

2003 Biometric Consortium, Sept. 24, 2003, Arlington, Virginia

BIOMETRICS
DEPARTMENT OF DEFENSE

Department of Defense Biometrics Management Office Privacy Approach

Department of Defense
Biometrics Management Office
<http://www.dod.mil/nii/biometrics>

DEPARTMENT OF DEFENSE



POSITIVE IDENTIFICATION



Mike Wendling, Policy Team
DoD BMO / Booz Allen Hamilton

Agenda

- **Legislative Historical Perspective**
- **Office of Management and Budget (OMB) Guidance**
- **Department of Defense Guidance**
- **Implications for the Biometrics Management Office (BMO)**
- **Integrated Relationships and Coordination**
- **Past to Future Timeline**
- **Summary/Next Steps**

Historical Privacy Perspective

- **Significant Legislation**
 - **Fourth Amendment**
 - **Privacy Act of 1974**
 - **Computer Security Act of 1987**
 - **Paperwork Reduction Act of 1995**
 - **Patriot Act of 2001**
 - **E-Government Act of 2002**

OMB Guidance

- **OMB Circular A-130 (1996)**
 - Agencies must *“Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented.”*

- **OMB Memo (1996)**
 - Outlines principle for protecting privacy when conducting inter-agency data sharing.

OMB Guidance (cont.)

- **President's Management Agenda (2001)**
 - Emphasizes the importance of privacy protection.

- **OMB Circular A-11 (Sec. 300, rev. July 2003)**
 - Requires the completion of Privacy Impact Assessment (PIA) when major IT investment funds are expended.

- **Final OMB Guidance on Privacy Impact Assessments (PIA) is due in the near future.**

DoD Guidance on Biometric Privacy

- **Defense Privacy Office**
 - **Purpose – Balance the information requirements and needs of the Department against the privacy interests and concerns of the individual.**
 - Responsible for implementation of the DoD Privacy Program.
 - Provides a comprehensive framework regulating how and when the Department collects, maintains, uses or disseminates personal information on individuals.

DoD Guidance Protecting Your Privacy Rights

- **DoD Directive 5400.11, “*DoD Privacy Program*”**
 - Updates policies and responsibilities of the DoD Privacy Program.
 - Authorizes the Defense Privacy Board, the Defense Privacy Board Legal Committee and the Defense Data Integrity Board.

- **DoD Directive 8910.1, “*Management and Control of Information Requirements*”**
 - Collection of personal information is subject to guidelines established in Privacy Act; must be deemed necessary to support the role of agency.

- **DoD CIO Memo 28 Dec 2001**
 - Removal of personal information from publicly accessible web sites.

DoD Guidance Authorizing the Collection of Biometric Information

- **DoD Directive 8500.1, “*Information Assurance*”**
 - Designates Secretary of the Army as Executive Agent for integration of common biometric technologies throughout DoD.

- **DoD 5200.2-R, “*DoD Personnel Security Program*”**
 - Direction for implementing procedures to provide acceptance and retention of DoD military, civilian, consultant and contractor personnel.
 - Granting such persons access to classified information or assignment to a sensitive position which includes the collection of biometric information.

DoD Guidance Authorizing the Collection of Biometric Information (cont.)

- **Under Secretary of Defense for Personnel and Readiness Memo - JULY 1, 1997**
 - States that the Defense Manpower and Data Center “will need to capture electronically and store ... the right index finger of all eligible individuals in a pay or annuity status.”

- **The National Defense Authorization Act for Fiscal Year 2000, Congress provided that a “Smart Card,” as used by DoD personnel, “may” also employ “biometric information.”**

DoD Guidance Authorizing the Collection of Biometric Information (cont.)

- **Collection of Biometrics from Foreign Nationals is authorized by DoD Directive 5230.20- Visits, Assignments, and Exchanges of Foreign Nationals (8/98)**
- **Collection of Biometrics from Local Nationals is authorized by DoD 1400. 25-M – “Employment of Foreign Nationals” 12/96**
- **Deputy Secretary of Defense Memo, “*Department of Defense (DoD) Biometrics Enterprise Vision*” August 2003**
 - *“... Biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for logical and physical access control. ... In some instances, providing a biometric may be a condition of employment.”*

DoD Responsibilities for Protecting YOUR Biometric Information

- **DoD must ensure that Biometric information...**
 - **Is treated with the same sensitivity level as other personal information.**
 - **Is classified as a “record” under the Privacy Act of 1974.**
 - **Must be safeguarded with the appropriate security controls to protect confidentiality, integrity and non-repudiation of biometric data.**

DoD Responsibilities for Protecting YOUR Biometric Information (cont.)

- **DoD agencies must follow legislative and OMB guidance to ensure security controls are in place to protect biometric information.**
- **DoD agencies must establish the policies and procedures on the collection and use of biometric information.**
- **Security and information technology personnel must work together to ensure compliance with the policies that are established.**

DoD Responsibilities for Protecting YOUR Biometric Information (cont.)

- **Personnel who collect, access, or disseminate biometric data must be trained on the use of biometric technologies and privacy protection.**
- **The E-Government Act of 2002, requires Federal agencies to develop PIAs for all new information systems that collect personal information and outlines the privacy considerations and characteristics of the proposed enterprise architecture.**

Implications for the BMO

- **BMO must develop policies and procedures to comply with current laws and OMB guidance regarding biometrics privacy.**
- **BMO must educate DoD employees to ensure they know and understand their privacy rights.**
- **BMO Must provide training for verifying officials and biometrics collection personnel to ensure that they can respond to specific questions from those providing their biometric.**
- **BMO must securely store biometric information on individuals.**

Integrated Relationships and Coordination

- **National Science and Technology Council Biometrics R&D Interagency Group.**
- **American National Standards Institute M-1 Committee on Biometrics established an ad-hoc Committee on Trans-jurisdictional and Societal Issues which includes privacy protection.**
- **DMDC reviewing Privacy Protection Profile requirements.**

Biometrics Privacy Timeline

- **May 2003** BMO Director approved Privacy Plan
- **May 2003** Developed privacy requirements for Draft Biometrics DoDI and DoDD
- **June 2003** Begun Development of PIA
- **July 2003** Begun development of a Biometrics Privacy Education and Training Tool
- **Sept 15, 2003** Submitted Rights & Responsibilities Educational Brief on Biometrics Privacy
- **Sept 30, 2003** Submit Draft PIA to Director BMO
- **October 2003** Begin development of technical solutions to safeguard employee biometric data
- **Nov 2003** Explore current R&D concepts of biometric privacy

Next Steps

- **Develop a web enabled training course for personnel involved in the issuance process.**
- **Coordinate and cooperate with other Federal Agencies, DoD organizations, State & Local governments and private industry regarding privacy protection issues.**
- **Explore, in conjunction with NIST/other Federal agencies, the development of an information system privacy standard.**
- **Establish technical electronic privacy protection solutions.**

Questions/Comments?