



Department of Defense

Electronic Biometric Transmission Specification (DoD EBTS) Version 3.0 Transition and Adoption Guidance

December 2012

Version 1.0

BIMA-STB-GUI-13-002

This page intentionally left blank.

Department of Defense Electronic Biometric Transmission Specification (DoD EBTS)
Transition and Adoption Guidance

December 2012

Approved by: 
COL DAN McELROY, MP
Director, Biometrics Identity Management Agency

Prepared Under the Direction of:

Mr. William Zimmerman
Chief, Capabilities Integration Division
Biometrics Identity Management Agency
251 18th Street
Arlington, Virginia 22202

Revision History

Version	Date	Document Status	Participants/Comments
0.1	May 2012	Initial Draft	Brian Harrig – BIMA STB
0.2	28 June 2012	Updated Content	Brian Harrig / Matt Young – BIMA STB
0.3	09 July 2012	Version released to BWG	Director - BIMA Executive Manager (EM) for DoD Biometrics
0.4	20 September 2012	Updated based on community feedback	BIMA
0.5	27 November 2012	Revised based on Formal Staffing Comments	Ryan Triplett/ This version has been updated based on comments received from the formal staffing process. This version was circulated to members of the Biometric Working Group for final review prior to signature.
Version 1.0	December 2012	Final Version	Ryan Triplett/ This version has been approved for public release by the Executive Manager for Defense Biometrics

TABLE OF CONTENTS

1.0	Introduction.....	1
1.1	DoD EBTS v3.0 Adoption and Implementation Memo	1
1.2	Scope and Purpose	1
1.3	DoD EBTS Background	1
2.0	DoD EBTS Evolution	1
3.0	DoD EBTS Transition Guidance and Considerations	3
4.0	Adoption of DoD IT Standards.....	5
5.0	DoD EBTS Lifecycle	5
6.0	Conclusion	7

1.0 Introduction

1.1 DoD EBTS v3.0 Adoption and Implementation Memo

This document is consistent with (and expands upon) the 14 June 2012 memo titled “DOD ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (DoD EBTS) V3.0 ADOPTION AND IMPLEMENTATION” signed by Dr. Thomas Killion - Director, and Biometric Identity Management Agency (BIMA) & Executive Manager (EM) for DoD Biometrics.

1.2 Scope and Purpose

The purpose of this document is to supplement the more technical DoD EBTS v3.0 implementation guidance document and provide the DoD Biometric Enterprise Stakeholders the necessary guidance to successfully transition and adopt DoD EBTS version 3.0 (v3.0) by providing the following:

- Evolution of DoD EBTS v3.0
- DoD EBTS v3.0 transition considerations and guidance
- DoD EBTS v3.0 formal adoption guidance
- DoD EBTS lifecycle guidance

1.3 DoD EBTS Background

The DoD Electronic Biometric Transmission Specification (DoD EBTS) is a DoD extension of the American National Standards Institution/National Institute of Standards and Technology - Information Technology Laboratory (ANSI/NIST ITL) - “Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information” as its foundational reference. ANSI/NIST ITL provides the minimum set of required data elements for entities which communicate biometric and biographic data; while also allowing for specialized business needs and user-defined requirements to be satisfied by implementers through the use of organizational specific specifications. Based on the biometric and biographical data transmitted for DoD specific missions, these unique requirements are defined in the DoD EBTS and associated Application Profiles. This approach is consistent with other US Government Organizations which also maintain their own extensions of ANSI/NIST ITL such as the FBI Electronic Biometric Transmission Specification (FBI EBTS) and the DHS IDENT eXchange Message (IXM) Specification.

2.0 DoD EBTS Evolution

Biometrics is an evolving discipline with the introduction of new modalities; expanding operational applications; ongoing standards enhancements; deployment of new, more accurate, tactical collection devices; improved communication infrastructures; and implementation of new biometric databases. The scope of biometric data collection and sharing has expanded over the years to encompass a wider range of operational scenarios. This broader set of scenarios necessitates the use of more up-to-date standards to facilitate interoperability across the entire range of military operations.

The DoD ABIS was originally designed to be similar to the FBI Criminal Justice Information Services (CJIS) Integrated Automated Fingerprint Identification System (IAFIS) and therefore its interface was based on the FBI’s Electronic Fingerprint Transmission Specification (EFTS). Because of the different nature of DoD encounters and detainment circumstances, the DoD had additional operational requirements beyond those defined in the FBI EFTS; therefore released the first widely distributed

version of DoD EBTS v1.2 based on the FBI Electronic Fingerprint Transmission Specification (EFTS) version 7.0 and ANSI/NIST-ITL 1-2000.

Since the release of DoD EBTS v1.2 a number of events shaped the release of an updated version of the DoD EBTS - Version 2.0. The scope of DoD biometric data collection and sharing had expanded to a wider range of operational scenarios. This broader set of scenarios necessitated the use of a mechanism to tailor the DoD EBTS to individual applications. This mechanism was deemed an “Application Profile” which was an addition to the base DoD EBTS v2.0 specification. It started the concept of customizations for individual biometric operational scenarios which only referenced the DoD EBTS. Additionally, data elements pertaining to biometric data collection and sharing were further defined in a Glossary, a Data Dictionary, and a Data Model. Furthermore, the ANSI/NIST-ITL 1-2000 was updated to ANSI/NIST-ITL 1-2007 and the DoD ABIS had evolved into the Next Generation ABIS (NGA) which provided additional functionality such as searching of iris images and face images, and DoD EBTS needs began to evolve for communications with DoD biometric repositories beyond ABIS (or NGA).

Since 2007 biometric technology has matured to include new collection capabilities. Stakeholder requirements have evolved requiring new and more refined data fields such as International Caveats. These additional requirements and changing technologies along with the publication of ANSI/NIST ITL 1-2011 and FBI EBTS v9.3 factored into the development of DoD EBTS v3.0. This version adds new critical capabilities for the DoD Biometrics Enterprise and includes record types to: exchange DNA and related data (Type-18); store source data from which biometric sample was derived (Type-20); input associated information such as pocket litter (Type-21); and allow information assurance to ensure data integrity (Type-98).

The biometric standardization community is currently making progress to standardize additional modalities and update current record types. The projected 2013 standardized enhancements include Dental (Type-12) in order to identify deceased individuals when facial features and / or fingerprints are not available or DNA cannot be matched. The additions to Type-10 Records will include Pattern Injury, Perioral/ Cheilosopic Imagery, Sonograms, X-Ray Images, and MRIs. Another significant standardization enhancement in 2013 will be the inclusion of Voice Data (Type-11). The aforementioned standardization efforts will ultimately drive enhancements to DoD EBTS and provide the broader Biometric and Forensic Enterprise with a standardized means of exchanging data from the most up-to-date biometric technologies.

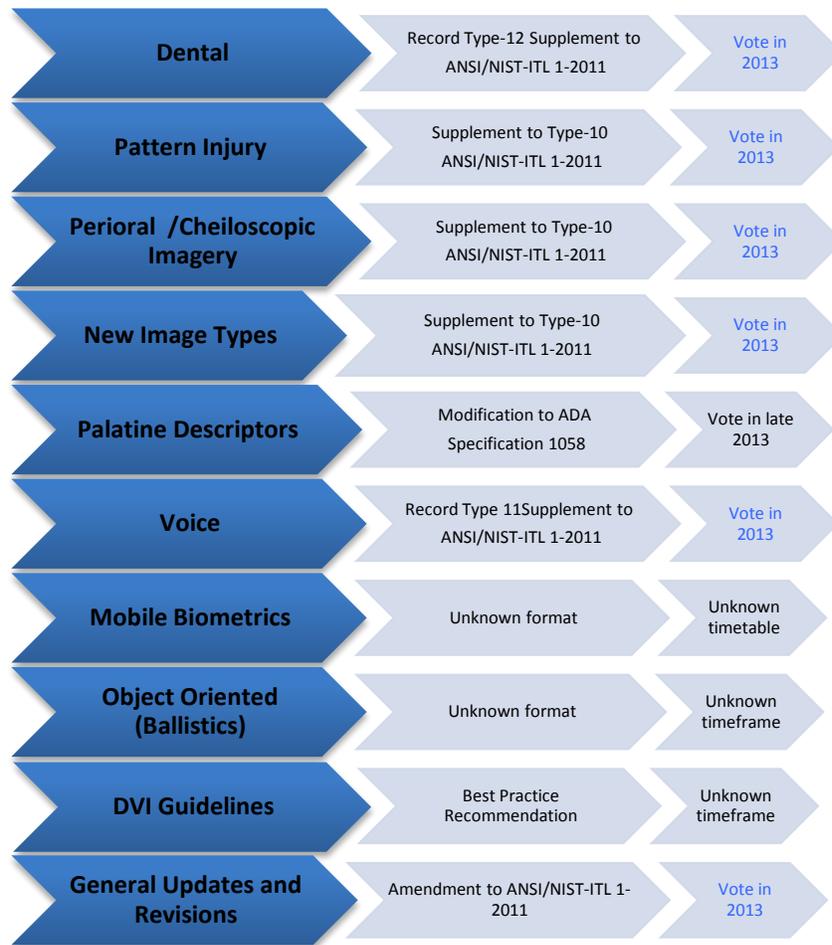


Figure 1 – Near-Term Biometric Standardized Initiatives

The Biometrics Identity Management Agency will continue to serve as the editor to refine and mature the DoD EBTS. All biometric stakeholders can influence the development of DoD EBTS by submitting formal change request and through active participation in the DoD Biometrics Standards Working Group.

3.0 DoD EBTS Transition Guidance and Considerations

One of the major challenges facing the Biometrics Enterprise is modernizing legacy systems using state-of-the-art biometric technology and implementing updated standards. From the start of an acquisition program, the DoD Biometric Enterprise must consider not only how to get useful biometric capabilities to the field quickly, but also how it can upgrade the biometric systems later. The transition to current biometric technology and DoD EBTS v3.0 (See Table 1) must be synchronized to meet acquisition program milestones and be managed with the warfighter mission in mind. Technology transitions can occur during the development of systems, or even after a system has been in the field for a number of years. The ability to transition technology smoothly and efficiently is a critical enabler for evolutionary acquisition.

Organizations taking advantage of the new capabilities and functionality of DoD EBTS v3.0 and beyond should consider who they are exchanging biometric and biographical data with as well as any associated requirements, policy, and national laws. The transition to DoD EBTS v3.0 in some instances, due to the significant technological advances, may cause data to not be fully backwards compatible with legacy devices and vice versa. For example, files provided by updated systems which originate transactions (i.e. collection devices) may not be in a format supported by systems that receive transactions (i.e. biometric repositories), especially if multiple versions of the DoD EBTS have been implemented. To ensure the latest requirements and capabilities have been implemented in both systems that generate DoD EBTS files and systems that ingest DoD EBTS files, implementers are strongly encouraged to coordinate with host organizations to agree upon a timeline for transitioning to DoD EBTS v3.0 prior to exchanging biometric data.

It is common practice for organizations to have established a change control board to oversee proposed system changes, which may include new functionality identified in transitioning to DoD EBTS v3.0 and beyond. Often times change control boards are necessary if incremental implementation or rapid technology advances to capabilities occurs; such as in the field of biometrics. These changes may impact functionality, cost, security, and/or schedule and must be reviewed by the appropriate decision makers to ensure the transition to DoD EBTS v3.0 can be made in an efficient and effective manner.

Logical Record Supported EBTS 1.2		Logical Record Supported EBTS 2.0		Logical Record Supported EBTS 3.0	
Type-1	Transaction Information ANSI/NIST ITL 1-2000	Type-1	Transaction Information ANSI/NIST ITL 1-2007	Type-1	Transaction Information ANSI/NIST ITL 1-2011
Type-2	User - Defined Descriptive Text ANSI/NIST ITL 1-2000	Type-2	User - Defined Descriptive Text ANSI/NIST ITL 1-2000	Type-2	User - Defined Descriptive Text ANSI/NIST ITL 1-2000
Type-4	Fingerprint Image Data (High Resolution Grayscale) ANSI/NIST ITL 1-2000				
Type-7	Image Data (User-defined) (FBI EFTS 7.1 - Latent Images)				
Type-9	Minutiae Data (FBI EFTS 7.1 AFIS Feature Set)	Type-9	Minutiae Data (FBI EFTS 8.1 IAFIS Features), (INCITS M1-378 Features)	Type-9	Minutiae Data (FBI EFTS 9.3 IAFIS Features), (INCITS M1-378 Features)
Type-10	Facial & SMT Image Data ANSI/NIST ITL 1-2000	Type-10	Facial and SMT image ANSI/NIST ITL 1-2007	Type-10	Face, other body part, or scar, mark tattoo (SMT) image ANSI/NIST ITL 1-2011
Type-13	Latent Image Data (Variable-resolution) ANSI/NIST ITL 1-2000	Type-13	Variable-resolution Latent Image ANSI/NIST ITL 1-2007	Type-13	Variable-resolution latent friction ridge image ANSI/NIST ITL 1-2011
Type-14	Tenprint fingerprint Impressions (Variable-resolution) ANSI/NIST ITL 1-2000	Type-14	Variable-resolution fingerprint image ANSI/NIST ITL 1-2007	Type-14	Variable-resolution fingerprint image ANSI/NIST ITL 1-2011
		Type-15	Variable-resolution palmprint image ANSI/NIST ITL 1-2007	Type-15	Variable-resolution palmprint image ANSI/NIST ITL 1-2011
Type-16	User-defined Testing Image Data (Variable-resolution) (DoD EBTS 1.2 - Iris Image)	Type-17	Iris image ANSI/NIST ITL 1-2007	Type-17	Iris image ANSI/NIST ITL 1-2011
				Type-18	DNA data ANSI/NIST ITL 1-2011
				Type-20	Source Representation ANSI/NIST ITL 1-2011
				Type-21	Associated context ANSI/NIST ITL 1-2011
				Type-98	Information assurance ANSI/NIST ITL 1-2011
		Type-99	CBEFF biometric data record ANSI/NIST ITL 1-2007	Type-99	CBEFF biometric data record ANSI/NIST ITL 1-2011

Table 1 – Logical Record Progression

Organizations transitioning to DoD EBTS v3.0 should consider strategy, policies, threats, capabilities, doctrine, technology, and budgets. Each organizations is encouraged to assess their current biometric capabilities and develop evolution plans that describe how the system, or the architecture in which the system is embedded, will evolve over a lengthy period of time to become in alignment with DoD EBTS v3.0 and beyond.

4.0 Adoption of DoD IT Standards

The DoD IT Standards Governance process selects best available standards, develops standards portfolios, and adopts them for DoD use. The approved/mandated standards and profiles are retained in the Defense Information Technology Standards Registry (DISR). The Department of Defense (DoD) DISR consists of citations of information technology standards specified through a consensus process as the *minimum* set of IT standards for the acquisition of all DoD systems that produce, use, or exchange information. The use of the DISR is mandated for the development and acquisition of new or modified fielded IT and National Security Systems (NSS) throughout the Department of Defense.

In keeping with the DoD and IC Joint Enterprise Standards Committee (JESC) mission to “facilitate a net-centric environment”, the Biometrics Identity Management Agency works across the DoD and the IC stakeholders and subject matter experts through the Biometrics Standards Working Group to successfully research and provide recommendations for the formal adoption of biometric related standards such as DoD EBTS v3.0.

Emerging standards include candidate published standards that help the program manager determine those areas likely to change creating a concern for "upgradeability". *Emerging* candidate published standards may be implemented, but shall not be used in lieu of a *mandated* standard. The use of non-mandated DISR standards must be approved by the PM or other duly designated component cognizant official and documented by a waiver notification provided to the DoD Chief Information Officer.

In order to successfully transition to DoD EBTS v3.0 it is imperative for the Biometrics Enterprise to develop a consensus during the DISR Baseline Review Cycle and formally adopt the agreed upon biometric transmission specification.

5.0 DoD EBTS Lifecycle

The DoD EBTS is processed under the DoD lifecycle standards portfolio concept and is guided by four governing principles:

- **Transparency.** DoD program managers, communities of interest, stakeholders, and other interested parties will have access to the decision-making process.
- **Participatory decision-making.** Strong DoD-wide user participation will be encouraged.
- **Accountability.** Quantifiable targets and schedules will be established and used to monitor progress in the lifecycle.

- **Consensus.** Consensus is characterized by the absence of sustained opposition to substantive issues by process participants but it does not imply unanimity. The views of all parties concerned will be taken into account and efforts made to reconcile differences. In those cases where full consensus is not reached, the process stipulates that a vote can be taken under which case decisions can be made on the basis of a pre-defined rule.

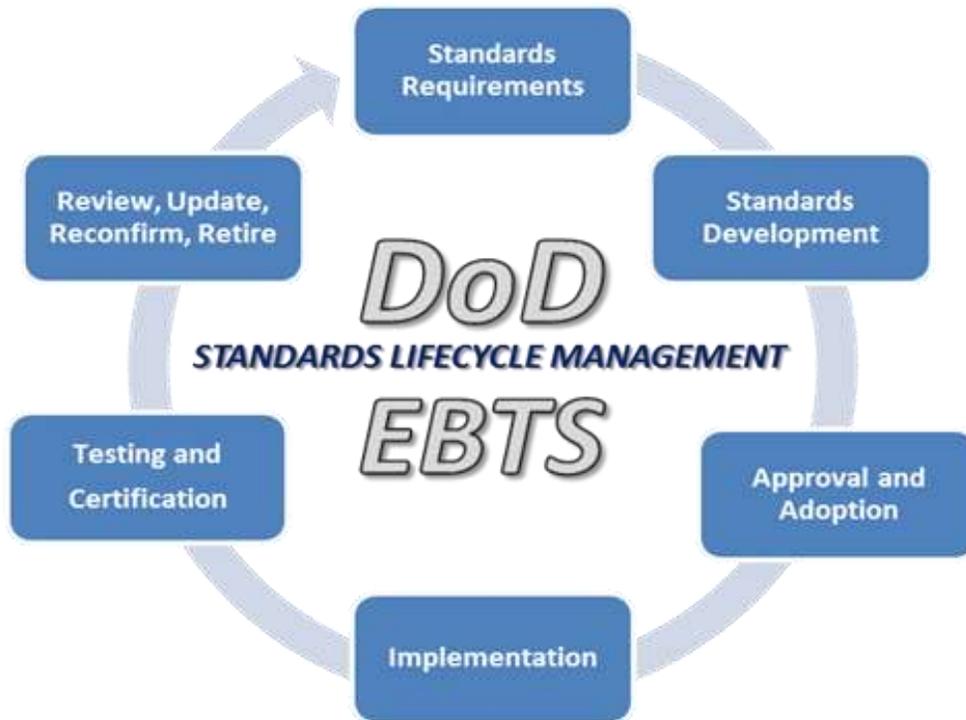


Figure 2 – DoD EBTS lifecycle

Standards Requirements. The standards lifecycle begins when system or technology requirements — or advances in biometric capabilities — necessitate the identification or development of biometric standards. DoD systems developers will identify the standards requirements that are integral to systems development, systems engineering, architecture, and integration efforts. Complementing this process are white papers, technical analyses, and review against the DISR listing of *emerging*, *mandated*, and *sunset* standards. Collaboration with the DoD Biometrics Standards Working Group is a key source for the identification of technology trends and emerging standards activities.

Standards Development. Development of a standard begins when requirements are generated for developing/updating systems or remedying a gap in capabilities. An SDO/SSO — whether government or non-government activity, consortia, professional society, national or international entity — will initiate development of a specification that will provide a solution to the biometric capability required. The appointed DoD Representative and/or ITSC sub-committees, in this instance the BIMA will follow the development and determine the need for a standard. The BIMA representative will keep the ITSC sub-committee apprised of the progress of the development and ensure, where possible, that DoD needs are considered and implemented within the standard.

Approval and Adoption. The approval process for including *mandated* standards in the DISR is through a Change Request. This process is discussed in the “*Standard Operating Procedures for the Information Technology Standards Committee, IT Subcommittee Chairs, and Technical Working Groups*”. The DoD Biometrics Standards Working Group is responsible for standards selection and initiating the approval process for *mandated* standards.

Implementation. The implementation of the standard should result in the predicted, measurable degrees of interoperability—as reflected in the comparison of standards conformance to subsequent operational testing.

Testing and Certification. The principal goal of mandating IT standards is to enable interoperability of DoD systems. To support that goal, an objective testing program and standards profile assessment must be administered throughout the lifecycle of both the standards and the systems that implement them. This testing can generally be divided into three categories: (1) testing the standards (validation testing), (2) testing systems against the standards (conformance testing), and (3) testing information exchange among systems and networks (interoperability testing).

It is DoD policy that a Standards Development Organization/Standards Setting Organization (SDO/SSO) should be responsible for developing and implementing appropriate standards validation testing programs for the standards they develop. System developers are responsible for having their products and systems undergo conformance testing to prescribed standards. System developers are also responsible for having their systems and products tested and certified for interoperability prior to fielding.

Review, Update, Reconfirm, and Retire. The DISR contains the database of *emerging, mandated, sunset, and inactive/retired* military or DoD IT standards. An automatic review date is part of the standards configuration management process, with an interval for automatic reconfirmation not to exceed one year. The DoD IT Standards Committee Secretariat will submit change requests for reconfirmation and notify the Biometrics Identity Management Agency.

6.0 Conclusion

The DoD EBTS v3.0 was developed through consensus by the DoD Biometrics Standards Working Group. The DoD EBTS 3.0 was developed in synchronization with USG interagency partners. The DoD EBTS, as well as the FBI Electronic Biometric Transmission Specification (FBI EBTS) and DHS IDENT eXchange Message (IXM) Specification all utilize ANSI/NIST ITL as their framework. This approach provides for a common set of data fields and maximization of interoperability while meeting DoD specific requirements. The FBI EBTS v9.3 and DHS IXM v6.0 were all developed on the same timeline as DoD EBTS v3.0. Future revisions to the DoD EBTS and USG transmission specification are expected as technology advances and requirements evolve. Considerations should be made to develop biometric systems that are flexible and have the ability to evolve with both technology and the needs of the warfighter.

For additional DoD EBTS transition or adoption guidance please contact the Biometrics Identity Management Agency Standards team.