NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards

NSTC Subcommittee on Biometrics and Identity Management

September 7, 2007

About the National Science and Technology Council[1]

Authority for this policy is derived from Executive Order 12881[2], which establishes the National Science and Technology Council (NSTC) and its authority to ensure that science and technology policy decisions and programs are consistent with Presidential goals, National Security Presidential Directives and Homeland Security Presidential Directives. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the federal research and development enterprise. Chaired by the President, the NSTC is made up of the Vice President, the Director of the Office of Science & Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals.

About the NSTC Subcommittee on Biometrics and Identity Management[3]

The Subcommittee serves as part of the internal deliberative process of the NSTC. Reporting to and directed by the NSTC Committee on Technology, the Subcommittee is chartered to:

- Develop and implement multi-agency investment strategies that advance biometric sciences to meet public and private needs;

- Coordinate biometrics-related activities that are of interagency importance;

- Facilitate the inclusions of privacy-protecting principles in biometric system design;

- Ensure consistent message about biometrics and government initiatives when agencies interact with Congress, the press and the public;

- Strengthen international and public sector partnerships to foster the advancement of biometric technologies.

[1] http://www.ostp.gov/nstc
[2] http://www.ostp.gov/nstc/html/_executiveorder.html
[3] http://www.biometrics.gov/nstc/Default.aspx

1 FOREWORD

In the United States, responsibility for setting product and process standards rests almost exclusively (and appropriately) with the private sector. Government agencies rely heavily on voluntary standards, which they often incorporate into regulatory and procurement requirements. Related conformity assessment processes are often developed to ensure that products, processes, or systems comply with regulations or voluntary standards. These processes include tests of components, certification of test results, and accreditation methods that assess the competence of testing laboratories.

In recent years, standards developing organizations have developed numerous biometric consensus standards that will aid the U.S. Government (USG) and the private sector as they develop systems, methods and tools to achieve real-time, verifiable, interoperable, and privacy-protecting root identification. The success of Federal biometric applications is particularly dependent on the interoperability of biometric systems. Agencies use biometrics for applications ranging from terrorist identification to benefits management, and the data they screen against has often been collected and managed by numerous other agencies. Standards for USG-wide biometric data sharing are therefore required to provide integrated, accurate and timely information to agency screening systems.

The NSTC Subcommittee on Biometrics and Identity Management (Subcommittee) has established an interoperability working group to assess options and develop plans to support appropriate biometric data sharing within the USG. In the case of Known and Suspected Terrorists (KST), an approach is being designed that will better support existing biometric data sharing policies and screening activities across USG agencies. The capability to share KST biometric information will be inherently dependent on the availability, and government-wide adoption, of numerous biometric standards and conformity assessment processes.

This *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* complements and builds upon existing efforts by tasking the Subcommittee's standards and conformity assessment working group to develop interagency consensus on standards-related items required to enable the interoperability of various Federal biometric applications, and to guide federal agencies as they develop and implement related biometric programs. This Policy was developed through a collaborative, interagency, process within the Subcommittee and approved by the NSTC Committee on Technology.

---

[4] Biometrics, as defined in the Subcommittee's Glossary (http://www.biometrics.gov/docs/glossary.pdf), is a general term used alternatively to describe a characteristic or a process.
- As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.
Terms used throughout this document agree with the Glossary definitions.

2 Policy Goal

The goal of this Policy is to establish a framework to reach interagency consensus on biometric standards adoption for the Federal government. Federal agency adoption of these recommended standards, and associated conformity assessment programs, will enable necessary next generation Federal biometric systems, facilitate biometric system interoperability, and enhance the effectiveness of biometrics products and processes.

3 Background Information

In 2006, the National Science & Technology Council's Subcommittee on Biometrics and Identity Management (Subcommittee) released *The National Biometrics Challenge*[5], which describes the major challenges the biometrics community must overcome to meet the needs of the Nation and the broader worldwide biometrics community. *The National Biometrics Challenge* identifies biometric systems interoperability as one of four pre-eminent challenges for the biometrics community[6], and identifies the following standards-based role for the Federal government: "Participate in biometrics open standards development, standards adoption, conformance test tool development, conformity assessment system development, and harmonization of biometrics, security and authentication standards."
Rapid, reliable and accurate biometric-based recognition of individuals is necessary for successful homeland security, counterterrorism, border control, law enforcement, e-commerce and e-government, and identity theft prevention. To address this need, the Subcommittee is developing plans for future biometric data sharing, as appropriate, that will enable real-time, verifiable, interoperable, and privacy-protecting root identification that meets specific agency mission objectives and Federal biometric system interoperability requirements approved by the National Security Council's Deputies Committee. In order to support such Federal biometric applications, robust standards and conformity assessment processes are required. Accordingly, in this document the Subcommittee has set forth a framework to provide the technical foundation for the Federal government to develop interagency consensus on biometric standards and to guide their adoption within agency biometric systems.

Federal policies on the use and development of voluntary consensus standards and on conformity assessment activities are outlined in OMB Circular A-119[7]. This circular also provides guidance for agencies participating in voluntary consensus standards bodies.

---

[5] http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf
[6] The four preeminent challenges identified within *The National Biometrics Challenge* are Biometric Sensors, Biometric Systems, Biometric Systems Interoperability, and Biometrics Communications and Privacy
[7] http://www.whitehouse.gov/omb/circulars/a119/a119.html. This Circular is codified within the "National Technology Transfer and Advancement Act of 1995" (Pub. L. 104-113)

4 Principles and Key Actions

To enable biometric system interoperability and support Federal agency biometrics needs, the USG should be guided by the following principles:

- ***Continued development of voluntary consensus standards for biometrics is vital to the security of our Nation and the stability of the US-based biometrics community.[8]*** Agencies should support national and international voluntary biometric standards development activities.

- ***Rigorous testing is required to ensure vendor and system compliance with biometric standards.*** Agencies should support the development of harmonized conformance, interoperability, performance, security, human factors, and operational scenario testing programs in support of procurement actions for biometric products, programs and services.

- ***Standards and conformity assessment processes must be identified and adopted across all agencies to ensure full interoperability.*** Agencies should participate in an interagency process led by the Subcommittee to review available standards and develop consensus recommendations regarding which standards should be adopted across the USG.

- ***The biometric standards and conformity assessment processes recommended by the Subcommittee should be promulgated.*** The Subcommittee shall develop a registry of adopted biometric standards at www.standards.gov/biometrics[9].

- ***The biometric standards and conformity assessment processes recommended by the Subcommittee should be integrated into agency plans whenever feasible.*** Agencies should strive to build and operate biometric systems that are based on the Subcommittee's recommended standards.

- ***Timely adoption and use of appropriate standards is critical to achieving biometrics goals.*** Following selection of recommended standards, the Subcommittee should work to advance adoption of standards for use in Federal biometrics programs and services.

---

[8] This is a unique co-reliant relationship: the biometrics community is reliant upon USG initiatives because of the government's role as the industry's primary customer; the USG is reliant on the biometrics community to provide tools that enable screening functions for numerous government functions.

[9] This information will also be made available on the Federal government's web site for biometric activities at www.biometrics.gov/standards.

5 IMPLEMENTATION TASKS

The following table presents initial and ongoing tasks necessary for the implementation of this policy. The Subcommittee is directed to further develop these tasks into a comprehensive interagency action plan.

Implementation Task	Action
USG Participation in Biometric Standards Development	USG agencies should continue to provide administrative and technical leadership for national and international biometric standards development, and should coordinate USG positions and contributions to these standards developers through the Subcommittee. Based upon each agency's mission, USG agencies should participate in relevant biometrics and related standards developing organizations (SDO), such as: • FBI Criminal Justice Information Services (CJIS) Advisory Policy Board • National Institute of Standards and Technology Information Technology Laboratory (NIST/ITL)[10] • International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Joint Technical Committee 1- Subcommittee 37 (JTC 1 SC 37) • InterNational Committee for Information Technology Standards -Technical Committee M1 (INCITS M1)[10] • International Civil Aviation Organization (ICAO) Technical Advisory Group (TAG) New Technologies Working Group (NTWG)
Backwards Compatibility of Standards	While participating in SDO activities, the USG should promote the concept that voluntary consensus standards be backward compatible to the maximum extent possible to ensure interoperability of new systems with legacy data, or new data with legacy systems.
Interagency Analysis and Determination of Recommended Standards for USG Adoption	The NSTC Subcommittee on Biometrics and Identity Management should establish definitions for emerging, mature, and stable biometric standards. Based upon these model criteria, the Subcommittee should review available standards and collectively determine and promulgate which standards should be recommended for adoption throughout the USG.

---

[10] Accredited by the American National Standards Institute (ANSI)

Consistent Application of Biometric Standards in Agency Plans	The NSTC Subcommittee on Biometrics and Identity Management should assist agencies as they develop biometric system plans to ensure that recommended standards and associated testing are used to the maximum extent practicable. Agencies should develop internal procedures to ensure citation of relevant standards from the registry of USG recommended biometric standards in biometric procurement actions.
Exchange of Proprietary Data	Agencies should use the proprietary data fields in standardized data formats from the registry of USG recommended biometric standards for the exchange of proprietary data. Agencies with closed systems that do not require system or interagency interoperability should only use proprietary data formats if standardized data formats can be documented to be inadequate.
Lifecycle Handling of Biometric Samples	The NSTC Subcommittee on Biometrics and Identity Management should develop a set of guidelines to ensure the quality and usability of biometric samples. This guidance should highlight the importance of obtaining raw biometric samples upon collection (using biometric standards on the registry of USG recommended biometric standards when possible) and deprecate the collection of biometric templates only.
Consistent Collection and Use of Metadata	The NSTC Subcommittee on Biometrics and Identity Management should support agencies as they develop agency-specific guidelines for the collection, maintenance, and use of metadata for USG biometric applications.

6 ROLES AND RESPONSIBILITIES

This policy requires multiple interagency actions as well as departmental actions to ensure successful implementation. The NSTC Subcommittee on Biometrics and Identity Management is the responsible party for developing interagency consensus and facilitating agency adoption in support of this policy. By participating actively in the Subcommittee, agencies are ensured that their requirements will be considered in the interagency review and determination of which standards should be adopted.

The NSTC Subcommittee on Biometrics and Identity Management is the responsible party for the:

- Coordination of USG activities in national and international voluntary biometric standards development;

- Establishment of model criteria for the adoption and maintenance of biometric standards;

- Interagency analysis, determination and promulgation of recommended standards for USG adoption;

- Facilitation of access to adopted standards by USG personnel; and

- Identification of research, development, test and evaluation needs that are required to enable this Policy, and prioritization of those needs in the Subcommittee's ongoing RDT&E agenda development.

The roles and responsibilities of agencies with biometric programs are to:

- Support the Subcommittee's designated responsibilities by ensuring appropriate agency personnel and resources are provided;

- Ensure the use of appropriate biometric standards from the registry of USG recommended biometric standards internally and in awarded projects, unless the standards can be documented to be operationally inadequate or are fiscally untenable for the anticipated benefits;

- Identify agency-specific requirements on the use of biometric standards (capture, use, dissemination, and disposition of biometric data) consistent with *The National Biometrics Challenge*; and

- Ensure compliance, where applicable, with the requirements of the Privacy Act of 1974 and the E-Government Act of 2002[11] when using standards-based biometric image or template data, as it is considered to be personally identifiable information.

[11] as well as other applicable privacy-related laws and agency policies

7 Membership of the NSTC Subcommittee on Biometrics and Identity Management

Subcommittee on Biometrics and Identity Management

Co-chair: Duane Blackburn (Executive Office of the President)
Co-chair: Jim Dray (Commerce)
Co-chair: Brad Wing (Homeland Security)

Department Leads

Martin Herman (Commerce)
Thomas Dee (Defense)
Thomas Coty (Homeland Security)
James Loudermilk (Justice)
John Atkins (State)
Bill Baron (Transportation)
Zaida Candelario (Treasury)
Sankar Basu (National Science Foundation)
Usha Karne (Social Security Administration)
David Temoshok (General Services Administration)
Michael Wash (Government Printing Office)
Duane Blackburn (Executive Office of the President)

Standards and Conformity Assessment working group
    Co-chair: Mike Hogan (Commerce, National Institute of Standards & Technology)
    Co-chair: Brad Wing (Homeland Security, US-VISIT)

Department of Commerce
Gordon Gillerman (National Institute of Standards & Technology)
Patrick Grother (National Institute of Standards & Technology)
Fernando Podio (National Institute of Standards & Technology)

Department of Defense
Sam Aloi (Army Biometrics Fusion Center)
Thomas Dee (Defense Research and Engineering)
Avram Isaacson (Army Biometrics Task Force)
Dave Lohman (Army Biometrics Fusion Center)
Thomas McKenna (Office of Naval Research)

Department of Energy
Carl Pocratsky (Office of Security and Safety Performance Assurance)

Department of Homeland Security
Thomas Coty (Science & Technology Directorate)
Bert Coursey (Science & Technology Directorate)
Trent DePersia (Science & Technology Directorate)
Joe Kielman (Science & Technology Directorate)
Joyce Nyman (US Coast Guard)
James Pattan (Customs and Border Protection)
Chris Miles (Science & Technology Directorate)
Peter Sand (Privacy Office)
Kimberly Weissman (US-VISIT)
Steve Yonkers (US-VISIT)

Department of Justice
Janice Bland (Federal Bureau of Investigation)
Stanley Erickson (National Institute of Justice)
Thomas Hopper (Federal Bureau of Investigation)
Stan Larmee (Terrorist Screening Center)
James Loudermilk (Federal Bureau of Investigation)
John Manzo (Federal Bureau of Investigation)
Todd Mullenax (Federal Bureau of Investigation)
Scott Swann (Federal Bureau of Investigation)

Department of State
John Atkins (Consular Affairs)
Sarah Francia (Consular Affairs)

Department of Transportation
Bill Baron (Research and Innovative Technology Administration)
Susan Sexton (Federal Aviation Administration)

Intelligence Community
Bob Calandra (National Counterterrorism Center)
Jeff Dunn (National Security Agency)
Neal Pollard (National Counterterrorism Center)
Gerald Thames (National Counterterrorism Center)

Executive Office of the President
Duane Blackburn (Office of Science and Technology Policy)

[12] Federally Funded Research and Development Center

www.biometrics.gov