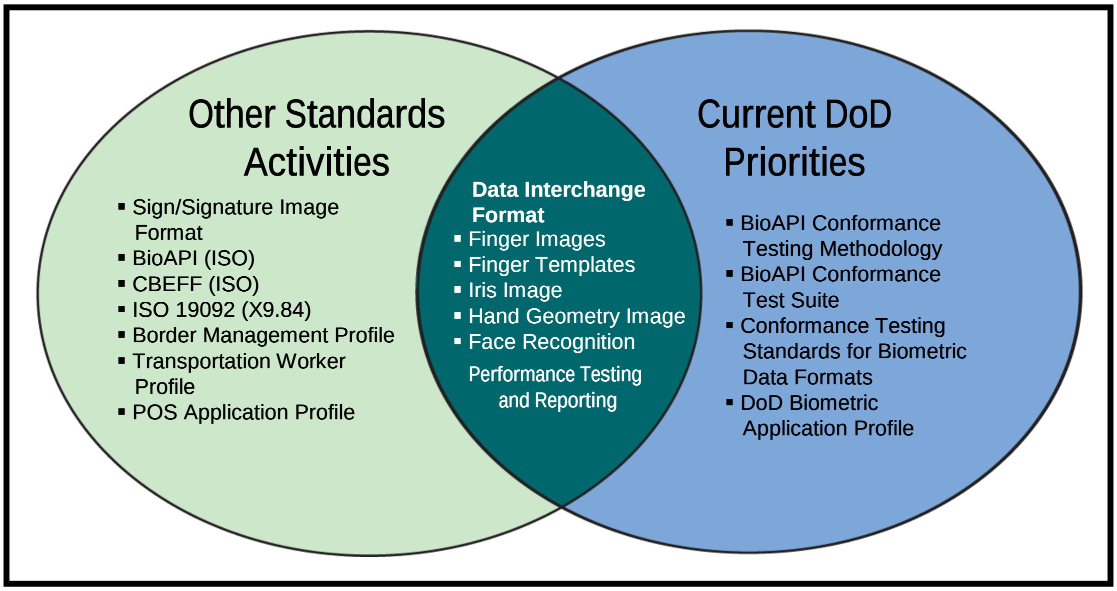

Other Standards Activities
▪ Sign/Signature Image Format
▪ BioAPI (ISO)
▪ CBEFF (ISO)
▪ ISO 19092 (X9.84)
▪ Border Management Profile
▪ Transportation Worker Profile
▪ POS Application Profile
Data Interchange Format
▪ Finger Images
▪ Finger Templates
▪ Iris Image
▪ Hand Geometry Image
▪ Face Recognition
Performance Testing and Reporting
Current DoD Priorities
▪ BioAPI Conformance Testing Methodology
▪ BioAPI Conformance Test Suite
▪ Conformance Testing Standards for Biometric Data Formats
▪ DoD Biometric Application Profile

Figure 11 shows two circles of high-priority interests. The circle on the left depicts the issues on which biometric standards bodies are now working; the circle on the right depicts DoD biometric standards priorities. The left side of the left circle depicts standards development work that is progressing successfully without direct DoD intervention. Within this area, the BioAPI, CBEFF, and X9.84 standards are established U.S. biometric standards and are well on their way to becoming international standards. The three biometric application profiles listed are of interest to organizations outside of DoD but are not strategic priorities for DoD.

The center portion of Figure 11, where the two circles intersect, depicts standards development projects that are *both* actively under development by standards bodies *and* of high strategic priority to DoD. These include biometric data interchange format standards and biometric performance testing standards.

The right side of Figure 11 shows standards development activities that are of high strategic priority to DoD and are *not* currently receiving adequate attention from other participants in the M1 biometric standards body. Activities in this category include the development of conformance testing standards for the BioAPI specification (described in Section 3.3) and the Finger Image Data Interchange Format (described in Section 3.8), development of a conformance test suite for BioAPI, and DoD biometric application profiles. DoD must take a leading role in the development of standards in these areas to ensure that they are completed in a timely manner.

The initial version of this document served as a starting point for coordinating the development and advancement of biometric standards within the DoD and between the DoD and other U.S. Government organizations. The document was well received, and led to an inter-agency U.S. Government Workshop on “Biometric Standards in Support of the Global War on Terrorism” in May 2004. The workshop has generated a tremendous level of cooperation between the DoD, the Department of Homeland Security, and other organizations. More work and inter-agency coordination is needed, and the benefits for using biometrics as a tool in fighting the Global War on Terrorism are clear.

APPENDIX A: ADDITIONAL SELECTED POLICIES AND GUIDANCE

The policies shown below in Table A-1 are relevant to the importance, development, and implementation of standards. Although this table may expand the reader's knowledge of standards and interoperability policies, it does not claim to represent a complete listing of such policies.

Table A-1. Additional Selected Policies and Guidance

Name of Policy	Policy Statement(s)	Applicability to DoD
National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11	IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and IA-enabled IT products. These products should provide for the availability of the systems, ensure the integrity and confidentiality of information, and ensure the authentication and non-repudiation of parties in electronic transactions. Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with the Information Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement; the NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or the NIST Federal Information Processing Standard {FIPS) validation program. Accredited commercial laboratories, or the NIST will conduct the evaluation/validation of COTS IA and IA-enabled IT products.	This policy is important because there are currently no biometric products that are in compliance with this policy. The process for becoming certified is time consuming and expensive. However, product certification/validation increases the level of confidence in the security of such products.
Chairman, Joint Chiefs of Staff, Joint Vision 2010	Emphasizes common usage between Services and increased interoperability among the Services and multinational partners.	This policy is important because it demonstrates DoD's commitment to and requirement for interoperability between the Services and multinational partners.

Name of Policy	Policy Statement(s)	Applicability to DoD
Chairman, Joint Chiefs of Staff, Joint Vision 2020	Emphasizes interoperability as the foundation of effective joint, multinational, and interagency operations. Also emphasizes total interoperability, including technology, processes, and organizations.	This policy is important because it demonstrates DoD's long-term commitment to and requirement for interoperability for the successful performance of joint operations.
United States Code, Title 10, Section 2223, latest revision	Designates the responsibilities of Chief Information Officers, including ensuring that IT and national security systems standards that will apply throughout the DoD are prescribed.	This policy is important because it highlights the value of standards for IT and national security systems within DoD.
DoD Directive 4630.5: Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	Directs the use of a mission related, outcome-based approach to ensure interoperability and supportability of IT and NSS throughout the Department of Defense	This policy stresses the need for interoperability to be factored into the early stages of the life cycle of all DoD acquisition programs and procurements.
DoD Instruction 4630.8: Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	Directs the use of a mission related, outcome-based approach to ensure interoperability and supportability of IT and NSS throughout the Department of Defense	This policy expands upon the guidance in DODD 4630.5 and mandates use of interoperability test plans.

APPENDIX B: ABBREVIATIONS AND ACRONYMS

AAMVA	American Association of Motor Vehicle Administrators
ANSI	American National Standards Institute
API	Application Programming Interface
ASN.1	Abstract Syntax Notation 1
BFC	Biometrics Fusion Center
BioAPI	Biometric Application Programming Interface
BIR	Biometric Information Record
BMO	Biometrics Management Office
BSCG	Biometrics Senior Coordinating Group
C4IEWS	Command, Control, Communications, Computers, Intelligence, Electronic Warfare and Sensors
CAC	Common Access Card
CBEFF	Common Biometric Exchange Formats Framework
CID	Criminal Investigative Division
CJIS	Criminal Justice Information Services
CMS	Cryptographic Message Syntax
CMV	Cryptographic Module Validation
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DL	Drivers License
DoD	Department of Defense
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FICC	Federal Identity and Credentialing Committee
FIPS	Federal Information Processing Standard
FMR	False Match Rate
FNMR	False Non-Match Rate
FY	Fiscal Year
GSA	General Services Administration
GAO	Government Accounting Office
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
GSC	Government Smart Card
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IBIA	International Biometric Industry Association
ICAO	International Civil Aviation Organization
ID	Identification

IEC	International Electrotechnical Commission
IEW&S	Intelligence, Electronics Warfare and Sensors
INCITS	International Committee for Information Technology Standards
IP	Intellectual Property
IS	Interoperability Specification
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
IT	Information Technology
JPEG	Joint Photographic Experts Group
JTA	Joint Technical Architecture
JTC 1	Joint ISO/IEC Technical Committee 1
MAP	Master Action Plan
MILSPEC	Military Specification
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSA	National Security Agency
NSS	National Security System
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTTAA	National Technology Transfer and Advancement Act
OASIS	Organization for the Advancement of Structured Information Standards
PKI	Public Key Infrastructure
PP	Protection Profile
SC 37	Subcommittee 37 of ISO/IEC Joint Technical Committee 1
SMT	Scar Mark & Tattoo
TAG	Technical Advisory Group
USD (A&T)	Under Secretary of Defense for Acquisition and Technology
WG	Working Group
WSQ	Wavelet Scalar Quantization
XCBF	XML Common Biometric Format (component of X9.84-2003)
XCMS	XML Cryptographic Message Syntax
XML	eXtensible Markup Language

APPENDIX C: GLOSSARY

American National Standards Institute (ANSI). The principal standards coordination body in the United States.

Application Profile. A document that identifies a set of two or more existing prerequisite biometric standards and identifies the classes, subsets, options, and parameters of those base standards that are necessary for accomplishing a particular function.

Authentication. Security measure that verifies a claimed identity. Two types of authentication used in biometric systems are *verification* (or one to one matching) and *identification* (or one to many matching).

Base Standard. An existing standard that is referenced by other standards documents or draft specifications.

Biometric Information Record. The electronic representation of a human being's biometric data, such as fingerprint images, fingerprint templates, iris images, etc.

Biometric Service Provider. Low-level software that manages biometric device hardware.

Biometrics. Measurable physical characteristics or personal behavioral traits used to recognize the identity or verify the claimed identity of an individual.

Common Biometric Exchange Formats Framework. A standard that defines a common set of data elements that are necessary to support multiple biometric technologies. Defined in NISTIR 6529-A (to be published).

Common Criteria. An international standard, formally designated ISO standard 15408, that serves a catalog of security functionality and assurance requirements for evaluating information technology products.

Joint Technical Committee (JTC) 1. JTC 1 was formed in 1987 by the merger of ISO Technical Committee 97 and International Electrotechnical Commission (IEC) Technical Committees 47B and 83 to avoid development of possibly incompatible information technology standards by ISO and IEC. ANSI represents the U.S. Government in ISO and JTC 1.

International Organization for Standards (ISO). ISO is a worldwide federation of national standards bodies from approximately 100 countries (one from each country). ISO's work results in international agreements, which are published as International Standards.

M1. M1 is the principal U.S. standards body for biometrics**.** M1 is a technical committee of the InterNational Committee for Information Technology Standards (INCITS), and develops biometric standards that are ultimately reviewed and approved by the American National Standards Institute (ANSI).

National Information Assurance Partnership (NIAP). A collaboration between the National Institute of Standards and Technology and the National Security Agency with the goal of helping increase the level of trust that consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs.

Normative Reference. A standards document that provides details about the requirements that must be met to be compliant with the standard in question.

Protection Profile. An implementation-independent set of security requirements for a category of Targets of Evaluation that meet specific consumer needs.

Red Force. Enemy prisoners of war, detainees, civilian internees, and other persons of interest with respect to national security.

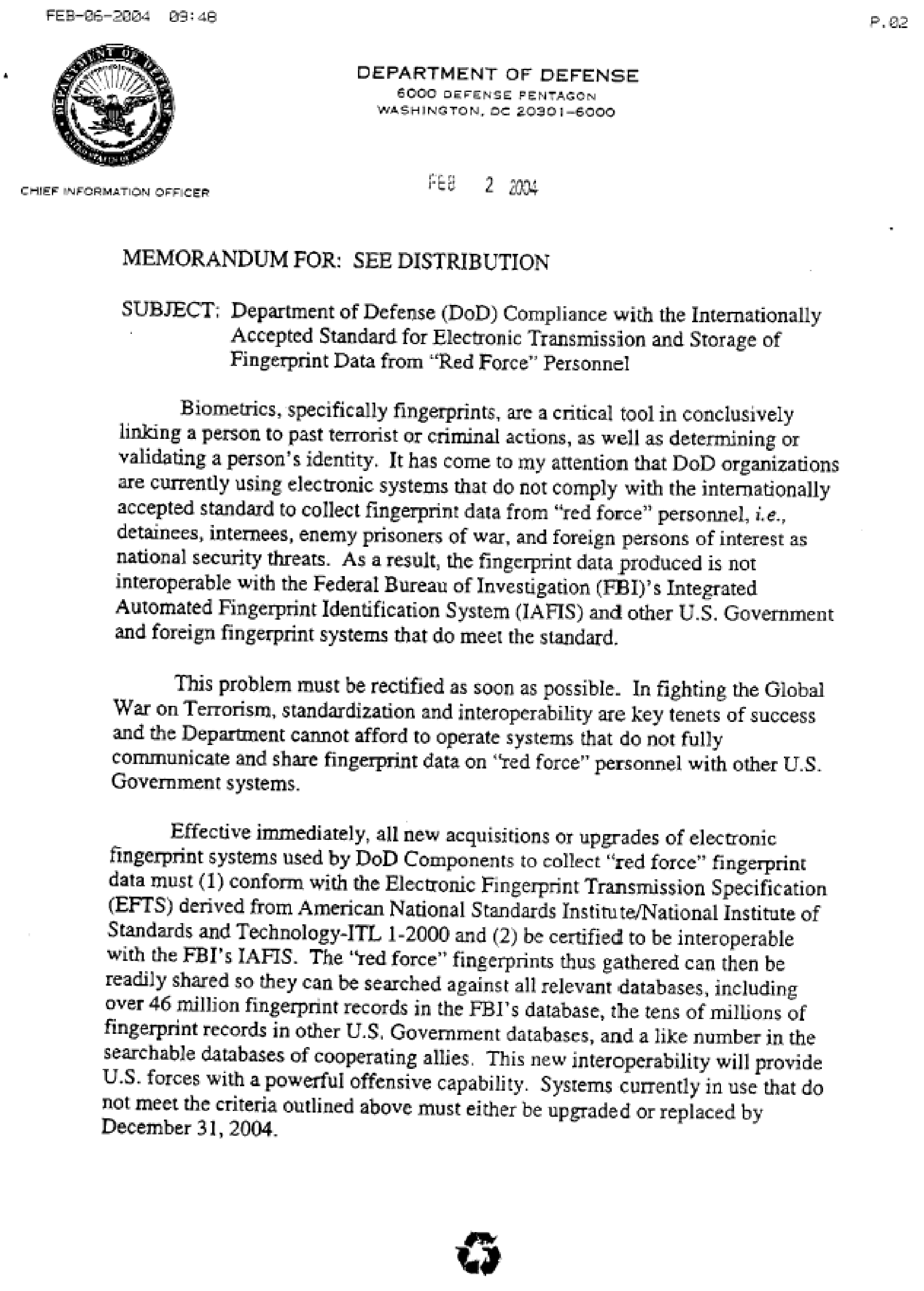
SC37. SC37 is the principal international standards body for biometrics**.** SC37 is a subcommittee of ISO/IEC Joint Technical Committee 1 (JTC1).

Target of Evaluation. An information technology product or system and its associated administrator and user guidance documentation that is the subject of a Common Criteria evaluation.

Template. A concise representation of the biometric measurement of an enrollee (human subject) in a biometric system.

APPENDIX D: ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION RED FORCE POLICY MEMORANDUM

In a 2 February 2004 memorandum, the Office of the Assistant Secretary of Defense for Networks and Information Integration directed that all DoD organizations must collect “Red Force” fingerprint data in a manner that complies with the ANSI/NIST ITL 1-2000 standard described in Section 3.1. The 2 February memorandum details requirements for the collection of fingerprint data from Red Force personnel only. Red Force personnel are defined as detainees, internees, enemy prisoners of war, and foreign persons of interest as national security threats. This memorandum is shown below.



FEB-06-2004 09:48 P.02

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

FEB 2 2004

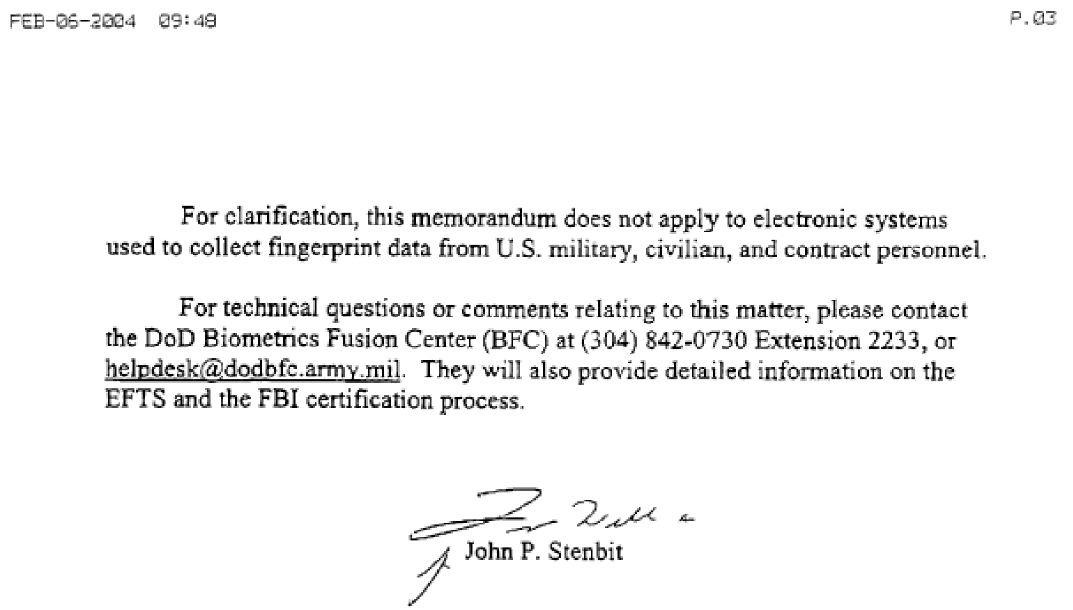
MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Department of Defense (DoD) Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from "Red Force" Personnel

Biometrics, specifically fingerprints, are a critical tool in conclusively linking a person to past terrorist or criminal actions, as well as determining or validating a person's identity. It has come to my attention that DoD organizations are currently using electronic systems that do not comply with the internationally accepted standard to collect fingerprint data from "red force" personnel, *i.e.*, detainees, internees, enemy prisoners of war, and foreign persons of interest as national security threats. As a result, the fingerprint data produced is not interoperable with the Federal Bureau of Investigation (FBI)'s Integrated Automated Fingerprint Identification System (IAFIS) and other U.S. Government and foreign fingerprint systems that do meet the standard.

This problem must be rectified as soon as possible. In fighting the Global War on Terrorism, standardization and interoperability are key tenets of success and the Department cannot afford to operate systems that do not fully communicate and share fingerprint data on "red force" personnel with other U.S. Government systems.

Effective immediately, all new acquisitions or upgrades of electronic fingerprint systems used by DoD Components to collect "red force" fingerprint data must (1) conform with the Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000 and (2) be certified to be interoperable with the FBI's IAFIS. The "red force" fingerprints thus gathered can then be readily shared so they can be searched against all relevant databases, including over 46 million fingerprint records in the FBI's database, the tens of millions of fingerprint records in other U.S. Government databases, and a like number in the searchable databases of cooperating allies. This new interoperability will provide U.S. forces with a powerful offensive capability. Systems currently in use that do not meet the criteria outlined above must either be upgraded or replaced by December 31, 2004.



FEB-06-2004 09:48 P.03

For clarification, this memorandum does not apply to electronic systems used to collect fingerprint data from U.S. military, civilian, and contract personnel.

For technical questions or comments relating to this matter, please contact the DoD Biometrics Fusion Center (BFC) at (304) 842-0730 Extension 2233, or helpdesk@dodbfc.army.mil. They will also provide detailed information on the EFTS and the FBI certification process.

John P. Stenbit

APPENDIX E: REFERENCES

AAMVA DL/ID-2000, AAMVA National Standard for the Driver License/Identification Card, 30 June 2000

AF-CIO Policy Memorandum 03-11, Extensible Markup Language Usage

ANSI/INCITS 358-2002, Information Technology: BioAPI Specification, 16 March 2001

ANSI/NIST-ITL 1-2000, Standard Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, 27 July 2000

ANSI/X9 X9.84-2001, Biometric Information Management and Security, 27 March 2001

BioAPI Consortium Website, http://www.bioapi.org

Biometrics Consortium Website, http://www.biometrics.org

CJIS-RS-0010 (V7), Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification, January 1999

Department of Defense, Department of Defense Joint Technical Architecture, version 4.0, 4 April 2003

DoD Biometrics Management Office, BMO Standards Vocabulary, version 2.2, 21 April 2003

OSD Memorandum, Policy for Registration of Extensible Markup Language (XML), 22 April 2002

OSD Memorandum, DoD Net-Centric Data Management Strategy: Metadata Registration, 3 April 2003

IBM Research Report RC22481, Biometrics 101, R. Bolle et al. 10 June 2002

ISO/IEC CD2 7816-11, Information technology—Identification cards: Integrated circuit(s) cards with contacts—Part 11: Personal verification through biometric methods, ISO/IEC JTC 1/SC 17/WG 4, 27 September 2001

M1 document register, http://www.incits.org/tc_home/m1htm/docs/m1docreg.htm

M1 Website, http://www.incits.org/tc_home/m1.htm

Mansfield, A.J., and J. L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, version 2.01, August 2002

National Technology Transfer and Advancement Act of 1995, 7 March 1996

NIST Government Smart Card Website, http://smartcard.nist.gov/

NISTIR 6529-2001, Common Biometric Exchange File Format, 3 January 2001

NISTIR 6887-2003, Government Smart Card (GSC) Interoperability Specification Version 2.1, 16 July 2003

NSTISSP No. 11, National Information Assurance Acquisition Policy, National Security Telecommunications and Information Systems Security Committee, 2003

TB1—Bionorm: Need for Specifications and Standardization to Achieve Interoperability in the Field of Smart Cards and Biometrics, Fraunhofer Institute for Secure Telecooperation, 23 October 2002

Team Command, Control, Communications, Computer, Intelligence, Electronic Warfare and Sensors (C4IEWS) Master Action Plan (MAP), Program Executive Office of Intelligence, Electronics Warfare and Sensors (IEW&S), 8 April 1999

United States General Accounting Office, GAO-03-174, Technology Assessment: Using Biometrics for Border Security, 14 November 2002.

X.509 Certificate Policy for the U.S. DoD, 18 December 2002, Version 7.0.

XML Common Biometric Format Committee Specification, 25 March 2003, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf