Department of Defense
DIRECTIVE

NUMBER 8521.01E
February 21, 2008

USD (AT&L)

SUBJECT: Department of Defense Biometrics

References: (a) Section 113 of title 10, United States Code
(b) Section 112 of the Emergency Supplemental Act of 2000, Pub. L. No. 106-246, July 13, 2000
(c) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(d) DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004
(e) through (z) see Enclosure 1

1. PURPOSE

Under the authority vested in the Secretary of Defense by Reference (a) and consistent with Reference (b), this Directive:

1.1. Establishes policy, assigns responsibilities, and describes procedures for DoD biometrics.

1.2. Designates the Director, Defense Research & Engineering (DDR&E), under the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), as the Principal Staff Assistant (PSA) responsible for oversight of DoD biometrics programs and policy, to include interagency coordination.

1.3. Designates the Secretary of the Army as the DoD Executive Agent (EA) for DoD biometrics. Supersedes the designation of the Secretary of the Army as the EA for the integration of common biometric technologies throughout the Department of Defense under Reference (c).

1.4. Reinforces responsibilities and authorities assigned under Reference (d) and DoD Directive (DoDD) 5400.11 (Reference (e)) to support the Personnel Identity Protection and Privacy Programs.

1.5. Supersedes Deputy Secretary of Defense Memorandums (References (f) and (g)) and conflicting portions of Reference (c). Additionally supersedes all other DoD issuances and other conflicting guidance regarding DoD biometrics.

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. The development and sustainment of biometric capabilities that support the collection, storage, use, and sharing of biometric data across the Department of Defense and interagency enterprise for purposes of both military operations and business functions.

2.3. This Directive does not apply to the Armed Forces Repository of Specimen Samples for Identification of Remains.

3. DEFINITIONS

Terms used in this Directive are defined in Joint Publication 1-02 and the National Science and Technology Council Subcommittee on Biometrics Glossary (References (h) and (i)), and are listed in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Biometrics is an important enabler that shall be fully integrated into the conduct of DoD activities to support the full range of military operations.

4.2. DoD biometrics programs shall be designed to improve the effectiveness and efficiency of biometrics activities throughout the Department of Defense by eliminating unwarranted duplication and overlap of technology development and information management efforts. For this purpose, all DoD Components' biometrics activities shall be coordinated through the DoD Biometrics Executive Committee (EXCOM).

4.2.1. Joint, Service, or common biometrics products, systems, and services shall be coordinated with the DoD EA for DoD Biometrics and acquired in accordance with procedures consistent with DoDD 5000.1 and DoD Instruction 5000.2 (References (j) and (k)). Consideration shall be given to available Government-wide and DoD enterprise acquisition vehicles and contracts when acquiring biometric products, systems, and services.

4.2.2. Biometrics capabilities determined to be Service-specific, and coordinated with the DoD Biometrics EXCOM, can be acquired through Military Service channels.

4.3. Biometric collection, transmission, storage, caching, tagging, and use shall be controlled through the use of DoD-approved national, international, and other consensus-based standards, protocols, best practices, and equipment to ensure consistency and support interoperability.

4.4. Biometric capabilities shall be developed to be interoperable with other identity management capabilities and systems, both internal and external to the Department of Defense, to maximize effectiveness. System development and capability implementation strategies shall be harmonized, integrated, and unified with identity protection and management stakeholder organizations to ensure consistency with DoD identity management principles, directives, and vision.

4.5. Development and deployment of biometric capabilities and systems shall consider privacy implications and comply with the requirements of Reference (e) and DoD 5240.11-R (Reference (l)), and support the programs outlined in Reference (d) and DoD 5240.1-R, DoDD 5200.27, DoDD 5015.2, and DoD 5200.08-R (References (m), (n), (o), and (p), respectively).

4.6. Biometric data is normally unclassified, in accordance with Reference (m); Homeland Security Presidential Directives (HSPDs) 6 and 11 (References (q) and (r)); and section 534 of title 28, United States Code (Reference (s)). However, elements of the contextual data, information associated with biometric collection, and/or associated intelligence analysis may be classified.

4.7. Authoritative sources of biometric data, associated information, and the means to exchange the data and information with Federal, State, local, tribal, territorial, and foreign governmental or multinational agencies shall be maintained.

4.8. Continuity of operations and disaster recovery plans for all biometrics-related missions and capabilities shall be developed and maintained by the responsible DoD Components.

4.9. The geographic Combatant Commander’s biometric policies relative to installation access take precedence over biometric policies of any DoD Component operating in that command’s area of responsibility (AOR).

4.10. In instances where a primary DoD point of contact with other U.S. Government (USG) agencies and international entities has already been established by existing authorities or statutes, the Biometrics PSA shall be consulted on corresponding activities that impact DoD biometrics.

4.11. DoD biometrics programs shall fully support the Information Sharing Environment (ISE) in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (Reference (t)).

4.12. All biometric data and associated information collected as a result of DoD operations or activities shall be maintained or controlled by the Department of Defense, unless otherwise specified by the DoD EA for DoD Biometrics.

5. RESPONSIBILITIES

5.1. The DDR&E, under the USD(AT&L), shall:

5.1.1. Serve as the PSA for DoD biometrics programs, initiatives, and technologies (hereafter referred to as the Biometrics PSA).

5.1.2. Oversee the activities of the DoD EA for DoD Biometrics.

5.1.2.1. Assess periodically, but at least annually, the assignments and arrangements made by the DoD EA for DoD Biometrics for continued effectiveness in satisfying end-user requirements. Recommend to the Secretary of Defense the establishment, continuation, modification, or cancellation of such assignments and arrangements, as appropriate.

5.1.2.2. Review the adequacy of biometrics funding across the Department of Defense, in support of Joint Requirements Oversight Council-validated requirements, and approved standards and architectures in order to determine whether they meet DoD biometrics program requirements and objectives.

5.1.3. Provide oversight of all biometrics-related strategy, standards, policy, and concept development activities.

5.1.4. Coordinate with all DoD executive level identity management boards and/or committees.

5.1.5. Report annually to the Secretary of Defense on the status of the DoD Biometrics Program.

5.1.6. Serve as Chair of the DoD Biometrics EXCOM with responsibilities as outlined in Enclosure 3.

5.1.7. Serve as the primary DoD point of contact with other USG agencies and international entities on all biometrics-related activities unless otherwise specified in this directive or existing statute.

5.2. The Under Secretary of Defense for Policy (USD(P)) shall:

5.2.1. Support DoD biometrics with overall policy development, implementation, and oversight of biometrics matters, to include international biometrics activities, homeland defense, stability operations, detainee affairs, counterterrorism, critical infrastructure protection, force

protection, anti-terrorism, special operations and low intensity conflict missions, and other areas under the cognizance of the USD(P).

5.2.2. In coordination with the Biometrics PSA, prepare and issue interagency and international cooperation agreements for biometrics activities as appropriate.

5.2.3. Review all proposed biometrics-related USD(P) acquisition programs and budget submissions. Through USD(P) participation in the DoD Biometrics EXCOM, coordinate with the Biometrics PSA on such programs and submissions.

5.3. The Under Secretary of Defense for Intelligence (USD(I)) shall:

5.3.1. Ensure that DoD intelligence, security, and counterintelligence policies and procedures address current biometric capabilities and conform to DoD established standards for their application.

5.3.2. Direct policy development and implementation for the application of biometrics to defense intelligence, counterintelligence, and established security requirements, as needed.

5.3.3. Ensure that biometric-related intelligence information is accessible through an intelligence sharing environment to tactical and operational users as well as the USG-wide intelligence, counterintelligence, foreign intelligence (as appropriate under existing policy and statutes), and security communities.

5.3.4. Serve as the principal advisor to the Biometrics PSA on all biometrics-related intelligence activities.

5.3.5. Provide oversight of the Defense Intelligence Agency (DIA)-led development of a DoD biometrically-enabled watchlist.

5.3.6. Review all proposed biometrics-related intelligence acquisition programs and budget submissions. Through USD(I) participation in the DoD Biometrics EXCOM, coordinate with the Biometrics PSA on such programs and submissions.

5.4. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall:

5.4.1. Ensure personnel, readiness, identity protection, and management policies and procedures address current biometric capabilities and conform to DoD established standards for their application.

5.4.2. Direct policy development and its implementation for the application of biometrics to Defense personnel, readiness, identity protection, and management as well as established security requirements, as needed. Oversee collection of biometrics used for the issuance of identity credentials to DoD personnel in accordance with Reference (d).

5.4.3. Lead the DoD efforts in meeting all requirements for the implementation of HSPD-12 (Reference (u)) in coordination with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/CIO). Provide periodic updates to the DoD Biometrics EXCOM. Retain oversight on the fielding of the personal identity verification credentials and all other biometric issues pertaining to Reference (u) compliance.

5.4.4. Maintain the authoritative source and reference archive for biometric information collected from friendly individuals issued a DoD credential in accordance with References (d) and (e).

5.4.5. In coordination with the Director of Administration and Management (DA&M), ensure compliance with privacy and security policies and procedures to protect personal privacy consistent with law and policy. Additionally collaborate with the DoD EA for DoD Biometrics on the development of non-U.S. person privacy policies.

5.4.6. Review all proposed biometrics-related USD(P&R) acquisition programs and budget submissions. Through USD(P&R) participation in the DoD Biometrics EXCOM, coordinate with the Biometrics PSA on such programs and submissions.

5.4.7. Ensure biometric technologies developed within and for the medical community are coordinated and integrated into the overall DoD biometrics strategy.

5.5. ASD(NII)/CIO shall:

5.5.1. Ensure that biometrics technologies for logical access control are developed, effectively integrated into information assurance efforts, and made available for physical access control and other identity protection and management applications across the Department of Defense, to include DoD contractors.

5.5.2. Ensure that the Global Information Grid supports biometric operational requirements and that biometric solutions operate optimally in a net-centric information environment and adhere to information assurance architectural standards and security requirements.

5.5.3. Provide acquisition oversight, as delegated by the USD(AT&L) in accordance with References (j) and (k), for all biometrics major automated information systems and biometrics acquisition of services initiatives.

5.5.4. Support DoD efforts, in coordination with USD(P&R), for the implementation of Reference (u).

5.5.5. Review all proposed biometrics-related ASD(NII)/CIO acquisition programs and budget submissions. Through ASD(NII)/CIO participation in the DoD Biometrics EXCOM, coordinate with the Biometrics PSA on such programs and submissions.

5.6. The DoD General Counsel shall:

5.6.1. Provide legal advice on all matters related to biometrics and, when appropriate, consult with relevant DoD Component counsels.

5.6.2. Review DoD biometrics acquisition matters and policy decisions.

5.7. DA&M shall:

5.7.1. Ensure that DoD biometrics policies and procedures are consistent with the requirements of References (e) and (l).

5.7.2 Review and address all biometric issues pertaining to the Privacy Act and Freedom of Information Act.

5.8. The Director, DIA, under the authority, direction, and control of USD(I), shall:

5.8.1. Partner with other members of the DoD intelligence community to develop implementing instructions as required to direct the applications of intelligence resources to support biometrics-related intelligence processing and analysis of all-source products for tactical, operational, and strategic customers.

5.8.2. Ensure DoD Intelligence Components develop collection and analysis capabilities to incorporate biometrics-derived contextual information.

5.8.3. Provide recommendations, through USD(I), to the Chairman of the Joint Chiefs of Staff pertaining to the planning, programming, budgeting, and use of intelligence resources to support biometrics capabilities.

5.8.4. Develop, maintain, and share a DoD biometrically-enabled watchlist.

5.8.5. Ensure joint intelligence policy and doctrine addresses biometrics-related intelligence functions, to include coordination and interaction among DoD Intelligence Components.

5.8.6. Advise the DoD EA for DoD Biometrics and USD(P) on foreign reliability of intelligence information, such as contextual data associated with biometrics data collection.

5.8.7. Develop a multi-discipline intelligence strategy for the current and near-term application of Defense intelligence community resources in support of biometrics capabilities.

5.8.8. In coordination with the Biometrics PSA, USD(P), USD(I), and USD(P&R), establish and maintain an intelligence-related biometrics sharing agreements with coalition partners and other international allies, as appropriate.

5.8.9. Serve as the Defense intelligence authority for certifying biometric systems on DoD intelligence information systems in coordination with the Defense Information Systems Agency (DISA) as the DoD interoperability certification authority.

5.8.10. Develop, maintain, update, and publish a list of real and potential security threats to DoD biometric technologies and systems.

5.9. The Director, DISA, under the authority, direction, and control of the ASD(NII/CIO), shall:

5.9.1. Provide collateral level, and below, DoD transport services used for voice, data, and video services and ensure the security of DoD biometrics enterprise systems by setting the conditions for proactive protections, attack detection, and performing other necessary security functions throughout the Department of Defense.

5.9.2. Serve as the DoD authority for certifying the interoperability of biometric systems.

5.9.3. As the EA for information technology (IT) standards, per Deputy Secretary of Defense Memorandum (Reference (v)), track, coordinate, and integrate all DoD IT standards activities, including the harmonization and consolidation of IT standards agreements for the purpose of nation-to-nation multinational systems interoperability.

5.10. The Heads of the DoD Components shall:

5.10.1. Coordinate all Component biometrics strategies, concepts, and requirements with the DoD Biometrics EXCOM through the DoD EA for DoD Biometrics prior to acquisition program initiation to ensure that all Component biometrics programs:

5.10.1.1. Conform to an overall DoD biometrics architecture.

5.10.1.2. Do not duplicate other programs.

5.10.1.3. Are developed fully compliant with DoD-approved standards.

5.10.2. Plan, program, and budget for DoD Component-required biometric capabilities, including capabilities to meet Joint Service or common biometrics and Component-specific capabilities.

5.10.3. Comply with DoD-approved policies, standards, processes, and procedures for collection, transmission, storage, archiving, caching, tagging, retrieval, and interoperation of biometric capabilities.

5.10.4. Ensure that DoD Component-level biometric training, direction, and implementation guidance is developed and implemented, as required.

5.11. The Secretaries of the Military Departments shall:

5.11.1. Designate a DoD Biometrics EXCOM member, who shall be a general or flag officer (G/FO) or Senior Executive Service (SES) equivalent, with responsibilities to identify Service biometrics requirements, coordinate Service programming for these requirements, and negotiate and resolve issues on behalf of their Services.

5.11.2. Coordinate all Service biometrics strategies, concepts, standards, and requirements with the DoD Biometrics EXCOM through the DoD EA for DoD Biometrics prior to program initiation or procurement actions to ensure that all Service biometrics programs:

5.11.2.1. Conform to an overall DoD biometrics architecture.

5.11.2.2. Do not duplicate other programs.

5.11.2.3. Are developed fully compliant with DoD-approved standards.

5.11.3. Plan, program, and budget for Service-specific and, where appropriate, joint and common biometric capabilities.

5.11.4. Comply with DoD-approved policies, standards, processes, and procedures for collection, transmission, storage, archiving, caching, tagging, retrieval, and interoperation of biometric capabilities.

5.11.5. Ensure that DoD Component-level biometric training, direction, and implementation guidance are developed and implemented, as required.

5.11.6. Support the geographic Combatant Commanders as they exercise overall responsibility for force protection in the AOR relative to compliance with Reference (p), by ensuring that sufficient resources are programmed in Military Department budgets to implement and synchronize Combatant Commander AOR-wide installation access requirements.

5.11.7. Review all proposed biometrics-related Service acquisition programs and budget submissions. Through Service participation in the DoD Biometrics EXCOM, coordinate with the Biometrics PSA on such programs and submissions.

5.12. The Secretary of the Army is hereby designated the DoD EA for DoD Biometrics in accordance with DoDD 5101.1 (Reference (w)) and, in addition to the responsibilities in paragraph 5.11, shall:

5.12.1. Execute responsibilities of the DoD EA for DoD Biometrics in accordance with Reference (w) and this Directive.

5.12.2. Appoint an Executive Manager for DoD Biometrics, who shall be a G/FO or SES equivalent, with responsibilities as outlined in Enclosure 4.

5.12.3. Provide for, manage, and maintain a biometrics center of excellence.

5.12.4. Appoint a single Program Management Office, under the authority of the Army Acquisition Executive, responsible for the development, acquisition, and fielding of common biometrics enterprise systems to support common, Service, and joint requirements.

5.12.5. In accordance with References (j), (k) and, when applicable, DoDD 5200.39 (Reference (x)), make recommendations to USD(AT&L) concerning acquisition category and milestone decisions for all biometric acquisition programs.

5.12.6. Program for and budget sufficient resources to support common enterprise requirements documentation, architecture development, materiel development, test and evaluation, lifecycle management, prototyping, exercises, records management, demonstrations, and evaluations to include efforts at maturing viable technologies and standards.

5.12.7. Program for and budget sufficient resources to support common biometric data management, training, operations, and lifecycle support.

5.12.8. Coordinate all component biometric requirements with DoD Component members of the DoD Biometrics EXCOM.

5.12.9. Develop, publish, and update as appropriate a DoD Biometrics Security Classification Guide.

5.13. The Chairman of the Joint Chiefs of Staff shall:

5.13.1. Validate joint requirements for biometrics capabilities, to include biometrics-related intelligence, for the Joint Force.

5.13.2. Review and assess the adequacy of biometrics acquisition programs and budgets to support joint objectives and operational plans, as well as ensure the integration of biometrics into strategic and operational plans as applicable.

5.13.3. Represent the biometrics program interests of the Combatant Commanders.

5.13.4. Coordinate with the Biometrics PSA and the DoD EA for DoD Biometrics to ensure the biometrics capability supports National Military Strategy and Combatant Commander requirements.

5.13.5. Serve as one of two Vice-Chairs of the DoD Biometrics EXCOM with responsibilities as outlined in Enclosure 3.

5.14. The Combatant Commanders shall:

5.14.1. Identify joint warfighting requirements, support the development of theater-specific operational policy and concepts of operations, and support the development and integration of theater strategic, campaign, and operational plans.

5.14.2. Make recommendations to the Biometrics PSA, the DoD EA for DoD Biometrics, and USD(P) on biometrics-related policies regarding functional needs and systems as required. Additionally advise the Biometrics PSA, DoD EA for DoD Biometrics, and USD(P) of strategic, operational, and tactical lessons learned with respect to the acquisition, installation, and employment of biometric programs, systems, and devices.

5.14.3. Geographic Combatant Commanders shall coordinate biometric policies and acquisition programs that support the protection of DoD elements and personnel in their AOR with the Heads of the Military Services, DoD EA for DoD Biometrics, Biometrics PSA, and across the interagency.

5.14.4. Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve biometric acquisition program objectives for each geographic Combatant Commander. Work with the Joint Staff and the Service component commands to ensure provision of necessary acquisition program resource requirements.

5.15. The Commander, U.S. Joint Forces Command, through the Chairman of the Joint Chiefs of Staff and in addition to the responsibilities in paragraph 5.14., shall:

5.15.1. Ensure biometrics systems support joint interoperability and joint warfighting capabilities consistent with DoDD 4630.05 (Reference (y)).

5.15.2. Support the Chairman of the Joint Chiefs of Staff in developing operational joint doctrine and training related to biometrics capabilities.

5.15.3. Ensure joint force- and Service-related exercises and experiments consider biometrics interoperability and supportability.

5.16. The Commander, U.S. Special Operations Command (USSOCOM), in addition to the responsibilities in paragraph 5.14., shall:

5.16.1. Designate a DoD Biometrics EXCOM member, who shall be a G/FO or SES equivalent, with responsibilities to identify USSOCOM biometrics requirements, coordinate USSOCOM programming for these requirements, and negotiate and resolve issues on behalf of USSOCOM.

5.16.2. Coordinate all USSOCOM biometrics strategies, concepts, and requirements with the DoD Biometrics EXCOM through the DoD EA for DoD Biometrics prior to acquisition program initiation to ensure that all USSOCOM biometrics programs:

5.16.2.1. Conform to an overall DoD biometrics architecture.

5.16.2.2. Do not duplicate other programs.

5.16.2.3. Are developed fully compliant with DoD-approved standards.

5.16.3. Plan, program, and budget for USSOCOM-required biometric capabilities, including capabilities to meet joint Service or common biometrics and USSOCOM-specific capabilities.

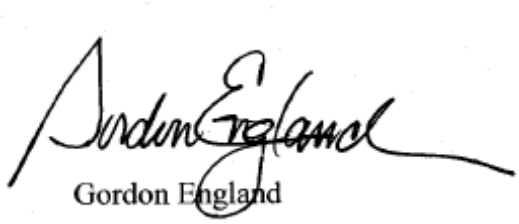
5.16.4. Comply with DoD-approved policies, standards, processes, and procedures for collection, transmission, storage, archiving, caching, tagging, retrieval, and interoperation of biometric capabilities.

5.16.5. Ensure that DoD Component-level biometric training, direction, and implementation guidance is developed and implemented, as required.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE

This Directive is effective immediately.



Enclosures – 5
- E1. References, continued
- E2. Definitions
- E3. DoD Biometrics EXCOM
- E4. Responsibilities of the Executive Manager for DoD Biometrics
- E5. Mission, Tasks, and Functions of the DoD Biometrics Center of Excellence

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Directive 5400.11, "DoD Privacy Program", May 8, 2007
(f) Deputy Secretary of Defense Memorandum, "Executive Agent for the DoD Biometrics Project", December 27, 2000 (hereby canceled)
(g) Deputy Secretary of Defense Memorandum, "Defense Biometrics," October 4, 2006 (hereby canceled)
(h) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
(i) National Science and Technology Council Subcommittee on Biometrics Glossary, September 14, 2006
(j) DoD Directive 5000.1, "The Defense Acquisition System", May 12, 2003
(k) DoD Instruction 5000.2 "Operation of the Defense Acquisition System", May 12, 2003
(l) DoD 5400.11-R, "Department of Defense Privacy Program", May 14, 2007
(m) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons", December 7, 1982
(n) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense", January 7, 1980
(o) DoD Directive 5015.2, "DoD Records Management Program", March 6, 2000
(p) DoD 5200.08-R, "Physical Security Program," April 9, 2007
(q) Homeland Security Presidential Directive 6, "Integration and Use of Screening Information," September 16, 2003[1]
(r) Homeland Security Presidential Directive 11, "Comprehensive Terrorist-Related Screening Procedures," August 27, 2004[2]
(s) Section 534 of title 28, United States Code
(t) Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458), December 17, 2004
(u) Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004[3]
(v) Deputy Secretary of Defense Memorandum, "DoD Executive Agent for Information Technology (IT) Standards," May 21, 2007[4]
(w) DoD Directive 5101.1, "DoD Executive Agent", September 3, 2002
(x) DoD Directive 5200.39, "Security Intelligence, and Counterintelligence Support to Acquisition Program Protection", September 10, 1997
(y) DoD Directive 4630.05 "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)", May 5, 2004
(z) DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004

[1] Copies of this document can be found at http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html
[2] Copies of this document can be found at http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html
[3] Copies of this document can be found at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html
[4] Copies of this document can be found at http://www.dtic.mil/whs/directives/corres/dir3.html

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Acquisition Program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need.

E2.2. Biometrics. As defined in Reference (i), 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.

E2.3. Biometrics-enabled Intelligence. Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist / insurgent network and related pattern analysis, facilitates high value individual targeting, reveals movement patterns, and confirms claimed identity.

E2.4. Biometric Sample. As defined in Reference (i), information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.

E2.5. Biometrics System. As defined in Reference (i), multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of: 1. Capturing a biometric sample from an end user; 2. Extracting and processing the biometric data from that sample; 3. Storing the extracted information in a database; 4. Comparing the biometric data with data contained in one or more reference references; 5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved. A biometric system may be a component of a larger system.

E2.6. Biometrics Programs. All systems, interfaces, acquisition programs, processes, and activities that are utilized to establish identities of people through the use of biometric modalities.

E2.7. Biometric Data. As defined in Reference (i), computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations.

E2.8. Collect. Capture biometric and related contextual data from an individual, with or without his or her knowledge. Create and transmit a standardized, high-quality biometric file consisting of a biometric sample and contextual data to a data source for matching.

E2.9. Contextual Data. Elements of biographical and situational information that are associated with a collection event and permanently recorded as an integral component of the biometric file.

E2.10. Credential. Information, passed from one entity to another, used to establish the sending entity's access rights.

E2.11. Friendly. As defined in Reference (h), a contact positively identified as friendly.

E2.12. Information Sharing Environment. An approach that facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities as well as the private sector through the use of policy guidelines and technologies.

E2.13. Match. For the purpose of this Directive only, the process of accurately identifying or verifying the identity of an individual by comparing a standardized biometric file to an existing source of standardized biometric data and scoring the level of confidence of the match. Matching consists of either a one-to-one (verification) or one-to-many (identification) search.

E2.14. Share. Exchange standardized biometric files and match results among approved DoD, Interagency, and multinational partners in accordance with applicable law and policy.

E2.15. Store. The process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on individuals when and where required.

E2.16. Unknown. As defined in Reference (h), an identity applied to an evaluated track that has not been identified.

E2.17. U.S. Person. A citizen of the United States, an alien lawfully admitted for permanent residence in the United States, or a member of the U.S. Armed Forces.

E3. ENCLOSURE 3

DoD BIOMETRICS EXECUTIVE COMMITTEE

E3.1. PURPOSE

The DoD Biometrics EXCOM serves as the DoD focal point and voice to ensure coordination of biometrics requirements, acquisition programs, and resources in support of the most operationally relevant and sustainable biometric capability across the Department of Defense.

E3.2. MEMBERSHIP

Chairman: Biometrics PSA (DDR&E)

Vice-Chairs: Chairman of the Joint Chiefs of Staff
(or designated G/FO or SES representative)
Executive Manager for DoD Biometrics (Army General Officer or SES)

Membership:
Department of the Army General Officer or SES
Headquarters Marine Corps General Officer or SES
Department of the Navy Flag Officer or SES
Department of the Air Force General Officer or SES
Joint Staff G/FO or SES
Deputy Under Secretary of Defense for Acquisition & Technology SES
USD(P) SES
USD(P&R) SES
Under Secretary of Defense (Comptroller)/Chief Financial Officer
USD(I) SES
ASD(NII)/DoD CIO SES
General Counsel, DoD
DA&M SES
Director of Program Analysis and Evaluation SES
Combatant Command G/FOs or SESs

E3.3. RESPONSIBILITIES

The DoD Biometrics EXCOM shall:

E3.3.1. Provide oversight, preclude duplication of effort, and undertake resolution of issues across DoD biometrics programs. Advise and make recommendations to USD(AT&L) concerning individual biometrics acquisition programs to ensure no unnecessary duplication of effort related to biometrics occurs across the Department.

E3.3.2. Ensure all DoD biometrics acquisition programs conform to an overall DoD biometrics architecture that enables interoperability with DoD-approved national-, international-, and other consensus-based standards.

E3.3.3. Review and approve the DoD biometrics program vision and strategy.

E3.3.4. Review and approve annual program plans and resources to support Service, joint, and common biometric capability requirements. Ensure that EA or DoD Component biometric decisions that create cost, schedule, or performance issues for other Components' biometric acquisition programs are fully coordinated and issues resolved prior to approval.

E4. ENCLOSURE 4

RESPONSIBILITIES OF THE EXECUTIVE MANAGER FOR DoD BIOMETRICS

The Executive Manager for DoD Biometrics shall:

E4.1. Provide biometrics research, technology, and information management support to the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, the Military Services, the Defense Agencies, and other DoD Field Activities, as required.

E4.2. Provide DoD biometrics research, technology, and information support to the Department of Justice, the Department of Homeland Security, the Director of National Intelligence, and other USG agencies as directed by the Secretary of Defense.

E4.3. Provide for the standardization of biometric data formats, technical interfaces, conformance methodologies, performance evaluations, and other related areas to permit interoperability, both internal and external to the Department of Defense, and to maximize utilization of DoD resources. Additionally, ensure consistency with approved national and/or international standards applicable to the enterprise. Communicate biometric technology standardization activities to DISA and National Institute of Standards & Technology for integration into overall DoD and USG IT standards processes.

E4.3.1. Provide for participation on national and international standards bodies to influence and accelerate standards development.

E4.3.2. Establish a DoD Biometrics Standards Working Group to coordinate and build consensus on biometrics standards development, recommend standards for DoD adoption, and provide guidance for consistent standards implementation.

E4.3.3. Submit recommendations for DoD adoption of published standards to DISA for review and approval per References (s) and (l).

E4.3.4. Collaborate with interagency community and other mission partners to facilitate consistent implementation and use of biometric standards.

E4.3.5. Provide for the development of tools to facilitate interoperability, both internal and external to the Department of Defense.

E4.4. Develop and maintain, in coordination with the Heads of the DoD Components as appropriate, the policy, processes, and procedures for the collection, processing, transmission, archiving, caching, and tagging of biometric data and associated intelligence.

E4.5. Develop a DoD biometrics vision and strategy, in concert with the Military Services, Joint Staff, and Office of the Secretary of Defense, for annual submission to the Biometrics PSA via the DoD Biometrics EXCOM.

E4.6. Coordinate DoD Science and Technology (S&T) plans and develop and maintain a DoD biometrics S&T "roadmap" that clearly demonstrates S&T transition points to acquisition efforts.

E4.7. Provide a means for unified acquisition and procurement of common biometric systems and equipment in accordance with References (j) and (k).

E4.8. Review DoD biometrics program plans for annual submission to the DoD Biometrics EXCOM and to the Secretary of Defense. Provide a report on progress in achieving the DoD policy goal to fully integrate biometrics in support of the full range of military operations and DoD business processes.

E4.9. Serve as one of two Vice-Chairs of the DoD Biometrics EXCOM. (See Enclosure 3.)

E4.10. Provide for the establishment and operation of a governance structure, composed of members from the DoD Components and subordinate to the DoD Biometrics EXCOM, to enable the development and execution of common requirements, standards, architectures, and research and development initiatives to support common and joint requirements.

E4.11. Manage authoritative DoD repositories of biometric samples on those individuals not issued a DoD credential in accordance with References (d) or (e) and act as a hub for biometric data sharing, to include providing for continuity of operations and disaster recovery in accordance with DoDD 3020.26 (Reference (z)).

E4.12. Coordinate all biometric program activities with identity protection and management stakeholder organizations to ensure consistency with DoD identity management principles, directives, and vision.

E5. ENCLOSURE 5

MISSION, TASKS, AND FUNCTIONS OF THE DoD BIOMETRICS CENTER OF EXCELLENCE

E5.1. The DoD Biometrics Center of Excellence, as directed by the Secretary of the Army, shall:

E5.1.1. Maintain master repositories of biometric data and non-intelligence associated information, as well as the means to exchange the data and information with other USG agencies and coalition partners, in conformance with existing regulations and statutes governing the release of classified and controlled unclassified data.

E5.1.1.1. Develop standards, processes, and procedures for biometric data archiving, caching, and tagging.

E5.1.1.2. Develop and maintain continuity of operations and disaster recovery for the Biometrics Center of Excellence in accordance with Reference (z).

E5.1.1.3. Maintain capability to rapidly store and match biometric samples submitted by the Department of Defense and other Government agencies.

E5.1.2. Conduct biometrics S&T research and engineering for the Department of Defense and other USG sponsors in support of the DoD S&T roadmap.

E5.1.3. Conduct biometrics test and evaluation activities.

E5.1.3.1. Conduct biometrics standards conformance testing for all products, programs, and services with appropriate test agencies. Relevant conformance tests include, but are not limited to, Electronic Biometric Transmission Specification/Electronic Fingerprint Transmission Specification and evaluations and assessments of biometric-enabled IT devices and systems that interoperate with the authoritative biometric database and other repositories of biometric data as appropriate.

E5.1.3.2. Provide support to DoD acquisition organizations in developmental testing, systems integration, and/or independent verification and validation of biometric systems. Coordinate this support with the appropriate test agencies.

E5.1.3.3. Support DoD operational test agencies for the conduct of operational test and evaluation activities that determine system operational effectiveness and suitability.

E5.1.3.4. Maintain awareness of the biometric marketplace and evaluate products useful to Federal government agencies; acquire and conduct commercial and government-off-the-shelf testing to identify functionality, performance, and conformance to DoD standards.