RAND ARROYO CENTER

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Arroyo Center

View document details

This product is part of the RAND Corporation reprint series. RAND reprints reproduce previously published journal articles and book chapters with the permission of the publisher. RAND reprints have been formally reviewed in accordance with the publisher's editorial policy.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2004**	2. REPORT TYPE	3. DATES COVERED **00-04-2004 to 00-06-2004**
4. TITLE AND SUBTITLE **DoD's Collaborative Approach to Developing Biometrics Standards**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **U.S. Government or Federal Rights License**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

DoD's Collaborative Approach to Developing Biometrics Standards

By John Woodward Jr.

Introduction

DoD has a growing need to control access to its many assets both in times of war and in times of peace. Similarly, DoD organizations must always be ready to identify "friend or foe." This requirement is heightened in the global war on terrorism, where the enemy has demonstrated its ability to use sophisticated methods to exploit flaws in current identity management systems. The terrorist attacks of September 11, 2001, reinforced the need for technologies that can enhance homeland security, force protection, and counterterrorism measures.

Biometric technologies may seem exotic, but their use is becoming increasingly common. In 2001, *MIT Technology Review* named biometrics as one of the "top ten emerging technologies that will change the world." DoD recognizes the fast-paced developments in biometric technology, and the great need for interoperability in DoD systems. Accordingly, DoD, through its Biometrics Management Office (BMO), has developed a collaborative approach for the development of DoD biometrics standards. This approach will enable DoD to guide biometrics standards development to ensure that the standards promote biometric technology's interoperability and support for the joint warfighter.

Compared with other, more established types of information technology, the commercial biometrics industry is still relatively new and evolving. The biometric industry has achieved successes in the growth of its capabilities, but from DoD's perspective, industry's efforts have sometimes resulted in competing, redundant, or proprietary-based capabilities.

In recent years, biometric technology has matured and become more viable for DoD uses. DoD endeavors to promote the efficiency of biometric technology development through the use of biometrics standards to prevent DoD from building stovepipes, to discourage developers from continually "reinventing the wheel," and to encourage DoD organizations to use biometric technologies that contribute to joint warfighter capabilities.

Coordinating Biometric Activities within DoD and Other Federal Agencies

On August 25, 2003, Deputy Secretary of Defense Paul Wolfowitz promulgated his "Department of Defense (DoD) Biometrics Enterprise Vision," which states that, "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 BMO to "ensure that a scalable biometrics component of the Global Information Grid (GIG) infrastructure is in place, and that the appropriate standards, interoperability tools, testing frameworks, and approved product validations are available to assist the DoD community in using this technology."

As part of its directive and in keeping with the guidance from the Secretary of the Army (DoD's Executive Agent for biometric technologies), via the Army Chief Information Officer (CIO), who has oversight responsibility, the BMO established the BMO Standards Working Group to coordinate biometrics standards activities within DoD. The BMO Standards Working Group membership includes the Defense Information Systems Agency, National Security Agency, U.S. Air Force, U.S. Navy, U.S. Army, Biometrics Fusion Center (BMO's technical arm), National Institute of Standards and Technology (NIST), and others.

One of the BMO Standards Working Group's major efforts in 2003–2004 has been the development of *DoD Biometrics Standards Development Recommended Approach*. This document details a recommended approach to the identification of, participation in, and development of biometrics standards. Various DoD and other federal agencies and oversight bodies are reviewing this document. If approved, the document will be the first concrete step toward coordinating the development of biometrics standards with other federal agencies.

Participating in National and International Standards Organizations

The National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) requires federal agencies to adopt commercial standards, particularly those developed by standards developing organizations, wherever possible, in lieu of creating proprietary, nonconsensus standards. Through active participation in national and international standards organizations, the DoD BMO exerts its influence to facilitate and promote DoD interests in the biometrics arena. As a result, the standards developed through these national and international organizations will better reflect and support the interests of DoD biometrics-related activities.

In the United States, the primary body responsible for developing national biometrics standards is the M1 biometrics standards committee of the International Committee for Information Technology Standards (INCITS). INCITS is the recognized standards development organization for information technology within the United States and operates under the rules of the American National Standards Institute (ANSI). It does not restrict membership and attracts participants in its technical work from 13 countries. Mr. Fernando Podio of NIST, an advisor to the BMO director and a member of the BMO Standards Working Group, chairs the INCITS M1 committee. The M1 committee, established in November 2001, is one of several standards committees that develop U.S. national commercial standards related to information technology.

Two other INCITS committees, B10 and T4, also are involved in biometrics-related issues. The B10 committee covers identification cards and related devices (for example, 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.

ANSI is the official representative to the International Organization for Standardization (ISO), the world's leading standards body. Under ISO, the counterpart biomet-

rics standards body to M1 at the international level is SC 37 of the ISO/International Electrotechnical Commission Joint Technical Committee 1 (JTC 1). Mr. Fernando Podio of NIST also chairs JTC 1 SC 37, which is the committee responsible for the development of international biometrics standards. INCITS M1 represents the United States in JTC 1 SC 37.

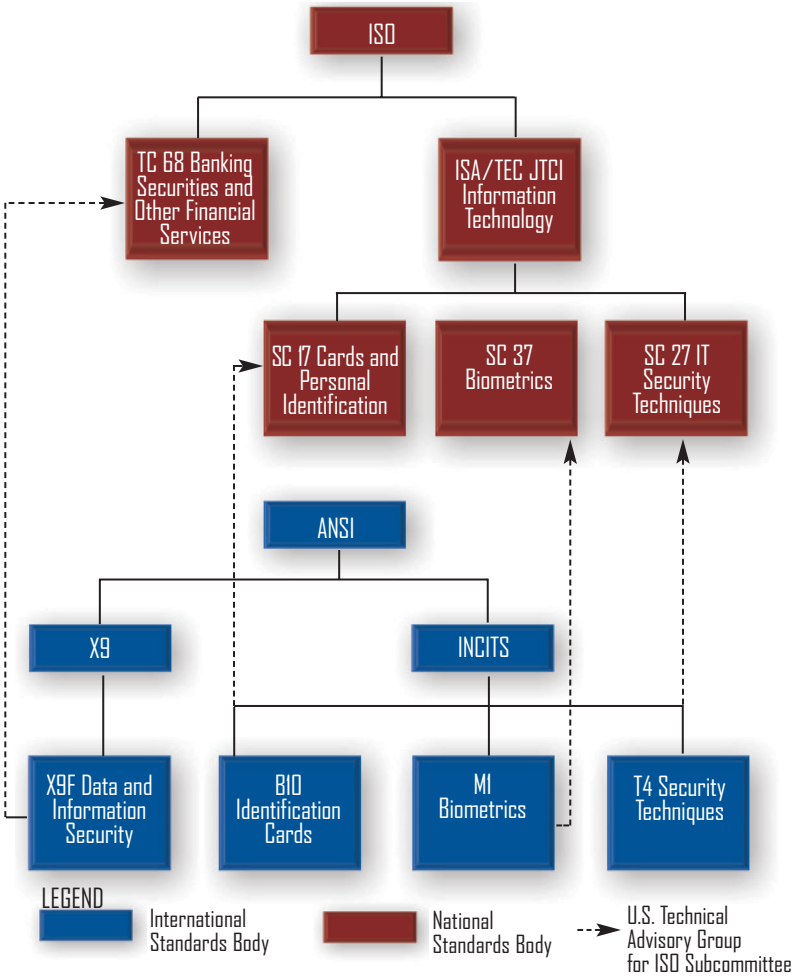
During a recent BMO Standards Working Group meeting, Mr. Podio stated that "the BMO's collaborative approach in the development of national and international biometrics standards is an example to imitate. Taking a proactive role in the development of these standards and seeking coordination with other government agencies and the industry will support DoD's decision of adopting open-system-based biometric technology solutions." Mr. Podio also said that "standards-based enterprise systems and applications are more likely to be interoperable, scalable, usable, reliable, secure, as well as more economical to the user than proprietary systems."

DoD's coordination with the NIST program in accelerating the development of national and international biometrics standards, DoD's related conformity assessment and interoperability efforts, and other U.S. government initiatives will support DoD's goals to provide high-performance, interoperable, and scalable biometrics solutions to the DoD community.

Figure 1 shows the relationship between the U.S. standards bodies working on biometric technology and their international counterparts. Currently, the BMO actively participates in INCITS M1, T4, B10, X9, and JTC 1 SC 37 (through INCITS M1) on behalf of DoD interests. Recent contributions to INCITS M1 include

- providing the coeditor for a project that is developing a conformance testing methodology for a Biometrics Application Programming Interface (BioAPI) specification within SC 37 and
- providing key technical contributions to this and other projects in SC 37's program of work (e.g., data formats and biometric performance testing).

FIGURE 1. U.S. National Standards Bodies for Biometrics and Their International Counterparts



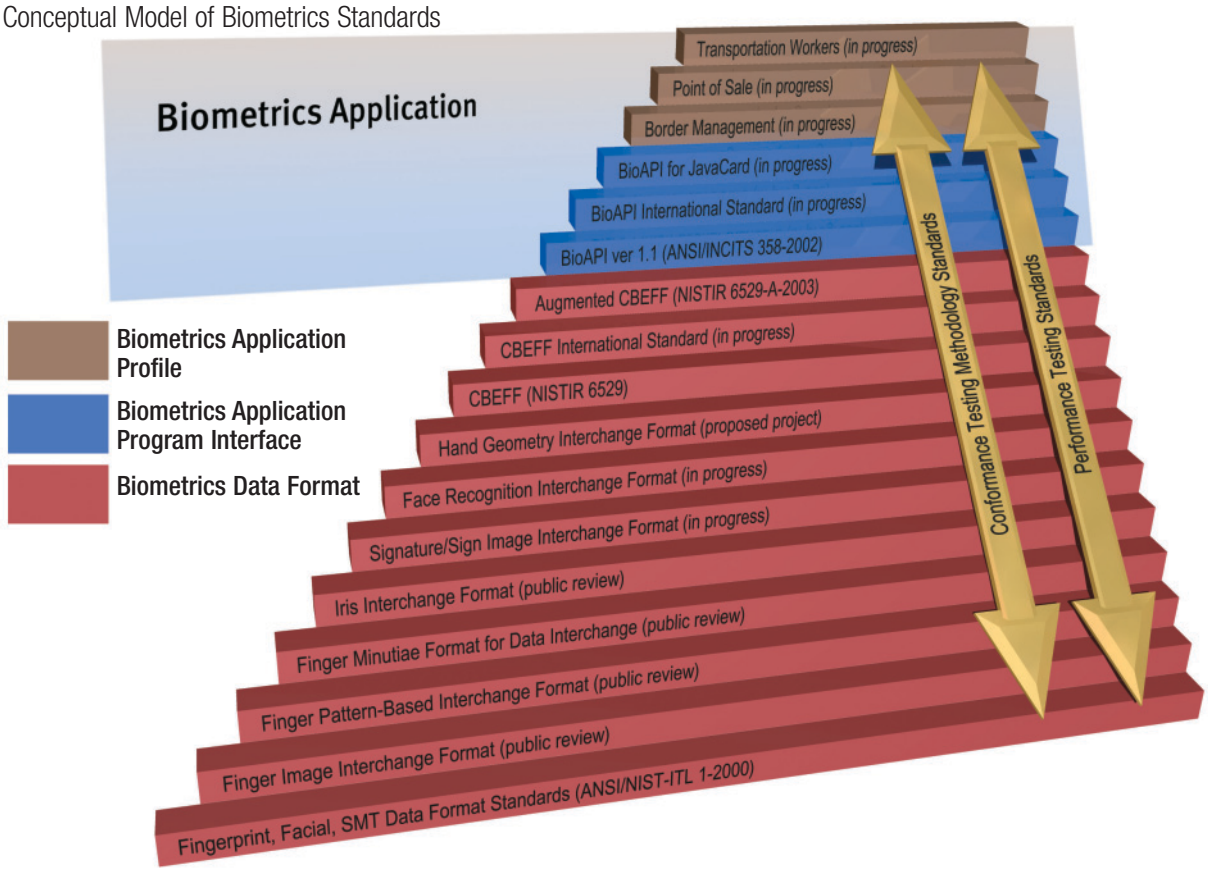
Within INCITS M1, the BMO is also developing a standard: "DoD Application Profile—Standards Guidance for DoD Implementation of Biometrics." This standard's development will include capturing DoD best practices for biometrics and facilitating an increase of interoperability and data interchange in DoD deployments of biometrics.

Status of Biometrics Standards Development

The BMO has developed a conceptual model to categorize the types of standards needed to promote biometric technology's interoperability and support for the joint warfighter and to clarify what biometrics standards exist and what standards are under development or planned. The model categorizes the standards as follows:

- Biometrics data format standards
  - Image standards

FIGURE 2. Conceptual Model of Biometrics Standards



- ▲ Template standards
- ▲ File format standards
- ▮ Interface standards
- ▮ Application profile standards
- ▮ Performance testing standards
- ▮ Conformance testing methodology standards.

Figure 2 depicts the model and indicates the status of the standards.

In summary, a significant amount of work on developing biometrics standards is well under way. The BMO must encourage and facilitate interoperability. With this goal in mind, *DoD Biometrics Standards Development Recommended Approach* represents a solid starting point for DoD's comprehensive, coordinated approach to DoD use of biometrics. Going forward, the BMO hopes that this approach will serve as a framework for biometrics standards in DoD and receive consideration from other U.S. federal agencies in their implementation of biometric technology. Ideally, U.S. government agencies should work together for a collaborative U.S. government strategic approach, leveraging the resources of participating agencies in the spirit of cooperation. This cooperation not only will advance the development of the necessary standards, but will accelerate the establishment of an environment of interoperability.

About the Author

John Woodward Jr. is the director of the DoD Biometrics Management Office. The BMO leads, consolidates, and coordinates the development and adoption of biometric technologies within DoD; it also tests and evaluates biometric technologies at its Biometrics Fusion Center. Mr. Woodward has testified about biometrics before Congress, the Commission on Online Child Protection, and the Virginia State Crime Commission. His numerous publications on the subject include *Biometrics: Identity Assurance in the Information Age* (McGraw-Hill, 2003).

Acknowledgment: The author thanks Mr. Donald Waymire and Dr. Ramy Guirguis, contractors supporting the BMO, for their invaluable assistance in drafting this article. The members of the BMO Standards Working Group also deserve praise for their dedicated efforts. The author also thanks Mr. Fernando Podio of NIST for his contribution to this article and for his continued support to the BMO Standards Working Group.

About DoD Biometrics

In wartime, DoD's dependence on information as a tactical and strategic asset requires DoD to carefully control its networks and information systems. From logistics flows to intelligence on enemy forces, DoD depends on confining access to its data to authorized personnel. This need for access control is also critical at the special operations and weapon system level, where, for example, a U.S. military operative deep in enemy territory must quickly and securely communicate actionable intelligence back to other units.

Access control issues are important to the peacetime DoD because improving the efficiency of operations, including controlling access to installations, facilities, computer systems, and networks, depends on fast and accurate identification. DoD also operates a vast set of human resource services involving health care, retiree and dependent benefits, and troop support services. These services create the need for identity assurance to prevent fraud and abuse.

Congress, the White House, and DoD leadership recognize that biometrics, or automatic recognition of a person using distinguishing traits, can be an enabling technology to provide better security through identity assurance.

Biometric systems take identity assurance beyond the basic "something you have" (e.g., a token badge) and "something you know" (e.g., user name and password), to "something you are"—a biometric. Biometric-based identity assurance systems rely on physical or behavioral characteristics—such as fingerprints, hand geometry, iris patterns, or signature verification—that are distinctive to individuals and can be measured to ensure that a person's identity is accurately determined.

The association between an individual and a "trusted identity" is the foundation for identity management. A trusted identity is something that proves beyond a doubt that you are who you say you are (your identity has been "vetted") and that another person cannot "assume" your identity or masquerade as you (your identity has been "fixed"). Identity management is the process that creates and maintains the use of trusted identity.

With the vetting and fixing of a trusted identity, identity management can be further associated with a set of assigned permissions and access rights. Before the information age, DoD faced its greatest identity challenge in the area of physical access control. However, the exponential growth and use of information technology throughout DoD has dramatically increased the security challenge for logical access control, of which trusted identity is essential.

No one is more aware of this challenge than Army CIO LTG Steven Boutelle, who has oversight responsibility for DoD biometrics. Borrowing from the Army slogan, LTG Boutelle seeks to make biometrics "ready and relevant" for DoD. He emphasized his guidance in his presentation to the September 2003 Biometric Consortium Conference: "Introducing biometric technologies into the DoD is not enough—they must be part of an integrated, interoperable, DoD-wide enterprise solution, in coordination with other U.S. Government initiatives."

At the same conference, LTG Boutelle also made clear his view that standards development work should be one of the BMO's highest priorities. Without comprehensive standards in place, DoD runs the risk of creating insular, fragmented, and expensive biometric "fiefdoms" that will not be able to share data or communicate with one another. Such an approach is bad for DoD and a detriment to national security.