Defense Standardization Program

Journal

October/December 2008

Biometrics Standardization

Biometric Interchange and Interoperability

A New Approach for Measuring Facial Image Quality

A Cultural Shift in Army Enterprise Architecture Paves the Way for Mission Success in an Era of Persistent Conflict

Defense Standardization Program

Journal

Contents *October/December 2008*

Departments

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published four times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to Editor, *DSP Journal*, Defense Standardization Program Office J-307, 8725 John J. Kingman STP 3239, Fort Belvoir, VA 22060-6233. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dla.mil
CD or DVD to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Gregory E. Saunders
Director, Defense Standardization Program Office

Timothy P. Koczanski
Editor, Defense Standardization Program Journal

Defense Standardization Program Office
8725 John J. Kingman STP 3239
Fort Belvoir, VA 22060-6233

703-767-6870
Fax 703-767-6876

dsp.dla.mil

For a subscription to the *DSP Journal*, go to **dsp.dla.mil/newsletters/subscribe.asp**

Ensuring That Biometrics Data Are Accessible, Interoperable, and Secure

Harry Truman once said that "America was not built on fear. America was built on courage, on imagination, on unbeatable determination to do the job at hand." Although the world has changed a lot since those words were spoken, many of the fears that were present then have reinvented themselves today. The Global War on Terror may be this generation's cold war as the attacks on September 11, 2001, are our Pearl Harbor. These mobilized the United States to focus resources, innovation, and ingenuity on securing our homeland and developing and refining technologies to assist with combating terrorism. Standards and standardization are fundamental building blocks for the technologies and tools that will be needed.

One area where innovation and ingenuity coupled with standardization is absolutely vital to our security is identity technology. We've all seen movie and television interpretations of scanning retinas, palms, faces, even brains in order to verify identities for access to secure buildings or information. It is clear that these kinds of identity verification techniques are no longer the province of science fiction. Many of them are in use today and are being further developed for expanded use in the future.

I know very little about biometrics, but I do know that at my place of work, at the airport, at companies, at government offices, and almost anywhere else I try to go, more identification verification is required than ever before. I now need to use a Common Access Card to gain access to my computer and my Blackberry, and I have a laptop that uses fingerprint recognition for my login.

More stringent and more comprehensive security methods, including strong identity authentication systems, are now pervasive. At no other time in our history has it been more important and more difficult to identify friend from foe. But biometrics is rapidly becoming the gold standard for ensuring the authenticity of one's identity. As the use of biometrics grows, the need to standardize and manage biometrics processes to ensure that biometrics data are accessible, interoperable, and secure also grows. Biometrics gives our security

Gregory E. Saunders
Director
Defense Standardization Program Office

forces, armed forces, border guards, and others an edge in being able to validate identity—a pivotal step to ensuring that only those with the right credentials have access to installations, databases, and networks. But what would happen if different installations used different systems and standards? What if credentialing wasn't done uniformly? The system would be effective only a small percentage of the time.

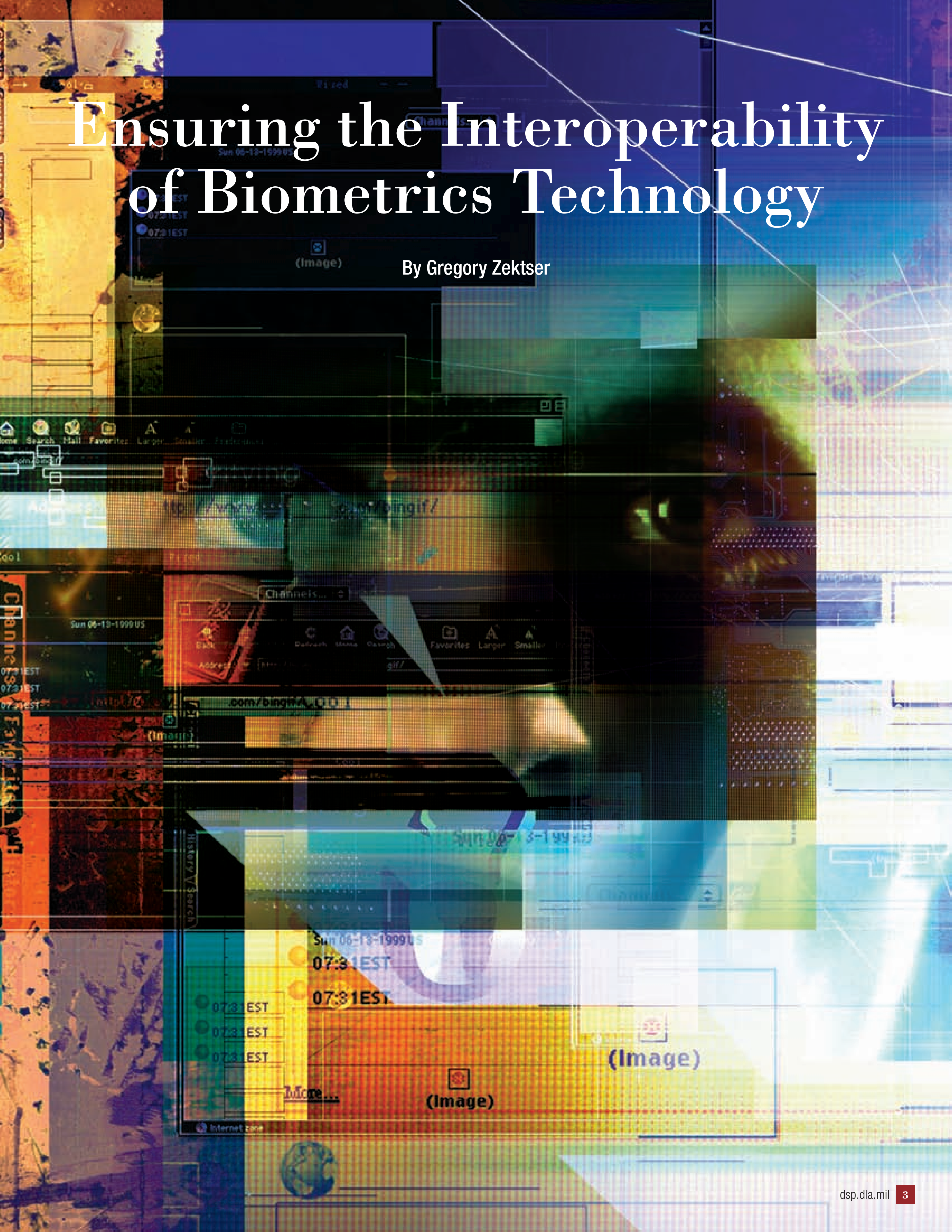
Although the use of biometrics is adding an extra layer of security in combat operations, it is essential that the biometrics data be stored in formats that can be interoperable and accessible. In one of the articles in this issue, "Ensuring the Interoperability of Biometrics Technology," author Gregory Zektser states that "standardization of nearly every aspect of biometrics technology is a necessary component of the DoD-wide biometrics solution." By having standardization within the biometrics domain, we thus minimize the "risks of creating insular, fragmented, and expensive biometrics silos that will not be able to share data or communicate with one another."

Biometrics captures our imagination of what's technologically possible, but it's not difficult to see how a lack of standards could seriously marginalize its usefulness. In this edition of the *DSP Journal*, you will read about some of the latest biometrics technologies and about how standardization enables those technologies. Many of the articles deal directly with concepts, initiatives, and issues that are facing the biometrics community, and they may pique your interest in some of the good work being done in the biometrics area. Many of the articles were submitted by the Biometrics Task Force, which is DoD's Executive Agent for biometrics and serves at the direction of the Army. We thank the task force for its submissions.

Biometrics and its associated technologies are manifestations of the imagination and determination that President Truman saw in America. Although he may well have been astounded at some of the accomplishments, I believe that he would also be quite pleased not only with the progress we've made, but also with our ability to place emphasis on doing what we need to do in order to get the job done. That would have to include the ability to standardize at the appropriate level to make these technologies available and interoperable.

Ensuring the Interoperability of Biometrics Technology

By Gregory Zektser



Biometrics technology is receiving increased attention as U.S. government agencies have recognized the perpetually growing need for stronger authentication and added security that biometric solutions can offer. DoD's Biometrics Task Force (BTF) has long been a front-runner in DoD-wide implementation of biometrics. The BTF's activities have included policy development, biometrics technology testing and deployment, and development and implementation of large-scale systems for real-world biometric data collection and matching.

The technical solutions being developed and deployed are becoming increasingly complex. Moreover, biometric systems and system components need to collect, exchange, and process biometric data records in highly distributed environments. These two factors mean that interoperability of biometric implementations is vital for DoD and across the U.S. government, on both data exchange and interaction protocol levels.

Need for Biometric Standardization

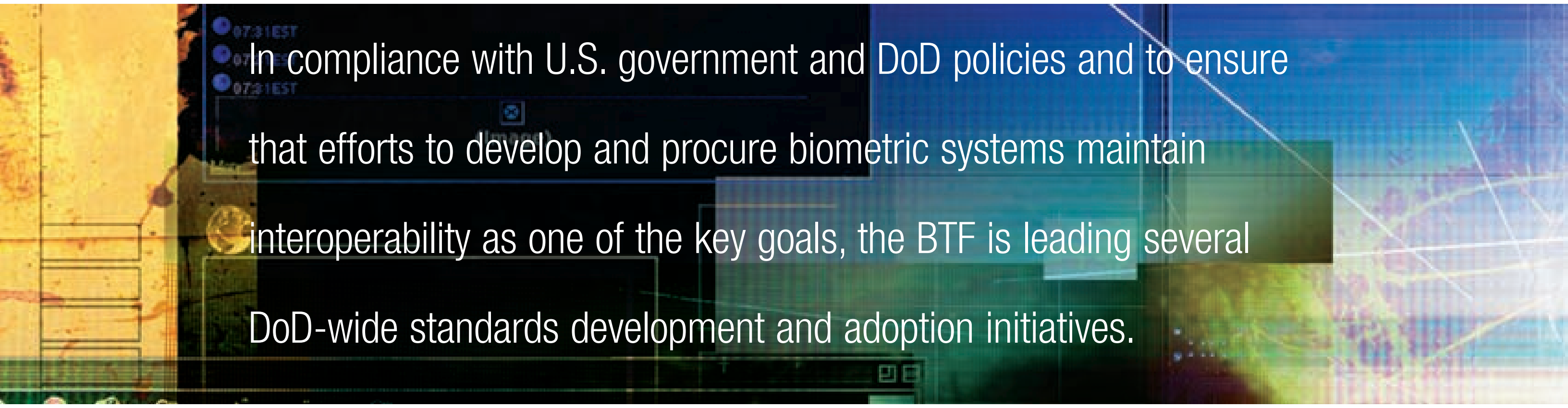
The importance and potential benefits of biometrics technologies are widely recognized. However, many technologies available in the marketplace implement proprietary and vendor-specific solutions. To satisfy end-user requirements and ensure that the best technical solutions are available to the biometric system developers, there is a need for use of biometric products manufactured by different vendors. The collected data records need to be exchanged across multiple systems and between different organizations for subsequent processing: storage, analysis, and matching. These processes can be significantly impaired when the biometric data records are stored and transmitted using different, incompatible formats.

To ensure the desired levels of interoperability, biometric products and systems rely heavily on the application of standards in the design and manufacture of system components, as well as in the testing and validation of these components. Standardization of nearly every aspect of biometrics technology is a necessary component of the DoD-wide biometrics solution, minimizing the risks of creating insular, fragmented, and expensive biometric silos that will not be able to share data or communicate with one another.

U.S. government agencies are required by law to use public standards. In 1996, the President signed into law the National Technology Transfer and Advancement Act (Public Law 104-113), which mandated the adoption and implementation of commercial standards. This law requires federal agencies to adopt private-sector standards, particularly those developed by standards developing organizations (SDOs), whenever possible.

DoD has long encouraged the use of commercial standards to ensure that mission objectives are met. For example, in his June 1994 memorandum, "Specifications and Standards—A New Way of Doing Business," Secretary of Defense William Perry specified greater use of commercial specifications and greater use of standards as two of the most important action items for DoD. To facilitate this new way of doing business, DoD issued policies to ensure and support the adoption and implementation of standards. DoD supports standards in policies such as DoD Instruction 4120.24, "Defense Standardization Program (DSP)," which specifies that communication information officers are to avoid developing and implementing DoD-specific standards, known as military specifications. Such policies signaled a shift away from government-specific standards toward commercial standards.

One of the most recent policies—DoD Directive 8521.01E, "Department of Defense Biometrics," issued in February 2008—directs the use of consensus-based biometric standards and the participation in national and international standards bodies. This policy states that execution of biometric functions must be ensured through the use of "DoD-approved national, international, and other consensus-based standards" and requires DoD to "provide for participation on national and international standards bodies to influence and accelerate standards development."


In compliance with U.S. government and DoD policies and to ensure that efforts to develop and procure biometric systems maintain interoperability as one of the key goals, the BTF is leading several DoD-wide standards development and adoption initiatives.

BTF Standardization Activities

In compliance with U.S. government and DoD policies and to ensure that efforts to develop and procure biometric systems maintain interoperability as one of the key goals, the BTF is leading several DoD-wide standards development and adoption initiatives. BTF is coordinating these initiatives with a number of other U.S. government agencies, such as the Department of Homeland Security, National Institute of Standards and Technology (NIST), and FBI. One of these initiatives is participation in biometric standards development. To ensure proper coordination of this initiative (as well as others), the BTF has created and is leading the DoD

Biometric Standards Working Group, a consensus-based forum with DoD-wide participation.

To meet DoD's needs for biometric standards, the BTF has adopted a two-step development approach:

- Collect and analyze DoD's requirements and ensure that these requirements are addressed to the maximum extent possible in national and international biometric standards
- Communicate DoD-wide the direction and status of the development of biometric standards so that system developers can adopt these standards early in the development life cycle.

In addition, one of BTF's major initial efforts was to publish *Biometrics Standards Development Recommended Approach*, which details the strategic, collaborative approach to the identification of, participation in, and development of biometric standards. The recommended approach enabled DoD to guide biometric standards development to ensure that the standards provide support for the joint warfighter and promote interoperability among forces, services, and components—human and technical. It identified the current status of biometric standards and the gaps that require development of new (or modification of existing) standards. The document was coordinated with DoD components and other U.S. government agencies prior to its finalization.

To implement this approach, the BTF is actively participating in both national and international standards bodies on biometrics. These bodies include the InterNational Committee for Information Technology Standards (INCITS), American National Standards Institute (ANSI), and the Joint Technical Committee/Subcommittee on Biometrics of the ISO/International Electrotechnical Commission (IEC). BTF's participation includes membership in working groups and participation in plenary meetings; BTF members also serve as standards editors and primary contributors. Recently, because the BTF standardization interests are expanding, participation in other standards bodies is being considered.

BTF's primary focus at the standards bodies has been to ensure that, in coordination with the DoD components and services (through the Biometric Standards Working Group), DoD interests are represented and protected as far as development of base biometric standards is concerned.

The BTF participates in the development of national and international biometric standards in the following categories:

- Technical interface standards, such as the Common Biometric Exchange Formats Framework and the Biometric Applications Programming Interface (BioAPI)
- Biometric data interchange format standards for multiple modalities (finger image, finger minutiae, iris image, facial image, etc.)
- Biometric testing standards, including performance testing and reporting, conformance testing, and biometric sample quality measurement standards
- Biometric application profiles
- Cross-jurisdictional and societal issues.

Standards for conformance testing methods are of particular interest to DoD. The BTF, as a primary contributor and editor, has led the development of conformance testing standards for the BioAPI specification and for data interchange formats (including a generalized testing method and specific test methods for fingerprint images). The BTF has also sponsored development of the recently published national standard on DoD-specific application profiles.

The status of the DoD-sponsored biometric standards is as follows:

- INCITS 429, "Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification" (published)
- ISO/IEC 24709-1, "Conformance Testing Methodology for BioAPI—Part 1: Methods and Procedures" (published)
- ISO/IEC 24709-2, "Conformance Testing Methodology for BioAPI—Part 2: Test Assertions for Biometric Service Providers" (published)
- ISO/IEC 29109-1, "Conformance Testing Methodology for Biometric Data Interchange Records—Part 1: Generalized Conformance Testing Methodology" (under development)
- INCITS 423.4, "Conformance Testing Methodology for INCITS 381, Finger Image Data Interchange Format" (published)
- INCITS 421, "American National Standard for Information Technology—Biometric Profile—Interoperability and Data Interchange DoD Implementations" (published).

In addition to work on national and international standards within the standards bodies, the BTF is an active participant in the development of other standards, such as the recently published ANSI/NIST Information Technology Lab 1-2007 and 2-2008. For DoD-specific needs, the BTF developed and is now working on a major revision of the DoD Electronic Biometric Transmission Specification, which is designed to ensure biometric data exchange across DoD.

The Way Ahead

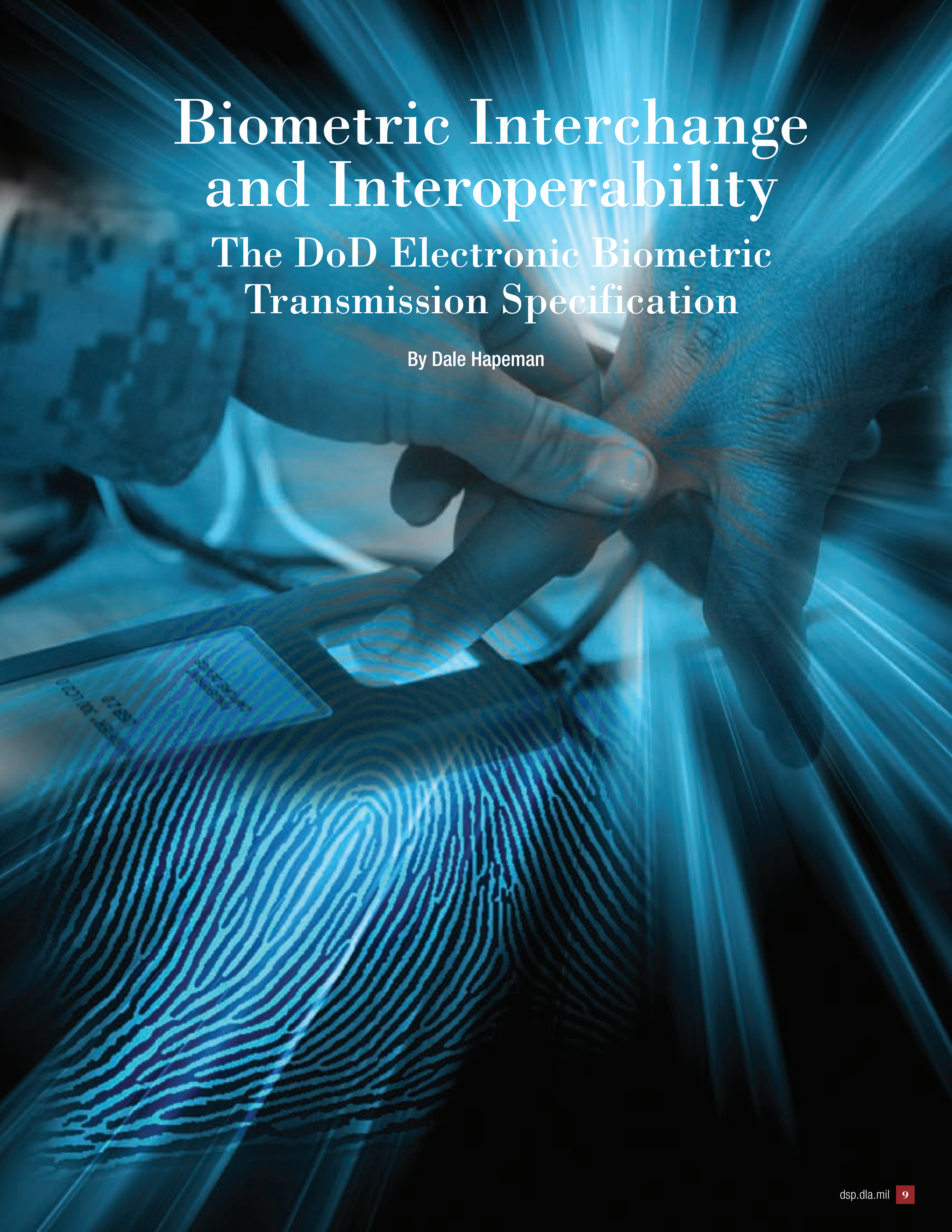
BTF's efforts and leadership in the development of biometric standards have been widely recognized by the biometrics community and within the U.S. government, but more challenges are to be met. For example, significant overlap exists between approved or published national biometric standards and counterpart international biometric standards. A comparative analysis performed by the BTF has shown that some of these standards are not entirely compatible and that conversion of conforming data records from one format to another may be problematic. A couple years ago, the BTF in coordination with the Department of Homeland Security and NIST, initiated a new approach that should eventually result in wide adoption of international standards instead of the corresponding national standards. This result would ensure higher levels of interoperability across national and international users. The BTF will continue this effort in the coming years.

As new biometric modalities emerge and technologies advance, there is a growing need for the development of new standards and the significant revision of published standards. The BTF will continue to take an active part in this process to ensure that DoD's needs are properly addressed.

As the BTF's scope of work expands into various biometric-related areas of identity management, BTF will need to expand its participation in the SDOs. The BTF will conduct analyzing which standards bodies are working on which standards and will determine how to expand its participation in the SDOs.

About the Author

Gregory Zektser is a support contractor and senior subject matter expert on DoD's Biometrics Task Force. Mr. Zektser's responsibilities and experience include work on biometric standards and test and evaluation. He has more than 20 years of experience in various areas of systems engineering, technical standards development, quality management, and biometrics.



Biometric Interchange and Interoperability

The DoD Electronic Biometric Transmission Specification

By Dale Hapeman

The fundamental purpose for collecting biometric samples is to enroll them or to match them against previously enrolled samples. Within DoD, this capability is used to meet internal business needs and warfighting needs. In most cases, biometric data, and other DoD-relevant data, must be moved from a collection location to a matching location. To accomplish that task, DoD has established the DoD Electronic Biometric Transmission Specification (EBTS).

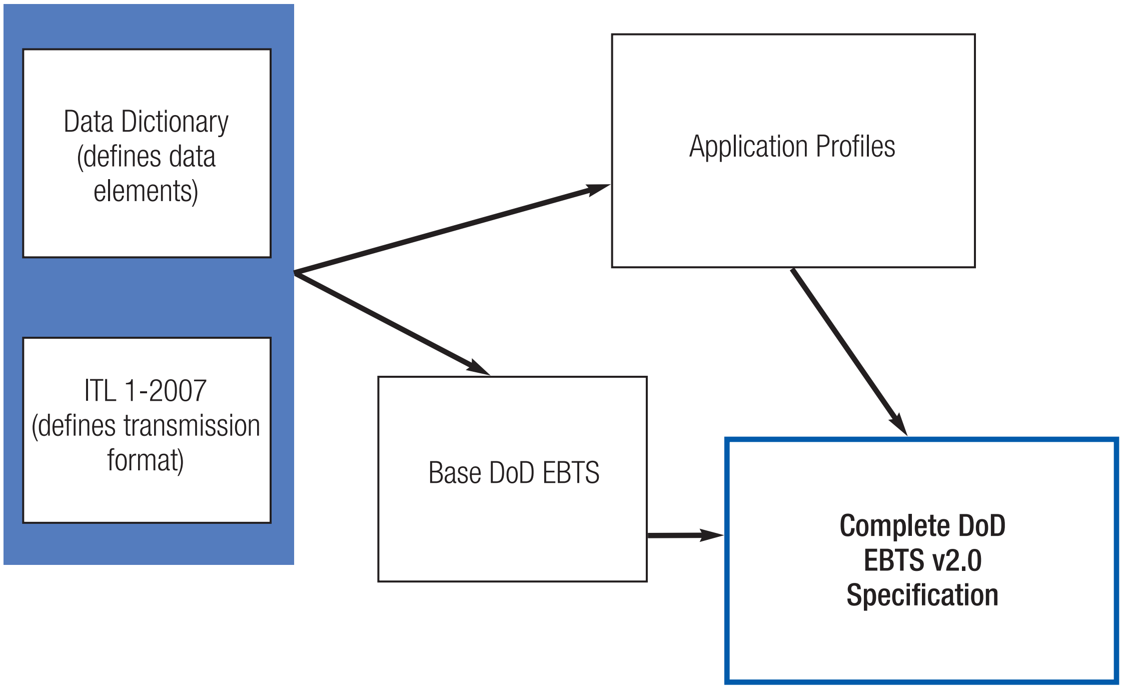
The DoD EBTS enables DoD biometric capabilities by establishing a mandated standard to which all DoD collection devices and matching engines must conform. This transmission specification creates a DoD biometric architecture in which data collected by any DoD device are interoperable with a central biometric matching engine. That central matching engine is the DoD Automated Biometric Identification System, which was initially modeled after the FBI's Integrated Automated Fingerprint Identification System. Following this relationship, the logical choice was to add DoD requirements to the FBI's current Electronic Fingerprint Transmission Specification (EFTS). The FBI's EFTS was an implementation of the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Information Technology Lab (ITL) fingerprint standard (known as ANSI/NIST-ITL 1-2000). This resulted in a version of DoD EBTS (v1.2) that was an extension of existing specifications.

Creation of the DoD EBTS was predicated on the fact that DoD has a different set of requirements than the FBI. DoD entities face multiple operational scenarios in which factors such as available time on target, volume of individuals encountered, and levels of danger all vary widely. For example, in situations in which a person of interest is in custody (such as an enemy prisoner of war) and time is not of the essence, many samples can be taken. On the other hand, when warfighters must screen high volumes of individuals at checkpoints; time is limited and safety is a high concern; in that situation, the warfighter may collect only a single fingerprint. Another extension of existing specifications was the capture of iris images, for which the FBI EFTS is not equipped.

Implementers quickly realized that these unique situations, requirements, and data sets could not be handled by the DoD EBTS alone. These additional capabilities were handled by a concept called an implementation domain. Although ANSI/NIST-ITL 1-2000 defines this concept, the standards team from DoD's Biometrics Task Force formalized the definition and coordination of these domains within DoD by generating a standard operating procedure. This procedure ensures that data elements are coordinated and do not conflict DoD-wide and that they are implemented consistently within collection and matching devices.

The continued evolution of a DoD biometrics capability and the creation of more scenarios and applications made it clear that the criminal justice basis for the DoD EBTS was not flexible enough. This led to a new model for the design of the next version of the DoD EBTS (v2.0). This effort was aided by the development of the integrated biometrics data dictionary. The data dictionary established a flexible method for defining the data elements that a DoD EBTS v2.0 would carry. The transmission format was still based on the construction rules established by an ITL document, ITL 1-2007 (which is an update of ITL 1-2000).

FIGURE 1. Process for Completing EBTS v2.0


Data Dictionary (defines data elements)
ITL 1-2007 (defines transmission format)
Application Profiles
Base DoD EBTS
Complete DoD EBTS v2.0 Specification

As shown in Figure 1, DoD EBTS v2.0 employs data elements defined in the DoD biometrics data dictionary. It moves the definition of capabilities that are required by specific applications (such as checkpoint situations) into a separate, application-specific document called an application profile. Thus, the base DoD EBTS is reliant on ANSI/NIST-ITL 1-2007 but not on an FBI specification. In other words, it is no longer criminal-justice-specific.

Additional tasks required to complete the development of a comprehensive DoD EBTS standardization program include a detailed configuration management plan and the implementation of a conformance testing capability. Configuration management will be coordinated across the data dictionary, the base DoD EBTS, and any application profiles. Each is interrelated, and changes will ripple across them all. A DoD EBTS conformance-testing capability is critical for ensured interoperability of vendor products and is currently under development at the Biometrics Task Force.

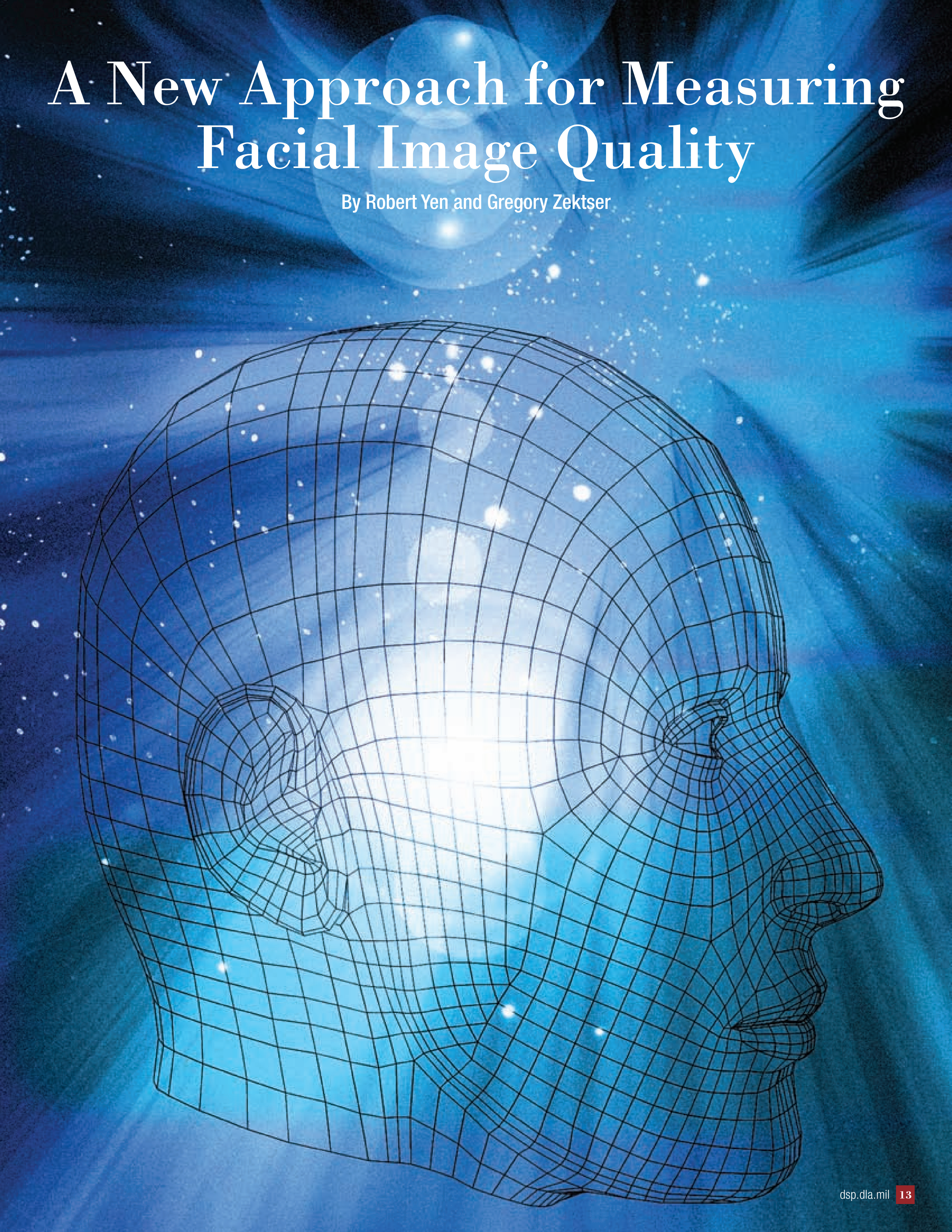
A final task will be to establish the DoD EBTS v2.0 as a DoD-mandated specification. This is accomplished by nominating and championing it through the Defense Information Systems Agency's registry of standards, the Defense Information Systems Registry. Also, from a government-wide perspective, the DoD EBTS will be proposed for inclusion in the Registry of U.S. Government Recommended Biometric Standards, which is maintained by the National Science and Technology Council's Subcommittee on Biometrics and Identity Management.

About the Author

Dale Hapeman is a support contractor and senior subject matter expert for the DoD Biometrics Task Force. He has been supporting the task force for more than 5 years, addressing architectural and system issues relating to biometrics for identification and access control. He has been the primary editor of DoD's Electronic Biometric Transmission Specification. Mr. Hapeman has a 20-year background in information assurance focusing on security standards and protocols.

A New Approach for Measuring Facial Image Quality

By Robert Yen and Gregory Zektser



Introduction

In general, face recognition systems are based on the matching algorithm to produce a similarity measure for the match of the *probe* image to each of the *gallery* images. A threshold can be set so that a match is reported only when the similarity measure between the probe and a gallery image exceeds the threshold.

The facial image data record format is used to provide interoperability between uses of face recognition systems and digital facial image storage systems. Measuring the quality of facial images is a crucial step in this identification process. The ideal facial image has certain features (for example, eyes and mouth) that are clear and computer recognizable. These facial features make each facial image unique. Quality measurement is based on the detection of facial features from an image. Facial image quality may significantly affect the performance of automatic face recognition systems during the matching and identification processes. However, the operational environment (lighting, equipment quality) in which a facial image is collected often causes poor image quality. Field operators need to have a method of quickly providing calculated quality scores of the collected images to assist them with rendering the "accept" or "reject" decisions. A trusted and widely used independent method for measuring facial image quality does not exist. This is because the operational databases are "contaminated" with poor quality images that negatively impact the performance of automatic face recognition systems.

Face recognition data records can, in general, be used for human examination as well as computer identification and verification. On May 13, 2004, the National Institute of Standards and Technology (NIST) published American National Standards Institute/InterNational Committee for Information Technology Standards (ANSI INCITS) 385-2004, "Face Recognition Format for Data Interchange." Standard facial image quality measurement will aid in the interoperability and performance of automatic face recognition systems.

This article proposes a new approach to measuring facial image quality. This approach—FaceQM—ensures that only a good quality facial image can be selected for further processing, which is one of the conditions for improved performance of the face recognition process. The proposed approach has four steps: (1) define a good skin color space, (2) define a good maximum likelihood estimation (MLE) using a Non-Uniform Binary-Splitting (NUBS) algorithm, (3) detect and verify facial features through a training process, and (4) determine the quality score. We describe these steps below. We then describe the FaceQM tool—an application that implements the proposed measuring algorithm. Finally, we address the use of FaceQM as a conformance testing tool for ANSI INCITS 385-2004.

Skin Color Space

Skin color space is the most important factor that should be considered when building a statistical model for segmenting skin-colored regions. Segmentation of face region becomes robust if only the skin component is used in analysis. From previous work, the color-of-skin data actually are a combination of red, yellow, and brown.[1] Therefore, luminance, hue, saturation, chrominance red, and chrominance blue are chosen to build the skin color space model. Research has shown that skin color is clustered in a small region of the chrominance, hue, and saturation spaces. Table 1 summarizes the color component conversion coefficients from red, green, and blue (RGB) bytes.

TABLE 1. Summary of Color Component Conversion Coefficients

Luminance	$Y = 0.299R + 0.587G + 0.114B$
Chrominance red	$Cr = (131R/256 + 110G/256–21B/256) + 128$
Chrominance blue	$Cb = [131B/256–44R/256–87G/256] + 128$
Hue	$H = [\pi/2–\tan^{-1}\{(2R–G–B)/3^{1/2}(G–B)\} + \pi;\ G < B]/2\pi$
Saturation	$S = [9/5(r'^2 + g'^2)]^{1/2}$, where $r' = r–1/3$, $g' = g–1/3$, and $r = R/(R+G+B)$, $g = G/(R+G+B)$
Cr^2	$Cr \times Cr$
Cb^2	$Cb \times Cb$

The skin color distribution in the planes is modeled as Gaussian. A large skin color pixels collection database is used to train the Gaussian model. The skin pixels from facial images are carefully cropped out to form a training dataset.

NUBS Algorithm

A natural way to define classes is utilizing the property of nearest neighbors or characteristics in a V color space. A vector v should usually be put in the same class as its nearest neighbor or characteristics based on MLE. The goal of MLE is to find the representative variables that make the observed data fit to a known density distribution. Let v_i = [Hue Cr^2 Cb^2]^T denote the feature vector of an input pixel i.

In the NUBS process, the input vector V = { v_i } drawn from an N-dimensional space is mapped into a finite set of representation mean vectors C = { C_j: j = 1, 2, …, M } contained in the space. The mapping is completely characterized by the class P = { P_j: j = 1, 2, …, M } in the input space V, which assigns an input vector v ε P_j to the representative mean vector C_j.

The algorithm begins with the calculation of the mean vector μ of current class j. The definition of the mean vector μ_j of the class j is $\mu_j=(\varepsilon_i\ v_i\ )/N_j$, where i is for all vectors inside the class j and N_j is the total number of vectors in class j.

Then, set the two subclass initial vectors as equal to μ_j. Each vector v_i is classified by the calculation of weighted distance and decision made to the nearest class.

If we define D_1 as the distance between the class 1 and vector v_i and D_2 as the distance between the class 2 and vector v_i, then,

$$D_1 = \{ \varepsilon_k(C_j{-}v_{ik})^2 \}^{1/2}, \text{ and}$$

$$D_2 = \{ \varepsilon_k(C_{j+1}{-}v_{ik})^2 \}^{1/2}, \text{ where } k = 1 \text{ to N-dimension of features.}$$

If D_1 is less than D_2, then we classify v_i to P_j and update the mean vector C_j by calculation of v_i and C_j with weighting coefficients in each term. The calculation of updated C_j is

$$C_j = \frac{N_j}{N_j+1} C_j + \frac{1}{N_j+1} v_i.$$

And update the value of N_j by $N_j + 1$. Otherwise, we classify v_i to P_{j+1} and update the C_{j+1} by the following equation:

$$C_{j+1} = \frac{N_{j+1}}{N_{j+1}+1} C_j + \frac{1}{N_{j+1}+1} v_i.$$

And update the value of N_{j+1} by $N_{j+1} + 1$. The initial values of N_j and N_{j+1} are always set to equal the number of vectors of current class j before splitting.

In an ideal case, we want our training dataset to have equal numbers in each class. It is also preferred to have an equal number of samples from the collected dataset for each class. In reality, however, this is not the case. We solved this problem by adjusting the "feature-weights" parameter in our splitting implementation. The feature-weights ($N_j/N_j + 1$, $1/N_j + 1$, $N_j/N_{j+1} + 1$, and $1/N_{j+1} + 1$) are used in the above calculations for updating C_j and C_{j+1}.

Applying the same process on each input vector v_i forms two subclasses. Each subclass has its own estimated feature density function, which is presented by mean vector μ_j, variance σ_j^2, and the number of vectors N_j. We then repeat the same process on each class until the variance of each class is less than the defined threshold value, ε.

Since iteration processing always splits the data into two subclasses and is based on the detection of a certain class whose variance value is larger than ε, this new approach is called the NUBS algorithm. In this algorithm, the maximum number of classes can be achieved (equal to the number of input vectors) by setting $\varepsilon = 0$. The maximum number of iterations is calculated by subtracting 1 from the number of input vectors.

The NUBS algorithm processing procedure has eight steps:

1. Calculate the mean vector of all training data
2. Apply the NUBS algorithm and split parent data into two subclasses
3. Calculate the mean vectors and variances of each subclass
4. Register the splitting path into a decision tree (DT)
5. Compare both variances to defined threshold ε
6. Return to step 2 to process subclass if necessary
7. End process.

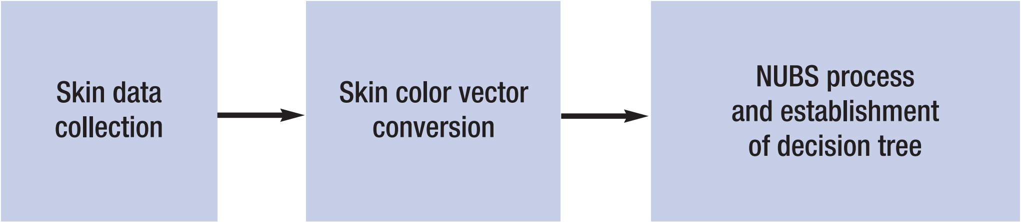
The goal of the NUBS algorithm is to reach maximum classification accuracy over the images and provide a well-estimated classifier system that will meet the following demands and constraints:

- Real-time operation on a standard personal computer
- Fast path to identify each entry color pixel into the class
- Near-optimization of the skin data feature classifiers.

Training Process

The training process operates in three successive stages, shown in Figure 1. The first stage of the training process attempts to collect a reasonably large skin data set, adopted from the digitized face color image database. This process includes a human verification step to guarantee that all the data come from a human skin area. Inputs of this stage are digitized color images, and outputs are guaranteed human skin color pixels. That includes 4,194,304 color skin pixels. This image will act as the fundamental training database.

FIGURE 1. Training Process


Skin data collection
Skin color vector conversion
NUBS process and establishment of decision tree

The second stage converts a regular RGB three-byte pixel value to a skin color feature vector. The third stage establishes a decision tree and separates the training data into different classes by using the NUBS algorithm. The DT is a decision path and is used as a final decision maker for each input color vector later in the skin detection process. Each class represents a possible skin class in a certain light source environment.

The training process is based on the NUBS algorithm. The purpose of the training process is to attempt to build an efficient DT. Each node (subclass) inside the DT will be represented by its mean vector and variance. The training data set is the collection of verified skin color pixels. Each individual entry feature vector is converted from its low-passed RGB bytes. The iterative training process begins with the whole training data set. The maximum length of the classes can be calculated during the iteration process.

The training procedure has eight steps:

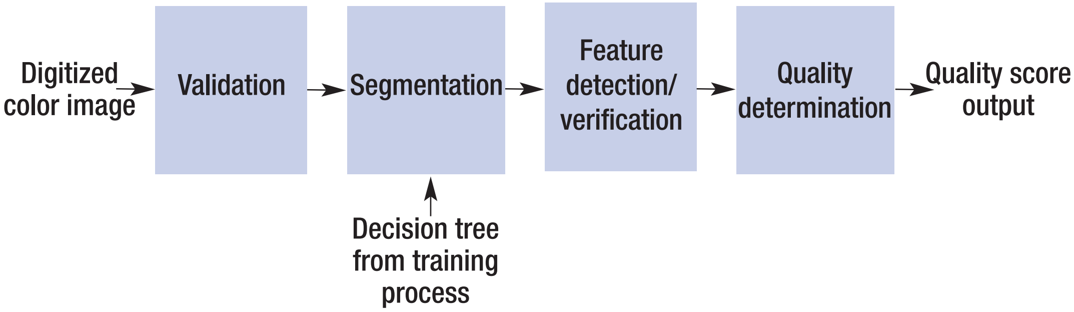
1. Set the ε value
2. Initialize the count of established node n_C, which starts from 1
3. Calculate the mean vector and variance
4. Split vectors into two subclasses by using the NUBS algorithm
5. Calculate the mean vectors and variances for both subclasses
6. Register the nodes, mean vectors, and variance into the DT
7. If all variance values are less than ε then end the process, or
8. Identify the node for which variance is higher than ε, then go to step 4.

Adjustment of ε values is necessary in the training process to fine-tune the DT. This DT provides the decision rules on the face area segmentation process. The DT is well trained from the training process with the NUBS algorithm. The training data set may need to be updated or exchanged, which could happen on different characteristics of inputs, for example, scanned resolutions or sizes of the facial images.

Quality Score

The quality score is determined through a measuring process that occurs in four successive modules, as shown in Figure 2 and described below.

FIGURE 2. Quality Measuring Process



VALIDATION MODULE

This module validates the image header information with the requirements of ANSI INCITS 385-2004. Each image usually has a header section providing the detailed information in each field, for example, scanned resolution, number of rows, number of columns, and size of image. This module validates and verifies the value of each field with the requirements of ANSI INCITS 385-2004. The nonconformant facial images will be filtered out by this module.

SEGMENTATION MODULE

Segmentation is a real-time process for each input image. The purpose of the segmentation process is to attempt to identify skin areas from that image. The process is based on a DT that applies each color feature vector to identify and verify skin areas.

This module segments the face region from entry image by the DT that is built from training data with the NUBS algorithm. This module labels each pixel with the nearest class number from the DT as well. This label information provides the opportunity to do further processing if necessary.

The segmentation steps are as follows:

1. Set skin feature similarity threshold value, σ
2. Convert each pixel's RGB byte to a v vector
3. Use DT to identify and verify all face pixels with defined σ value
4. End the process.

FEATURE DETECTION/VERIFICATION MODULE

Various facial features will be detected from the segmented face area. Eyes, mouth, and ears are the most important features for face recognition and estimation of head pose. We use luminance, chrominance, and edge information to locate eyes, mouth, and ears directly. Several other features—for example, blur measurement, red-eye detection, luminance dynamic range, contrast, percentage of face area, position of eyes, centered image, roll angle, yaw angle, and color saturation ratios—can be detected from the segmented face area as well.

QUALITY DETERMINATION MODULE

This module determines the quality score—translated as "Good Image" or "Need to Rescan"—for each facial image, based on verification results of facial features. Each facial feature has its own constraint. Table 2 lists the constraints of all detected facial features. The determined "Good Image" quality score means that all detected facial features of the facial image satisfy all constraints. Any undetected or unsatisfied features will cause the measured facial image to have a "Need to Rescan" quality score. The 5 percent tolerance in some features' constraints allows for variations that might occur during the picture-capturing process. To determine the quality score, we developed an application—a FaceQM tool—that implements the proposed measuring algorithm.

TABLE 2. Constraints of Facial Features

Feature	Constraints
Eyes' locations	To be detected
Mouth's location	To be detected
Ears' locations	To be detected
Blur	To be identified
Red eye	To be examined
Distance between eyes	Image width/4 ± 5%
Pose angle–roll	± 5°
Pose angle–yaw	± 5°
Position of eyes	50%–70% of the vertical distance up from the bottom edge of the captured image
Centered image	△ (middle of eyes–middle of image width) < 5% of half image width
Head width ratio	Image width:head width = 7:4
Head height ratio	Head height:image height < 80%
Grayscale density	The dynamic range of the image should have at least 7 bits of intensity variation in the facial region of the image
Color contrast	0.45 < average contrast value < 0.95
Color saturation	Top half:bottom half area and left half:right half area should have close to 1 in both saturation distributions

FaceQM Tool

The FaceQM tool determines the quality score from a facial image with 12 features from the detected face area. These 12 features fall into four different categories:

- Distance, including the near/far feature
- Position, including the centered image and eye position features and red-eye examination
- Pose angle, including roll angle and yaw angle features
- Lighting, including contrast, vertical saturation ratio, horizontal saturation ratio, luminance dynamic range, and blur identification features.

The quality score is presented in two forms: a D-Score and a C-Score.

The value of the D-Score is the total number of facial features that satisfy the quality constraints such as contrast or roll angle. The minimum D-Score is 0, which means that none of the evaluated values of the 12 features satisfy the constraints. The maximum D-Score is 12, which means that all of the evaluated values of the 12 features satisfy all constraints. For example, the FaceQM tool gives a quality score of 11 to a facial image that has satisfied all constraints except one feature (such as yaw angle).

The value of the C-Score is the minimum value from the quality levels of 12 facial features and ranges from 0 (worst quality) to 100 (best quality):

$$\text{C-Score} = \text{Minimum value of } q_i,$$

where i = 1 to 12 and q_i is the i^{th} feature's quality level between 0 and 100.

Each feature's quality level is converted from measured value with its piece-wise mapping functions, which are based on the constraints listed in Table 2. If the image fails to satisfy the constraints of a given feature, it is not counted and the image quality score is decremented.

Figure 3 shows a frontal facial image that was processed with the proposed approach and is determined to be a "Good Image" (D-Score = 12 and C-Score = 84). Figure 3A is the original image. Figure 3B displays the segmented face area; 16 skin classes were clustered by the DT. Figure 3C has the eyes, mouth, and ears marked inside the green rectangular box that indicates the detected face area; within that area, the mouth is marked by a white rectangular box, the centers of the eyes are marked by white squares, and the centers of the ears are marked by white dots. Figure 3D shows the results of the facial features verification; the blue color values indicate that the detected features are satisfying the constraints.

Figure 4 illustrates an image determined to have unacceptable quality scores (D-Score = 11 and C-Score = 49) and therefore needs to be rescanned. This result is based on the determination that the subject's yaw pose angle is toward the left and greater than the constraint.

FIGURE 3. Example of "Good Image"

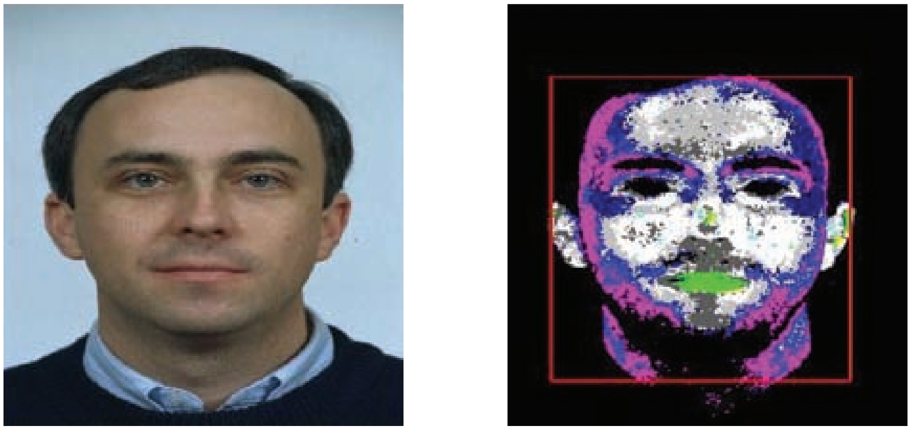


FIGURE 3A. Original Image

FIGURE 3B. Segmented Image

FIGURE 3. Example of “Good Image,” cont.

FIGURE 3C. Facial Feature Image

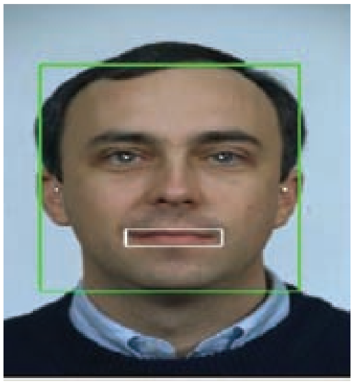
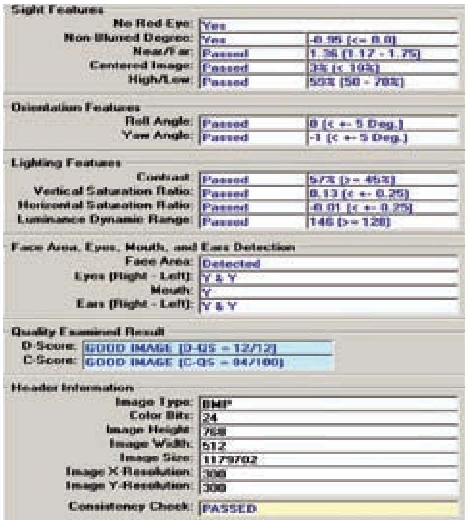


FIGURE 3D. Feature Verification Results



```
Sight Features
                No Red Eye:  Yes
        Non-Blurred Degree:  Yes          -0.95 [<= 0.0]
                  Near/Far:  Passed       1.36 [1.17 - 1.75]
            Centered Image:  Passed       3% [< 10%]
                  High/Low:  Passed       55% [50 - 70%]

Orientation Features
                Roll Angle:  Passed       0 [< +- 5 Deg.]
                 Yaw Angle:  Passed       -1 [< +- 5 Deg.]

Lighting Features
                  Contrast:  Passed       57% [>= 45%]
 Vertical Saturation Ratio:  Passed       0.13 [< +- 0.25]
Horizontal Saturation Ratio: Passed       -0.01 [< +- 0.25]
  Luminance Dynamic Range:   Passed       146 [>= 128]

Face Area, Eyes, Mouth, and Ears Detection
                 Face Area:  Detected
        Eyes [Right - Left]: Y & Y
                     Mouth:  Y
        Ears [Right - Left]: Y & Y

Quality Examined Result
  D-Score:  GOOD IMAGE [D-QS = 12/12]
  C-Score:  GOOD IMAGE [C-QS = 84/100]

Header Information
                Image Type:  BMP
                Color Bits:  24
              Image Height:  768
               Image Width:  512
                Image Size:  1179702
        Image X-Resolution:  300
        Image Y-Resolution:  300

         Consistency Check:  PASSED
```

FIGURE 4. Example of “Need to Rescan”

FIGURE 4A. Original Image

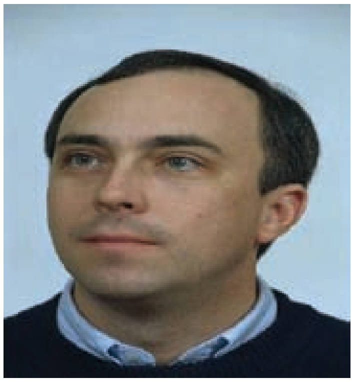


FIGURE 4B. Segmented Image

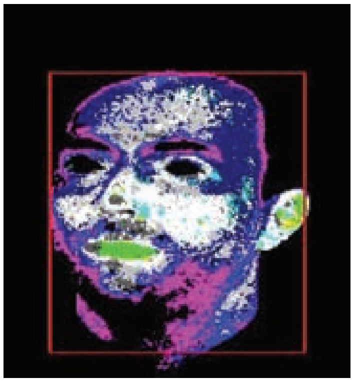


FIGURE 4C. Facial Feature Image

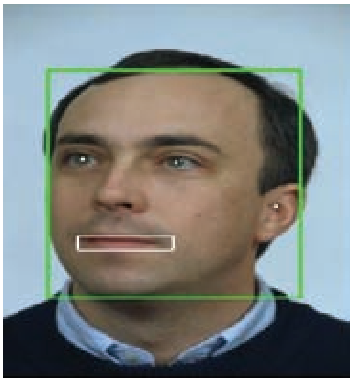
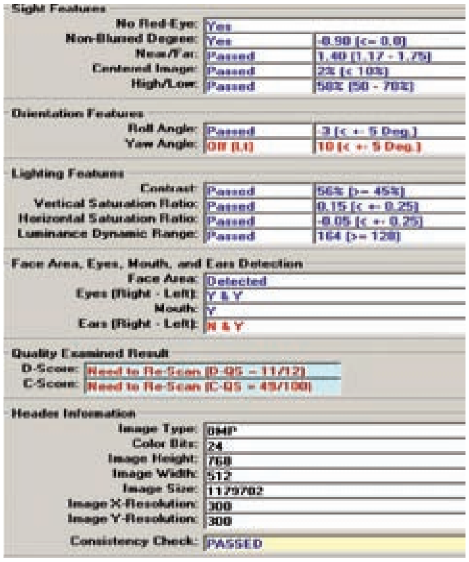


FIGURE 4D. Feature Verification Results



```
Sight Features
                No Red-Eye:  Yes
        Non-Blurred Degree:  Yes          -0.90 [<= 0.0]
                  Near/Far:  Passed       1.40 [1.17 - 1.75]
            Centered Image:  Passed       2% [< 10%]
                  High/Low:  Passed       58% [50 - 70%]

Orientation Features
                Roll Angle:  Passed       -3 [< +- 5 Deg.]
                 Yaw Angle:  Off [L1]     10 [< +- 5 Deg.]

Lighting Features
                  Contrast:  Passed       56% [>= 45%]
 Vertical Saturation Ratio:  Passed       0.15 [< +- 0.25]
Horizontal Saturation Ratio: Passed       -0.05 [< +- 0.25]
  Luminance Dynamic Range:   Passed       164 [>= 128]

Face Area, Eyes, Mouth, and Ears Detection
                 Face Area:  Detected
        Eyes [Right - Left]: Y & Y
                     Mouth:  Y
        Ears [Right - Left]: N & Y

Quality Examined Result
  D-Score:  Need to Re-Scan [D-QS = 11/12]
  C-Score:  Need to Re-Scan [C-QS = 49/100]

Header Information
                Image Type:  BMP
                Color Bits:  24
              Image Height:  768
               Image Width:  512
                Image Size:  1179702
        Image X-Resolution:  300
        Image Y-Resolution:  300

         Consistency Check:  PASSED
```

The sample images in Figure 3A and Figure 4A are adopted from the DoD Counter-drug Technology Program, which sponsored the Facial Recognition Technology (FERET) program and development of the FERET database. NIST is serving as the technical agent for distribution of the FERET database.[2,3]

Using FaceQM as a Conformance Testing Tool for ANSI INCITS 385-2004

Most of the FaceQM tool measurement features are adopted from ANSI INCITS 385-2004. However, the current version of the FaceQM tool does not cover all of the standard's facial image features (for example, eye color, hair color, expression, eyeglasses, and pitch angle), because some of them are difficult to evaluate in the image provided. For example, the pitch angle cannot be evaluated in a two-dimensional frontal facial image, and the detected eye and hair colors may not match the specifications of the standard.

Table 3 lists the requirements of 23 features that are related to the quality of basic full-frontal or token facial images described in ANSI INCITS 385-2004. The last column of

TABLE 3. ANSI INCITS 385-2004 Features Related to Quality Measurement

Facial image type	Requirement type	Name of features	ANSI INCITS 385-2004	Included in FaceQM v 1.0?
Frontal	Scene	Pose	Section 7.2.2 (p. 26)	Yes (pose angle)
Frontal	Scene	Expression	Section 7.2.3 (p. 26)	No
Frontal	Scene	Shoulders	Section 7.2.5 (p. 27)	No
Frontal	Scene	Subject and scene lighting	Section 7.2.7 (p. 27)	Yes (lighting)
Frontal	Scene	Shadows over the face	Section 7.2.8 (p. 27)	Yes (face area detection)
Frontal	Scene	Shadows in eye sockets	Section 7.2.9 (p. 27)	Yes (eyes detection)
Frontal	Scene	Hot spots	Section 7.2.10 (p. 27)	Yes (lighting)
Frontal	Scene	Eyeglasses	Section 7.2.11 (p. 27)	No
Frontal	Scene	Eye patches	Section 7.2.12 (p. 28)	No
Frontal	Photographic	No over- or underexposure	Section 7.3.2 (p. 28)	Yes (lighting)
Frontal	Photographic	Focus and depth of field	Section 7.3.3 (p. 28)	No
Frontal	Photographic	Unnatural color	Section 7.3.4 (p. 28)	No
Frontal	Photographic	Color or grayscale enhancement	Section 7.3.5 (p. 28)	No
Frontal	Photographic	Radial distortion of the camera lens	Section 7.3.6 (p. 28)	Yes (face area detection)
Frontal	Digital	Geometry	Section 7.4.2 (p. 29)	Yes (consistent checking)
Frontal	Digital	Grayscale density	Section 7.4.3.1 (p. 29)	Yes (lighting)
Frontal	Digital	Color saturation	Section 7.4.3.2 (p. 29)	Yes (lighting)
Frontal	Digital	Color space	Section 7.4.3.3 (p. 29)	Yes (consistent checking and lighting)
Full frontal	Photographic	Centered image	Section 8.3.2 (p. 31)	Yes (position)
Full frontal	Photographic	Position of eyes	Section 8.3.3 (p. 31)	Yes (position)
Full frontal	Photographic	Width of head	Section 8.3.4 (p. 31)	Yes (distance)
Full frontal	Photographic	Length of head	Section 8.3.5 (p. 32)	No
Full frontal	Digital	Resolution	Section 8.4.1 (p. 32)	Yes (eyes detection)

the table indicates which components are evaluated in the current version of the FaceQM tool. FaceQM Version 1.0 includes the capability to measure 15 out of 23 components from Table 4. The full-frontal face image type and the token facial image type are the subclasses of the frontal image type and therefore obey all normative requirements of the frontal image type.

TABLE 4. **ANSI INCITS 385-2004 Parameters Tested by the FaceQM Tool**

Category	Feature	Rule	ANSI INCITS 385-2004
Distance	Near/far	$\alpha = W_p/W_h$ $4/7 \leq \alpha \leq 6/7$	Section 8.3.4 (p. 31): The minimum (image width: head width) ratio is 7:4.
Position	Eye position	Center point between the eyes must be located between 50% and 70% of the vertical distance up from the bottom edge of the captured image	Section 8.3.3 (p. 31): An imaginary horizontal line BB through the center of the eyes shall be located between 50% and 70% of the vertical distance up from the bottom edge of the captured image.
Position	Centered image	$\pm W_p \times 0.05$	Section 8.3.2 (p. 31): The approximate horizontal midpoints of the mouth and the bridge of the nose shall lie on an imaginary vertical line AA positioned at the horizontal center of the image.
Pose	Pose–roll	$\theta_R = 0° \pm 5°$	Section 7.2.2 (p. 26): Rotation of the head shall be less than ± 5 degrees from frontal in every direction–up/down, rotated left/right, and tilted left/right.
Pose	Pose–yaw	$\theta_Y = 0° \pm 5°$	Section 7.2.2 (p. 26): Rotation of the head shall be less than ± 5 degrees from frontal in every direction–up/down, rotated left/right, and tilted left/right.
Lighting	Horizontal saturation ratio	Color saturation ratio between left half and right half in detected face area	Section 7.4.3.2 (p. 29): The color saturation of a 24-bit color image should be such that, after conversion to grayscale, there are 7 bits of intensity variation in the facial region of the image.
Lighting	Vertical saturation ratio	Color saturation ratio between upper half and lower half in detected face area	Section 7.4.3.2 (p. 29): The color saturation of a 24-bit color image should be such that, after conversion to grayscale, there are 7 bits of intensity variation in the facial region of the image.
Lighting	Contrast	$45\% \leq \text{Contrast} \leq 95\%$	—
Lighting	Luminance dynamic range	≥ 128	Section 7.4.3.1 (p. 29): The dynamic range of the image should have at least 7 bits of intensity variation (span a range of at least 128 unique values) in the facial region of the image. The facial region is defined as the region from crown to chin and from the left ear to the right ear.

Conclusion

Facial image quality measurement could be determined from facial features. The measurements of the majority of facial features are dependent on the face area detection and the locations of eyes, mouth, and ears. The determined "Good Image" or "Need to Rescan" quality score of each processed facial image could allow an operator to quickly render accept and reject decisions in the field.

The performance of the FaceQM algorithm can be improved through calculation of the quality score with weighting coefficients since different image quality criteria have a differing degree of impact on the matching performance.

This FaceQM algorithm can be used not only to measure quality of facial images, but also to evaluate face recognition matchers, for example, to determine which quality parameter a specific matcher (and its image enhancement utility) is especially sensitive to the matching score.

[1] H. Rossotti, *Color: Why the World Isn't Grey* (Princeton: Princeton University Press, 1983).

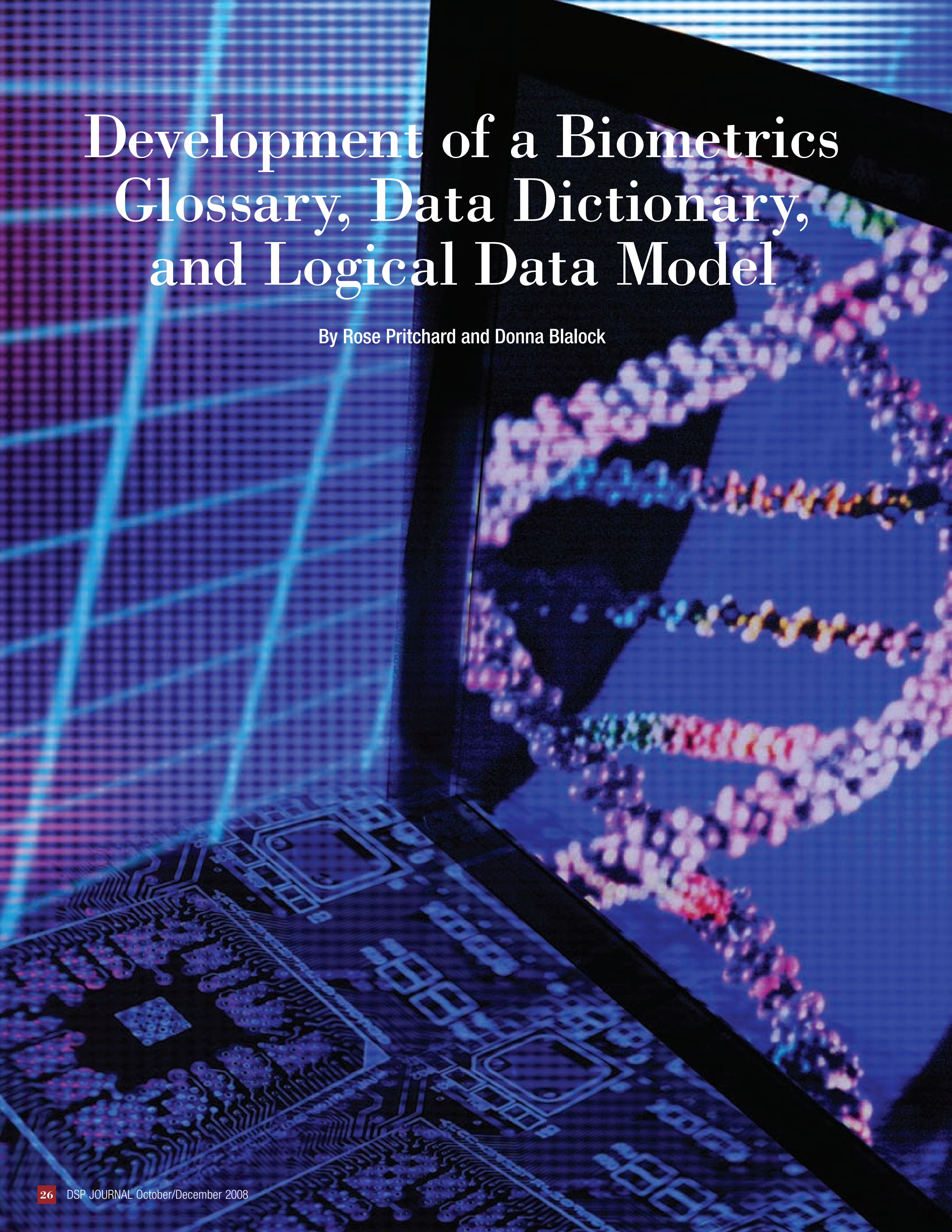
[2] P.J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET Database and Evaluation Procedure for Face Recognition Algorithms," *Image and Vision Computing*, Vol. 16, No. 5 (1998), pp. 295–306.

[3] P.J. Phillips, H. Moon, S.A. Rizvi, and P.J. Rauss, "The FERET Evaluation Methodology for Face Recognition Algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22 (2000), pp. 1090–1104.

About the Authors

Dr. Robert Yen and Gregory Zektser are support contractors and senior subject matter experts on DoD's Biometrics Task Force. Dr. Yen has responsibility for development and assessment of all biometric image quality-related tasks. He has more than 20 years of experience developing real-time imaging systems, including optical/intelligent character recognition, biometric imaging, and medical imaging.

Mr. Zektser's responsibilities and experience include work on biometric standards and test and evaluation. He has over 20 years of experience in various areas of systems engineering, technical standards development, quality management, and biometrics.



Development of a Biometrics Glossary, Data Dictionary, and Logical Data Model

By Rose Pritchard and Donna Blalock

Three essential data products—a glossary, a data dictionary, and a logical data model—are needed to support a key goal of the Biometrics Task Force: define and standardize an architecture that will meet DoD's current and future biometric requirements in support of business and warfighter needs. Together, the three products will help establish and promote a consistent language for the data that are used and exchanged within the DoD community.

Biometrics Glossary

The biometrics glossary was jointly developed to establish an official vocabulary of terms for the DoD biometrics community. Initially published in February 2008 and updated in June and again in August, the glossary provides definitions for the conceptual and operational terms that are commonly used in biometrics discussions and in formal documents such as DoD directives, concepts of operations, and materials required in the Joint Capabilities Integration and Development System process, for example, initial capabilities documents, capabilities design documents (CDDs), and capabilities production documents (CPDs).

Versions of the biometrics glossary were used in the Next Generation Automated Biometric Identification System (ABIS) v1.0 CPD and in support of the initial capabilities development team.

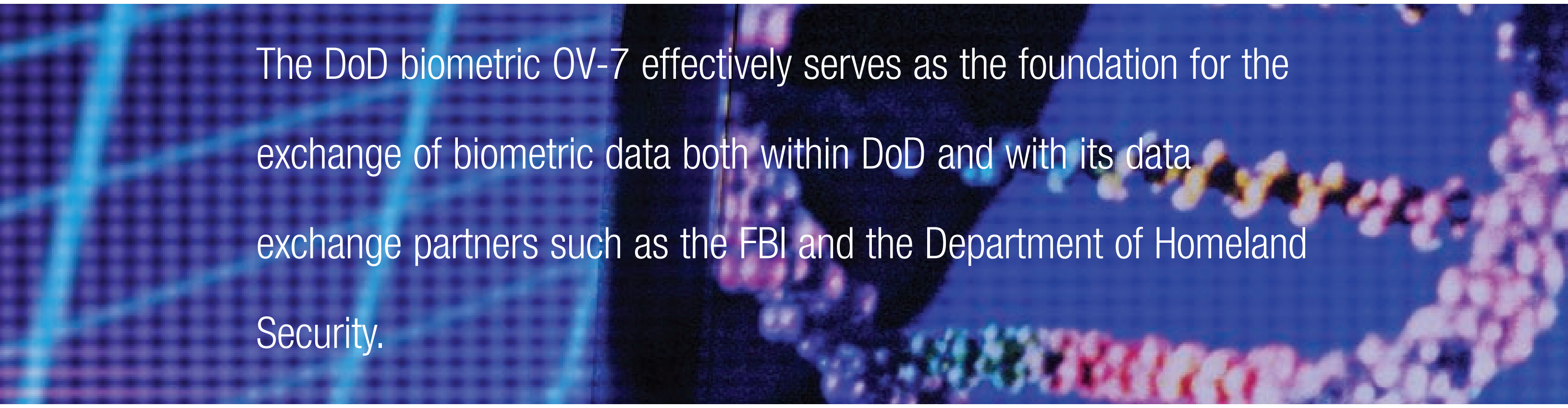
Going forward, the biometrics glossary will be published semiannually, with future editions expected to contribute to documents required for Biometric Enabling Capabilities Milestone B and the Joint Personnel Identity Management System (JPIMS) CDD.

Integrated Data Dictionary

The initial version of the integrated data dictionary for biometrics was published in the fall of 2007. The dictionary contains detailed definitions of the data elements of interest to the DoD biometric community and of the primary attributes or characteristics of the data elements. The dictionary will serve as a reference for members of the DoD biometrics community who have a vested interest in specific data-element-level information (for example, the material developers of the DoD biometric systems) and will help establish consistency across the DoD biometric systems as they interoperate with each other and with other U.S. government and international biometric systems.

The data of the following critical DoD biometric systems were analyzed and used as the basis of the initial integrated data dictionary:

- Automated Biometric Identification System
- Biometrics Automated Toolset
- Biometric Intelligence Repository
- Biometrics Identification System for Access
- Defense Biometrics Identification System
- Detainee Reporting System
- Expanded Maritime Interdiction Operations Tool Set
- Handheld Interagency Identity Detection Equipment
- Next Generation ABIS
- Special Operations Command Jump Kit.



The DoD biometric OV-7 effectively serves as the foundation for the exchange of biometric data both within DoD and with its data exchange partners such as the FBI and the Department of Homeland Security.

Data elements of the in-scope systems have been cross-referenced as an initial step toward identifying current data-sharing deficiencies and will be used to help drive the requirements to resolve them. The integrated data dictionary is also being used to help validate the core biometrics data model.

Logical Data Model

Logical data models, or entity-relationship models, describe the structure of data and the business rules that govern them. The logical data model can represent the concepts of an entity (a concept of interest), an attribute (characteristics of the entity), a relationship (a link between entities), and a domain (the possible values for an entity). In the DoD Architecture Framework (DoDAF), the logical data model is a system's Operational View (OV-7).

In 2007 and early 2008, DoDAF architecture-centric biometric data models were developed. Subsequently, work was done to extract and enhance a core biometric data model from those earlier data models. The core biometric data model was developed in collaboration with various DoD organizations, including Project Manager Biometrics, the Biometric Standards Working Group, the National Ground Intelligence Center, and the Architecture Integration and Management Directorate within the Training and Doctrine Command.

The core model—the DoD biometric OV-7—was integrated with the results of work on the integrated data dictionary. The result is a broadly applicable biometrics information exchange data model.

The DoD biometric OV-7 effectively serves as the foundation for the exchange of biometric data both within DoD and with its data exchange partners such as the FBI and the Department of Homeland Security. By creating consistent data structures, the core biometric data model provides a common schema for data interoperability among DoD systems with a biometric component.

An early version of the core biometric data model was included in the Next Generation ABIS v1.0 CPD. Currently, the core biometric data model is being refined to produce versions that will support specific needs of the biometrics community, including v2.0 of DoD's Electronic Biometrics Transmission Specification, Biometrics Enabling Capabilities Milestone B, and JPIMS CDD.

Conclusion

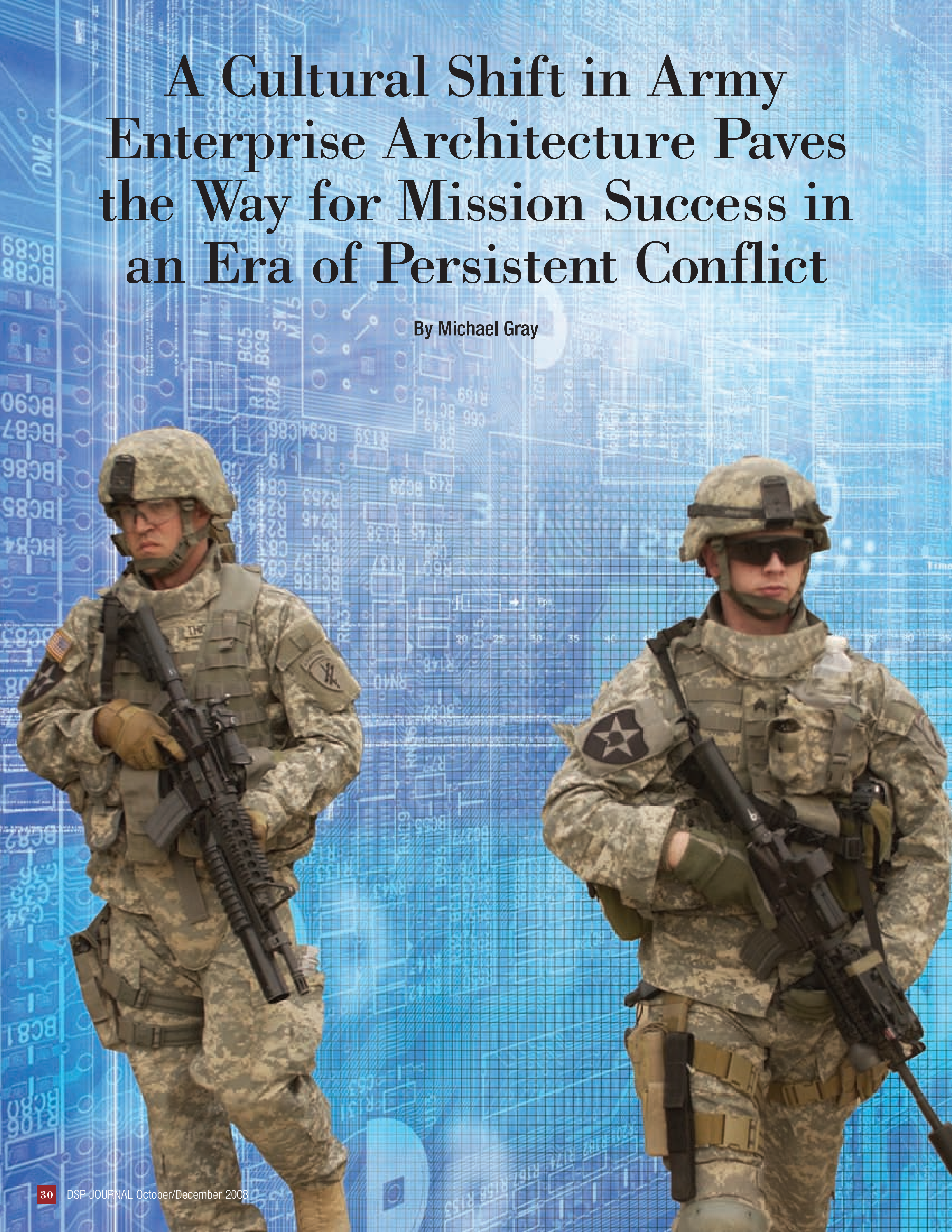
A Biometrics Data Sharing Community of Interest has been formed to be a primary vehicle by which the three essential data products—the biometrics glossary, the integrated data dictionary, and the core biometric data model—will be matured and reviewed by the biometrics community's many partners. Analysis of these products will inevitably identify areas of inconsistency—overlapping and disparate data elements and gaps that will make interoperability between critical in-scope DoD biometrics systems impossible without resolution to establish a common standard. The Community of Interest will provide the forum for members to discuss and resolve issues.

About the Authors

Rose Pritchard and Donna Blalock, support contractors from L-3 Command and Control Systems and Software, represent the Army Net-Centric Data Strategy Center of Excellence. Ms. Pritchard is the project manager of the Biometric Data Team (BDT), and Ms. Blalock is the administrator of the Biometrics Data Sharing Community of Interest (BDS COI). The BDT is responsible for leading the BDS COI and supporting the biometrics data architecture efforts of the Biometrics Task Force.

A Cultural Shift in Army Enterprise Architecture Paves the Way for Mission Success in an Era of Persistent Conflict

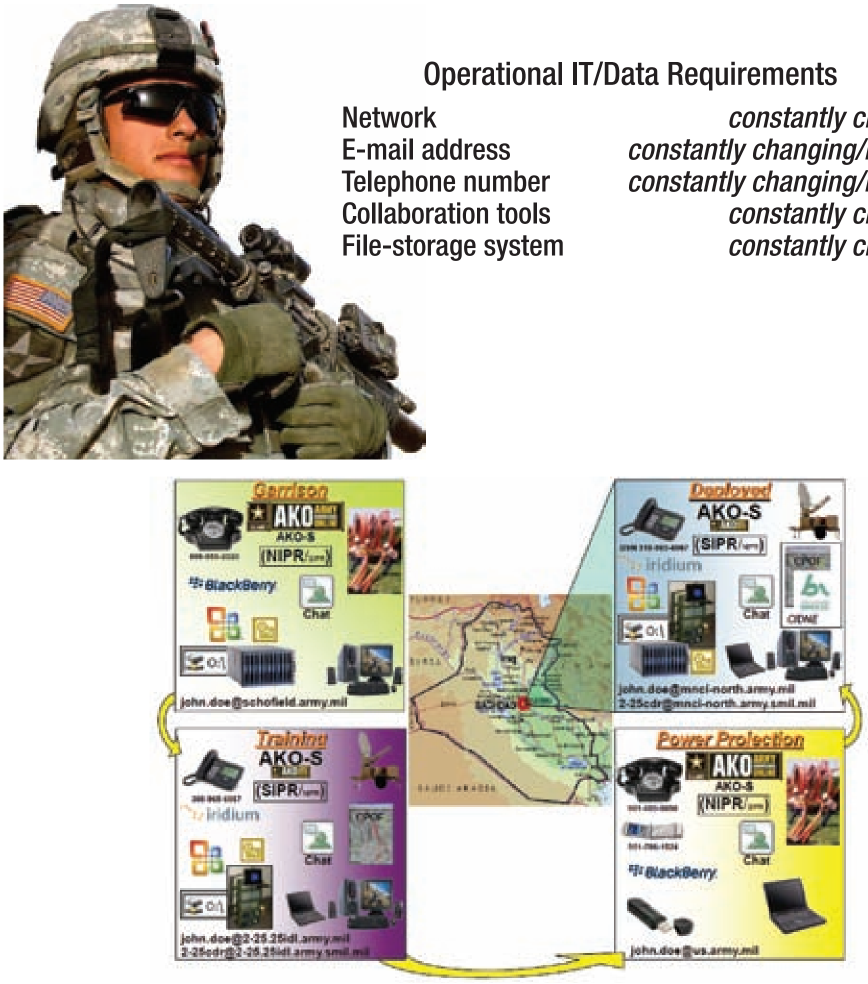
By Michael Gray



In an enterprise the size of the U.S. Army, one of the largest organizations in the world, it is impractical to entertain the idea that a single enterprise architecture (EA) could be used to deliver required results, for example, improved return on investment, greater support for net-centric transformation, and increased collaboration within and among agencies. In this era of persistent conflict, an innovative approach to architecture is needed as an essential enabler to the successful rebalancing of the Army, helping to establish conditions that allow combat power to be projected by Army units in hours or days, versus weeks or months, as was the case for Operation Enduring Freedom and Operation Iraqi Freedom.

The goal of the Army's enterprise architecture is to help adapt Army institutions so that they are supremely capable of supporting a flexible expeditionary force at war. Consider the varying technological needs of soldiers as they transition among varying roles and responsibilities. As depicted in Figure 1, warfighters in today's complex environment require adaptive technologies that can readily support constantly changing networks, collaboration tools, file-storage systems, e-mail addresses, and even telephone numbers.

FIGURE 1. A Soldier's Perspective of Technology Needs across Varying Roles and Responsibilities



Operational IT/Data Requirements

Network	*constantly changing*
E-mail address	*constantly changing/multiple*
Telephone number	*constantly changing/multiple*
Collaboration tools	*constantly changing*
File-storage system	*constantly changing*

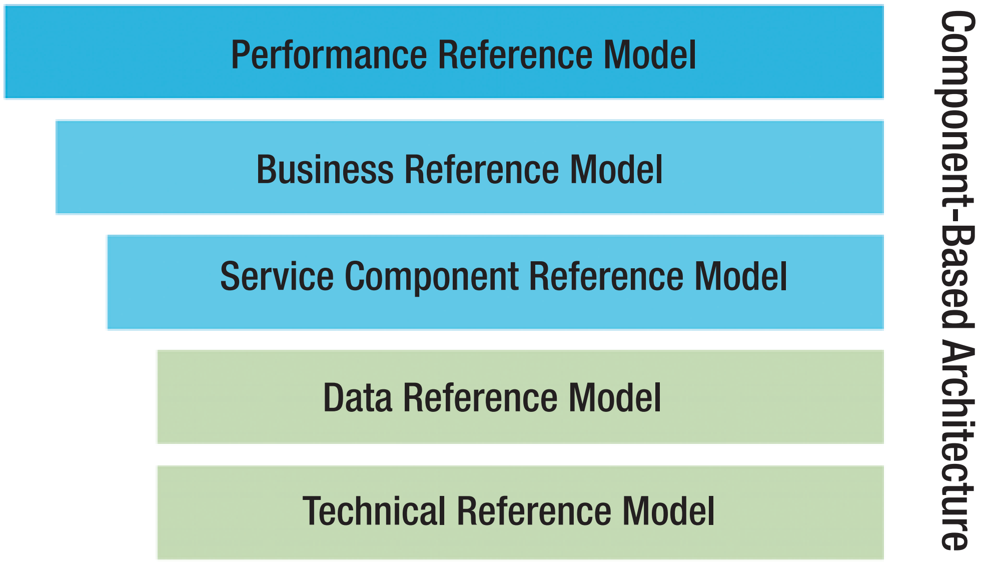
The complexity and dynamic nature of the Army requires the use of modern architectural approaches that enable efficient and effective transformation. Important decisions about programs, capabilities, and related expenditures often hinge on architectural concepts. And the architecture community must be able to deliver the right information, on demand with timely response, to support decision makers. This challenge is magnified by the absolute necessity of the Army to define its enterprise in the context of a DoD enterprise, including joint interagency, intergovernmental, and multinational mission partners.

Regardless of the Army's enormous size and unique characteristics, an enterprise perspective is needed to support tactical and strategic decision making. To establish the enterprise perspective in a pragmatic way, the Army has adopted and is adapting several best-practice methods from government and industry organizations. Key methods are the reference model approach from the Federal Enterprise Architecture (FEA) and the "bricks-and-patterns" concept developed by Gartner, Inc. The reference models, together with the Gartner bricks and patterns, will contribute to a better understanding of the demand for, and supply of, Army information technology (IT) services.

Reference Models

The Army is adapting the FEA reference models (see Figure 2) to create a standardized approach to managing its IT portfolio. By taking this approach, the Army expects to significantly reduce or avoid costs, as well as achieve greater IT performance, by eliminating duplicative investments and improving information-sharing capabilities. These results are possible because the reference models will provide a common language and framework that the IT acquisition, resource management, and force modernization communities across the Army can use to describe and analyze technology investments.

FIGURE 2. FEA Reference Models


Performance Reference Model
Business Reference Model
Service Component Reference Model
Data Reference Model
Technical Reference Model
Component-Based Architecture

The Army's reference models describe the relationships among major components of Army organizations, particularly the IT investments required to enable the business functions that drive the execution of the organization's mission. The models and their roles are as follows:

- Performance Reference Model (PRM)—defines performance objectives and metrics for each Army line of business
- Business Reference Model (BRM)—establishes business objectives and requirements to meet the performance goals for each Army line of business
- Service Component Reference Model (SRM)—defines applications and services that enable Army business requirements and data sharing/data exchanges
- Data Reference Model (DRM)—describes data that support the Army's business requirements
- Technical Reference Model (TRM)—identifies technologies that support and enable Army applications and service components.

One of the primary benefits of reference models is that they provide enough detail to characterize IT and other investments from an enterprise level without having to go through the resource-intensive process of developing an integrated architecture. Another key benefit is that the models provide a structure by which the Army can organize, federate, and segment its enterprise architecture—an approach that is endorsed by the Office of Management and Budget and has proven to be effective for large organizations.

As part of this approach, the Army is shifting its focus from more traditional architecture views to a perspective that focuses on the outputs that the architecture community's customers require to ensure the delivery of the right capabilities to support warfighters and mission success in a cost-focused culture. Program planning, budgeting and budget execution, force management, portfolio management, acquisition, and modeling and simulation are examples of the types of customer requirements that will be the focus of the architecture community.

Today, the provision and management of the Army's IT services are decentralized. However, through the judicious implementation of reference models and other best practices, the Army will be able to synchronize activities more effectively and thus deliver consistently reliable output-focused IT capabilities and enterprise services at reduced cost and greater speed. Moreover, investment decisions will be supported by higher quality and more timely analysis. At the same time, reference models will enable the Army to more precisely articulate and synchronize the design, engineering, and delivery of sustainable and measurable IT capabilities based on a thorough understanding of the demand for these capabilities.

Adopting this output- and demand-based approach to IT acquisition and development represents a major cultural shift. However, this approach is required to most effectively and efficiently implement advanced enterprise-wide initiatives such as the LandWarNet global construct and its Network Service Center. The center aims to, for example, horizontally and vertically integrate and coordinate global network enterprise assets, displacing the current networking scenario, which is marked by stove-piped implementations. Such implementations result in inconsistent capabilities across the Army and significantly hamper the agility and speed with which units are able to deploy and apply combat power. The concept is to permit any brigade combat team, and any soldier, to plug in to the network enterprise, anytime and anywhere, and to use a common set of enterprise services.

Bricks and Patterns

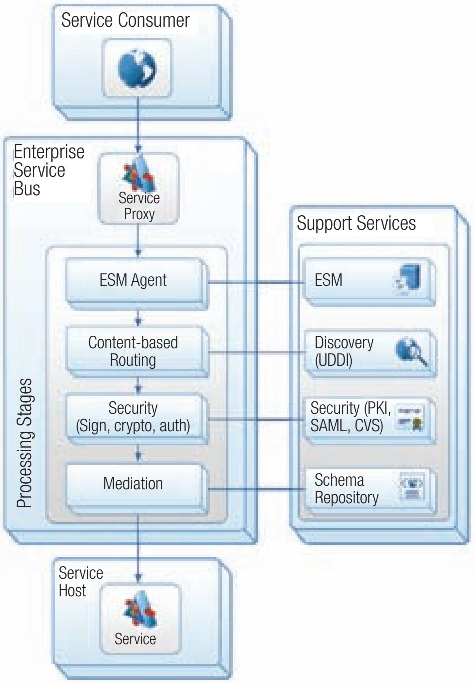
The bricks-and-patterns concept views bricks as the core technology building blocks of an enterprise, and it views patterns as the logical technology models. In other words, bricks are the underlying technologies that are common across multiple services and capabilities, and patterns are repeating elements that can be used across wide-ranging capabilities. For example, an Identity Management pattern would support information assurance efforts cutting across a large number of capabilities. Recognizing that a pattern is a logical model, the bricks-and-patterns concept includes specific physical model configurations for how a pattern is actually implemented.

Reference models can aid in the identification of bricks and patterns in two primary ways:

- Reference models can help identify areas that would benefit from being patterned—a pattern is useful only if it can be reused—by decomposing capabilities into business functions, services, data, technologies, and standards. Only then can areas of potential reuse be identified. Figures 3 and 4 are example patterns. As the figures illustrate, patterns provide only a very high-level, conceptual view of several technology components; they do not provide details about the architecture of the systems using the patterns.
- Reference models can help identify the reusable, individual technology building blocks referred to as bricks. The brick format is used to describe the current, near-term, and long-term requirements for a specific technology component of the enterprise. The brick illustrated in Figure 5, for example, describes enterprise service bus (ESB) capabilities.

The alignment of investments to the TRM (discussed below) will identify those technologies and standards that are common across multiple capabilities and that would yield benefits from standardization and the economies of scale possible in enterprise-wide pur-

FIGURE 3. Example Service Proxy Technical Pattern

ESB: Service Proxy Technical Pattern	Owner: CERDEC Version: 0.7 08.20.2008
 Service Consumer Enterprise Service Bus Service Proxy Processing Stages ESM Agent Content-based Routing Security (Sign, crypto, auth) Mediation Support Services ESM Discovery (UDDI) Security (PKI, SAML, CVS) Schema Repository Service Host Service	**Description** An ESB can host a proxy that is called by the consumer. The proxy performs additional preprocessing of the request message before calling the service and postprocessing of the responses. Routing decisions can be made in the ESB to determine the appropriate service instances. The proxy can mediate between XML dialects using an XSLT repository. The ESB can apply security policies. Service monitoring (ESM) can be applied to existing services.
	Benefits Service location is transparent. Security policy enforcement is centralized. Storage and distribution of XML schemas and transformations are centralized. Information is enriched. System policies are centralized once they are migrated to foundation.
	Limitations Performance may be negatively affected. Lack of standards for ESB features can lead to vendor-specific solutions. Registry entries for the service should only refer to the proxy; only the bus should use the actual service. Consumers must be modified to include information needed for security policy and other decisions.
Recommended Usage	**References**
Integrate services with SOA foundation capabilities. Expose data and features of ERP and legacy systems as services. Strengthen security for existing services. Translate existing services to common schemas.	Web services pattern. ESM pattern. Discovery pattern. Schema repository.

Notes: CERDEC = Communications-Electronics Research, Development, and Engineering Center, ERP = enterprise resource planning, ESM = enterprise service monitor, SOA = service-oriented architecture, XML = Extensible Markup Language, XSLT = Extensible Style Language Transformations.

chasing. The logical patterns and physical configurations, together with the supporting bricks, will be critical to delivering capabilities via system-of-systems and family-of-systems capabilities.

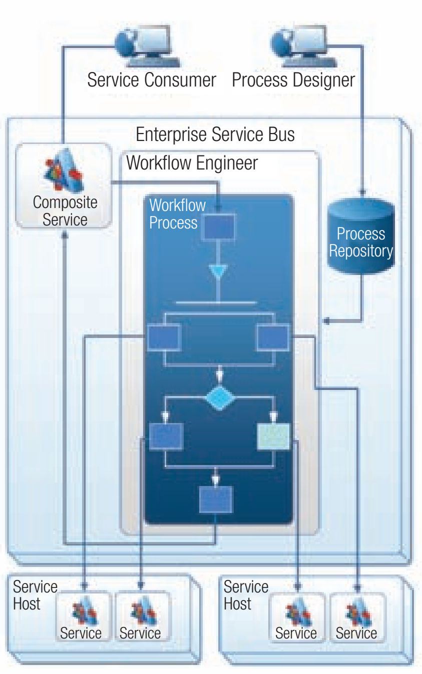
Overview of the Army's Reference Models

Through the use of reference models and of bricks and patterns, the Army's IT community can gain a valuable understanding of what the demand and supply factors are and how those factors should influence enterprise IT investments. Below is a brief introduction to the Army's BRM, DRM, and TRM (Army adaptations of the FEA's PRM and SRM are in development).

FIGURE 4. Example Service Orchestration Pattern

ESB: Service Orchestration Pattern

Owner: CERDEC Version: 0.7 08.20.2008



Description

Orchestration is an ESB feature that helps to create new capabilities by combining existing services. Service outputs are mediated into common schemas and combined into the composite response. Sequencing often uses workflow constructs (processes) that can include human interactions. Workflow is defined using BPEL Process Designer.

Benefits

Smaller general-purpose services can be developed.
Composite services can be rapidly developed with minimal coding.
Workflow in ESB is easier to monitor and control.
Robustness can be added, and error handling can be improved for existing services.

Limitations

Multiple services may have multiple security policies to be merged.
New development, debugging, and testing environments are needed.
Performance may be negatively affected.

Recommended Usage

Enrich information by using multiple sources.
Build human-machine coordinated process flows.
Rapidly develop composite applications or composite services.

References

Service proxy pattern.
BPM pattern.

Notes: BPEL = Business Process Execution Language, BPM = business process management.

ARMY BUSINESS REFERENCE MODEL

The Army BRM will be used to help define Army business areas and to prioritize them based on the need to focus, organize, and manage the different Army transformational efforts from an enterprise perspective. In line with that goal, the Army BRM is organized into three business areas: Battle Command, Generating Force Enterprise Activities, and Global Network Enterprise Construct (see Figure 6).

The Army's EA Federation Model provides an overarching structure that represents the top level of the Army BRM. The development of the Army EA Federation Model and the identification of lines of business within each business area were driven primarily by Army Field Manual 3.0 (*Operations*), the DoD BRM, and the Joint Capability Areas. Emphasis was placed on the field manual because it is Army specific. The subfunctions of each line of business were drawn from Army regulations, field manuals, and architectures.

The Army's EA Federation Model has three primary levels—enterprise, business areas

FIGURE 5. Example Enterprise Service Bus Capabilities Brick

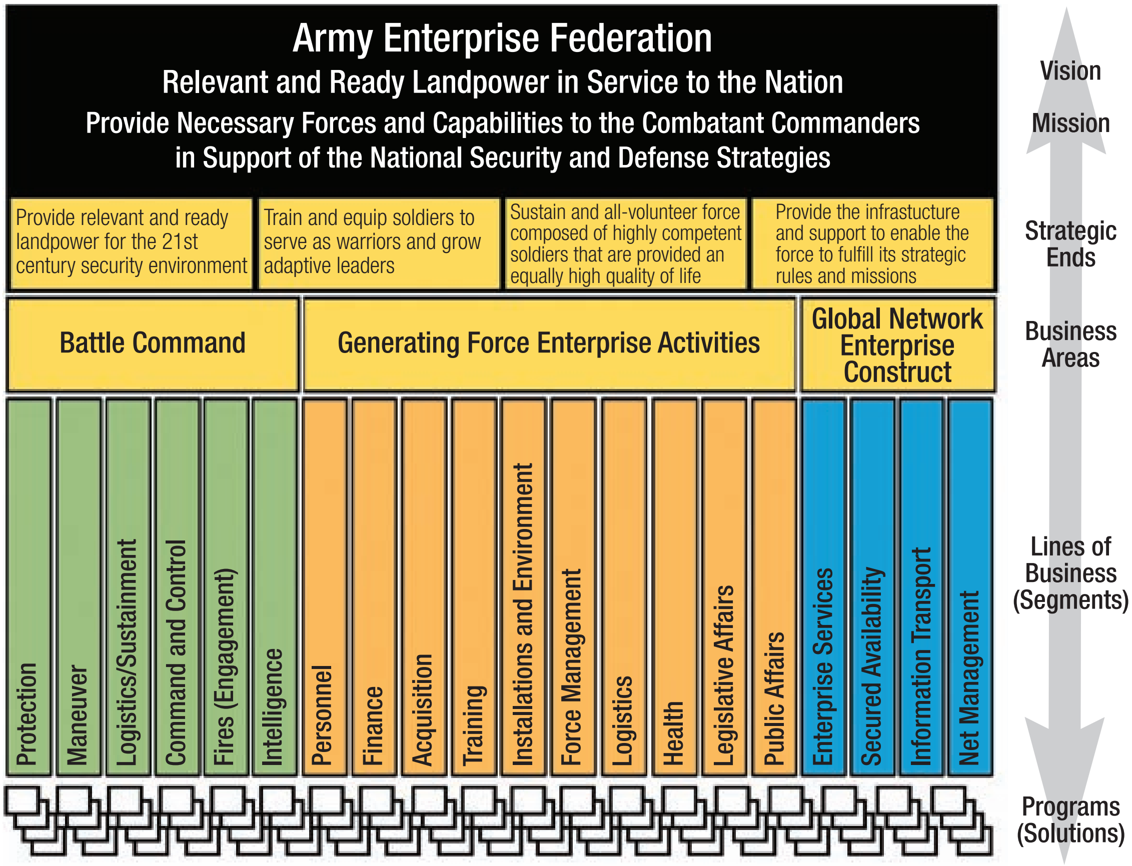
<table>
<tr><td>ESB: ESB Capabilities Brick</td><td colspan="2">Owner: CERDEC Version: 0.7 08.20.2008</td></tr>
<tr><td>Current</td><td>Near Term (0–2 years)</td><td>Long Term (3–5 years)</td></tr>
<tr><td>Mainstream
NCES security
Variety of COTS and open source products
Adapters for mainstream ERP systems
Support for common messaging protocols and systems</td><td>Mainstream +
SAML security, DoD PKI
Homogenous federation
External coprocessing (XML, security)
External foundation (ESM, UDDI, security)
Enterprise, tactical, development versions
Army DDS publish-subscribe
Adapters for Army systems and protocols</td><td>Mainstream + near-term +
DoD security
Interproduct federation
Java-Windows integrated bus
Joint and coalition federation</td></tr>
<tr><td>Retirement</td><td colspan="2">Mainstream</td></tr>
<tr><td>Army needs to negotiate enterprise licensing for COTS ESB and then retire existing ESBs from other vendors.
Army is migrating to SOA with web services as preferred implementation; other service protocols (CORBA, DCE, NIS) should be retired.</td><td>Service proxy (message processing and routing)
Service orchestration
XML processing (validation, transformation, mediation, compression)
Communication (MXP, web services, transport protocols, routing, addressing)
Management and administration (console, services, ESM, governance)</td><td>Quality of service (clustering, load balancing, failover, scalability)
Security
Service registration and discovery
Adapters (ERP, RDBMS, MOM)
BPM (design, workflow, monitoring, reporting, escalation)
Extensibility (customization, federation)</td></tr>
<tr><td colspan="2">Containment</td><td>Emerging</td></tr>
<tr><td colspan="2">Third-party middleware (message brokers)
COM, DCOM, RMI
REST</td><td>Use of BPM for orchestration
Integration with metadata repository
Runtime governance
ESB functionality for MS.net</td></tr>
<tr><td colspan="3">Implications and Dependencies</td></tr>
<tr><td colspan="3">Using an ESB implies that many requirements are delegated to the bus, and it becomes an integral component in the system architecture.
Using an ESB incurs performance impacts and delays between consumer and provider.
ESB features may be realized using multiple products from separate vendors.</td></tr>
<tr><td>Key Patterns</td><td colspan="2">Key Principles/Rationale</td></tr>
<tr><td>Proxy and orchestration
Legacy and ERP integration
Message exchange patterns</td><td colspan="2">An ESB has several features that implement the SOA; purchasing a COTS ESB improves the chances of the features being well integrated.
An ESB enables loose coupling, service location transparency, and continuity of operations.</td></tr>
</table>

Notes: COM = Component Object Model, CORBA = Common Object Requesting Broker Architecture, COTS = commercial off-the-shelf, DCE = Distributed Computing Environment, DCOM = Distributed Component Object Model, DDS = data distribution service, MOM = message-oriented middleware, MXP = MUD Extension Protocol, NCES = Net-Centric Enterprise Services, NIS = Network Information Service, PKI = public key infrastructure, RDBMS = relational database management system, REST = representational state transfer, RMI = remote method invocation, SAML = Security Assertion Markup Language, UDDI = Universal Description, Discovery and Integration.

and lines of business (segments), and programs (solutions)—and is consistent with *FEA Practice Guidance*, published by the FEA Program Management Office in December 2006:

- The enterprise level of the Army's EA Federation Model is primarily focused on providing the structure, policies, and guidance needed to direct the Army's architecture development. It is aligned with the domain and program levels.

FIGURE 6. Army Business Reference Model


Army Enterprise Federation
Relevant and Ready Landpower in Service to the Nation
Provide Necessary Forces and Capabilities to the Combatant Commanders in Support of the National Security and Defense Strategies
Provide relevant and ready landpower for the 21st century security environment
Train and equip soldiers to serve as warriors and grow adaptive leaders
Sustain and all-volunteer force composed of highly competent soldiers that are provided an equally high quality of life
Provide the infrastucture and support to enable the force to fulfill its strategic rules and missions
Battle Command
Generating Force Enterprise Activities
Global Network Enterprise Construct
Protection
Maneuver
Logistics/Sustainment
Command and Control
Fires (Engagement)
Intelligence
Personnel
Finance
Acquisition
Training
Installations and Environment
Force Management
Logistics
Health
Legislative Affairs
Public Affairs
Enterprise Services
Secured Availability
Information Transport
Net Management
Vision
Mission
Strategic Ends
Business Areas
Lines of Business (Segments)
Programs (Solutions)

- The business area and line of business (segment) level may extend the structure, policies, and guidance needed to meet specific needs, but the core concepts must remain consistent to provide alignment and traceability among the levels of the Army's EA Federation Model.
- The program level will be developed and maintained by the respective program offices. Each program/solution set is constrained by the domain segment it supports and by the structure, policies, and guidance provided by the domain and enterprise levels.

ARMY DATA REFERENCE MODEL

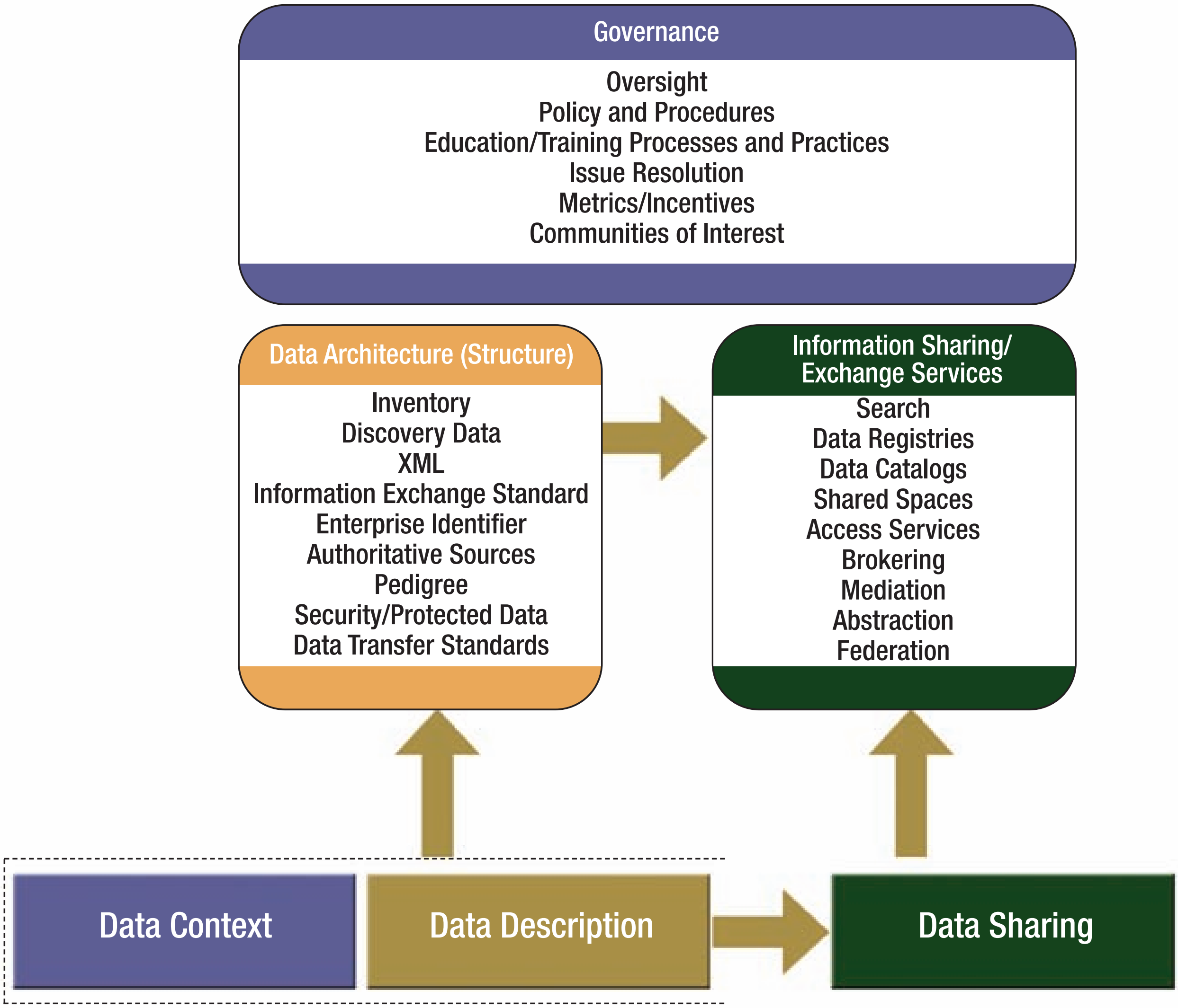
The Army DRM (see Figure 7) is designed to help ensure the alignment of the Army's data strategy within the Army and across DoD. The DRM employs three standardized categories—data context, data description, and data sharing—to describe data characteristics and facilitate the reuse and sharing of data. Using the Army DRM helps promote the use of consistent data management practices, facilitates communication among communities of interest, and better enables wide-ranging organizations to establish common ground on architectural issues.

The Army DRM supports the seven data goals of the DoD net-centric data strategy:

- Make data visible
- Make data accessible
- Institutionalize data management
- Enable data to be understandable
- Enable data to be trusted
- Support data interoperability
- Be responsive to user needs.

The Army DRM also documents how the Army plans to implement its net-centric data strategy in part via an Army Data Services Layer enabled by service-oriented architecture (SOA). The Army expects that SOA will enable the Army DRM through the use of authoritative data sources, information exchange standard specifications, Extensible

FIGURE 7. Army Data Reference Model



Markup Language (XML), and enterprise identifiers. SOA strategies and tenets support the following shifts in data-sharing philosophies:

- *From ownership to stewardship.* Data producers no longer hold tightly to their data, nor do they use it only for predetermined needs. Instead, they expose and publish data to the enterprise to benefit unanticipated needs and other users in the enterprise.
- *From need-to-know to right-to-know.* Data consumers, once authorized, can access enterprise data to obtain information critical to carrying out their responsibilities.
- *From systems to services.* Instead of building data-gathering and data-processing capabilities as hardware boxes and packaged applications, the enterprise is developing loosely coupled, reusable, and standards-based services.
- *From stove-pipes to enterprise-wide access.* Rather than maintaining data in silos and behind proprietary interfaces, the data-sharing infrastructure is built to enable data access and delivery across an enterprise information environment supported by enterprise-wide network resources.
- *From programs to portfolios.* From the governance perspective, the buildup of data-centric capabilities is not just the responsibility of individual acquisition programs. Instead, it also requires increased oversight and management as an enterprise-wide IT services portfolio.

By implementing these concepts, the Army can attain a comprehensive vision for sharing information across the enterprise.

ARMY TECHNICAL REFERENCE MODEL

The TRM uses a hierarchical categorization—service areas, service categories, and service standards—to describe the technologies and standards used to develop and deliver service components. In turn, these service components, which will be defined in the SRM, may be leveraged in the SOA and can also help deliver economies of scale via the identification of superior solutions that can be reused across agencies.

The Army TRM identifies the framework and standards that support the development and implementation of service components. As a result, the Army TRM helps guide and equip acquisition program managers with the tools they need to manage their resources more efficiently and effectively.

The four service areas in the Army TRM are service access and delivery, service platform and infrastructure, component framework, and service interface and integration (Figure 8). The terms and definitions of the Army TRM are the same as those of the FEA TRM. In addition, the Army has added several categories, which are highlighted in red on the figure.

FIGURE 8. Army Technical Reference Model

Service Access and Delivery

Access Channels
- Web browser
- Wireless/PDA
- Collaboration communications
- Other electronic channels

Delivery Channels
- Internet
- Intranet
- Extranet
- Peer to peer
- Virtual private network

Service Requirements
- Legislative/compliance
- Authentication/single sign-on
- Hosting

Service Transport
- Supporting network services
- Service transport

Service Platform and Infrastructure

Supporting Platforms
- Wireless/mobile
- Platform independent
- Platform dependent

Network Operations
- Network management
- Service-level management
- System management

Database/storage
- Database
- Storage

Delivery Servers
- Web servers
- Media servers
- Application servers
- Portal servers

Software Engineering
- Integrated development environment
- Software configuration management
- Text management
- Modeling

Hardware/infrastructure
- Servers/computers
- Embedded technology devices
- Peripherals
- Wide area network
- Local area network
- Network devices/standards
- Video conferencing
- Radio communications
- Satellite communications
- Voice communications

Component Framework

Security
- Certificates/digital signature
- Supporting security services
- Information assurance

Presentation/interface
- Static display
- Dynamic server-side display
- Content rendering
- Wireless/mobile/voice

Data Management
- Database connectivity
- Reporting and analysis

Business Logic
- Platform independent
- Platform dependent

Service Interface and Integration

Integration
- Middleware
- Enterprise application integration

Interoperability
- Data format/classification
- Data types/validation
- Data transformation

Interface
- Service discovery
- Service description/interface

Note: Terms highlighted in red are specific to the Army TRM; the remaining terms are the same as those in the FEA TRM.

The Way Ahead

Once the key components of the Army's new approach are in place, the Army will have the structure, processes, and governance it needs to provide an effective enterprise perspective, implement appropriate guidance and constraints through each level of architecture development, and improve its ability to meet the ultimate objective of supporting warfighters and decision makers. To help establish and implement the new approach to architecture, the Army's chief enterprise architect is focusing on the following activities:

- *Baselining enterprise reference models.* This activity will establish an enterprise perspective, provide alignment of the Army EA to the DoD and federal levels, and provide a framework for domain segments to extend the structure, policies, and guidance required to meet specific needs.

- *Developing a method for enterprise transformation.* This activity will provide a well-orchestrated and deliberate process for identifying priorities and architecture initiatives. It also will develop products to support decision makers.
- *Ensuring SOA foundation governance and architecture compliance.* This activity will provide methods and automated tools to help determine the SOA compatibility of applications and the compliance of architectures to the DoD level (for example, the Business Transformation Agency's Business Enterprise Architecture), as well as to the federal level.
- *Assisting with the development of the LandWarNet battle command capability set.* This activity will use the Army's new method for enterprise transformation to provide a consistent process for building the capability sets and reference models needed to consistently decompose capabilities and align programs.

Using effective EA methods to execute these four activities will enable the Army to harness the power of its vast information resources to deliver vital capabilities to warfighters. By helping to derive the most value possible from any given IT investment, the Army's architecture efforts are critical; they directly affect the efficiency and effectiveness of the entire Army. As a result, the Army's architecture community is committed to ensuring that its contributions are relevant to stakeholders and decision makers across all of the Army's organizations.

About the Author

Colonel Michael Gray is chief of the Enterprise Architecture Division within the Army Architecture Integration Center, a component of the Office of the Chief Information Officer/G-6, Headquarters, Department of the Army.

References

Defense Information Enterprise Architecture
http://www.defenselink.mil/cio-nii/sites/diea/

The Defense Information Enterprise Architecture (version 1.0) provides a common foundation to support accelerated DoD transformation to net-centric operations. It presents the vision of net-centric operations and establishes near-term priorities to address critical barriers that must be overcome to achieve the vision.

Federal Enterprise Architecture
http://www.whitehouse.gov/omb/egov/a-1-fea.html

The Federal Enterprise Architecture, being developed by the Office of Management and Budget, is a business-based framework for government-wide improvement. It is intended to transform the federal government to one that is citizen centered, results oriented, and market based.

Gartner, Inc.
http://www.gartner.com/

Gartner is a leading IT research and advisory company providing consulting services to help organizations use and manage information technology to enable business performance.

Program News

Topical Information on Standardization Programs

Awards Recognize the DMSMS Efforts of Individuals and Teams

On September 23, 2008, **Gregory Saunders**, Director, DSPO, and **Alex Melnikow**, Chair, DoD Diminishing Manufacturing Sources and Material Shortages (DMSMS) Working Group, presented 10 awards to recognize individuals and teams whose efforts demonstrably promoted tool development, management procedures, and policies related to DMSMS.

Special Recognition Awards

Kelly Gibson—Life-Cycle Logistics, Marine Corps Systems Command, Quantico, VA—was recognized for her outstanding vision and commitment to DMSMS management within the United States Marine Corps (USMC). She became the project manager for a contracted study on the state of DMSMS within USMC ground systems. She implemented the recommendations for DMSMS training and the creation of the first USMC DMSMS working group to address DMSMS policy and procedures. She helped establish the requirement that the DMSMS management plan be a mandatory part of independent logistics assessments. Ms. Gibson's vision enabled the development of the USMC Shared Data Warehouse module to help monitor and process DMSMS cases. Because of her contributions, the USMC is now enabled to proactively manage DMSMS.

The **DMSMS Training Development Team**—consisting of government and industry subject matter experts and leaders—received special recognition for its development of DMSMS management training for DoD. The team is a model of what can be accomplished when government agency and industry barriers are bridged. From the initial development of the memorandums of agreement, to the development of the instructor-led and computer-based training materials, the team worked together. As a result, the first DMSMS training courses were developed, critiqued, debuted, and then made available to government and industry through the Defense Acquisition University's Continuous Learning Center website and through instructor-led offerings. Before this training was developed, there were only a few knowledgeable DMSMS personnel in the country. Now, more than 4,100 people have been trained in the fundamentals and advanced techniques of proactive DMSMS management.

Individual Achievement Awards

David Robinson—DMSMS and Generalized Emulation of Microcircuits (GEM) Program, Defense Supply Center Columbus, OH—was recognized for his outstanding contributions to DMSMS management. His efforts are highlighted by the development of the Shared Data Warehouse, establishment of GEM as a possible source for DMSMS microcircuits, advancement of commonality efforts with Security Assistance and Foreign Military Sales programs, and general support of the Defense Logistics Agency (DLA) and DoD DMSMS communities. His knowledge of DMSMS helped win permission to establish a DLA DMSMS Council and to pursue the establishment of a DLA DMSMS Enterprise, with great benefit to both DLA and DoD activities. Mr. Robinson is always sought out to help resolve DMSMS issues at the policy, system, and commodity levels of management.

Samuel Calloway—F-15 System Program Office, Robins Air Force Base, GA—was recognized for his outstanding achievements in supporting the F-15 fighter. His comprehensive approach, development of tools, refinement of bills of materials, and other activities have ensured that F-15 avionics were free of DMSMS impediments. Some of his efforts have led to studies to implement portions of his program at the DoD level, such as gathering depot repair data for all DoD systems. He also set up the DoD/Raytheon Airborne Radar Sustainment Team to address common DMSMS component problems in military airborne radars. A leader within the DMSMS community, Mr. Calloway's concepts and methods are often used as an example of how to successfully mitigate DMSMS within a system.

William Pumford—Government-Industry Data Exchange Program (GIDEP), Corona, CA—has been instrumental in facilitating the sharing of DMSMS information between industry and DoD DMSMS communities. He helped establish the DoD central repository for DMSMS information and helped standardize the receipt and distribution of DMSMS notices from industry and DoD sources. He has participated on service and DoD DMSMS working groups as a trusted advisor to help resolve issues of information dissemination. Most recently, in concert with industry, he has been involved in the development of a metrics reporting tool and obsolescence data repository to help capture both metrics and solutions to be shared by anyone with a GIDEP user identification and password. Mr. Pumford's efforts have helped to ensure that the DMSMS community has the information it needs to resolve DMSMS issues before they affect readiness or increase life-cycle costs.

Walter Tomczykowski—Life Cycle Management, ARINC, Inc., Annapolis, MD—was recognized for his exceptional 20-plus years of contributions to solve DMSMS issues. These experiences helped him develop the DMSMS Program Managers Handbook, Cost Metrics, and Acquisition Guidelines. These documents became the core of the DoD DMSMS guidebook (SD-22), which he helped establish. Along with sharing guidance, he helped develop DMSMS cost models and helped pioneer the initial DMSMS teaming group. Mr. Tomczykowski is a recognized subject matter expert that helps DoD and industry plan ahead to mitigate DMSMS issues. Without his significant contributions, much of what we now take for granted in DMSMS management might not be available.

Team Achievement Awards

The **AEGIS Weapon System DMSMS Working Group**, established in 1992, continuously improves its integrated processes to derive innovative solutions for difficult DMSMS issues. The result is maximized cost avoidance and minimized production and fleet support issues. The group started out as a production DMSMS activity to ensure that contracted AEGIS deliveries would not be affected by obsolescence issues. Today, the group is an integrated activity of production and life-cycle DMSMS teams, encompassing AEGIS original equipment manufacturers (OEMs) and Navy agencies working collaboratively. In 2006, the Deputy Assistant Secretary of the Navy (Logistics), Nicholas Kunesh, stated that the AEGIS Weapon System process was one of the "best of breed" to be emulated by others. Since its inception, the working group has resolved 4,131 DMSMS issues with a benefiting cost avoidance of $342.3 million.

The **B-1 System Program Office Reliability and Maintainability Analysis (R&M)/DMSMS Team**, located at Tinker Air Force Base, OK, established a robust DMSMS process that, in the past 18 months alone, has resulted in a cost avoidance of approximately $28 million. The team is diverse, with personnel from the government program office, OEM, contractor, engineering, and logistics. The team gathers data relating to the reliability, supportability, and maintainability of systems, subsystems, line replaceable units, and shop reparable units. In addition, the team has the entire bill of material for the B-1 loaded into the GIDEP database and AVCOM (an obsolescence management tool), and it actively monitors all 105,000 OEM part numbers and 99,000 national stock numbers for DMSMS alerts.

F/A-18E/F Integrated Readiness Support Teaming (FIRST)—a program that provides performance-based logistics (PBL) support related to the Navy's Super Hornet, with a focus on obsolescence management—realized a cost avoidance of some $33 million in the 7 years since it was initiated. Moreover, there has not been a single instance of a "not mission capable supply" Super Hornet due to an obsolescence issue since the aircraft was introduced in 1999. FIRST is a joint arrangement between The Boeing Company, Naval Inventory Control Point (NAVICP) Philadelphia, and suppliers of unique F/A-18E/F Super Hornet equipment. The FIRST PBL program includes funds to pursue alternate parts or last-time buys when justified by business case analyses. With such funding in place, FIRST can react rapidly when last-time buys are mandated, thus avoiding the more costly option of a redesign. The FIRST program has become a benchmark for other DoD programs.

Personnel from BAE Systems/Manufacturing Technology, Inc., and Karta Technology, Inc., constitute a **Space and Command, Control, Communications, and Information (C3I) DMSMS Support Team**. The team has made great strides in obsolescence management and has provided the government with the benefit of substantial cost avoidance and return on investment for space and C3I systems. The team provides DMSMS support to integrated product teams for 11 different major space and C3I programs consisting of more than 60 different systems. BAE team members have responded quickly to special requests and provided daily real-time component status and real-time procurement data, along with alerts to provide early warnings of obsolescence. In addition, since February 2007, BAE and teams have worked in concert with the government to resolve DMSMS problems for the space and C3I community, performing tasks quickly and providing valuable and timely recommendations for management action. The professional interaction between government and contractor personnel has resulted in total program cost avoidance of $46.7 million.

Chairman of the 2009 DMSMS and Standardization Conference Invites Participation

As this year's chairman, I, **Alex Melnikow**, would like to invite you to participate in the DMSMS and Standardization 2009 Conference, which will be held September 21–24, 2009, in Orlando, FL. With a new administration taking the helm of the federal government, there will be change. The theme of this year's conference—New Directions and Challenges—will focus on what changes to expect and how these changes will affect the DMSMS and standardization communities.

The target audiences for this conference are DMSMS and standardization professionals who want to hone their skills and be a part of shaping the future of DoD acquisition and sustainment polices. In addition to a full day of tutorials taught by some of the top experts in government and industry and hands-on experience with some of the latest automated information tools, this conference gives attendees access to the new incoming DoD acquisition and sustainment leadership and a chance to hear about their goals, objectives, and direction.

After the incoming DoD leadership has set the stage for our new directions and challenges, workshops and discussion panels will allow audience participation and input into DMSMS and standardization policies, procedures, guidance, and automated tools. We have also invited an outstanding array of experts to share their experiences through technical presentations on how they have successfully addressed the challenges of obsolescence, counterfeiting, standardization, and parts management, as well as technical issues such as eliminating the use of lead.

The conference also provides ample opportunities for attendee interaction and peer-to-peer networking while attending an impressive technical exhibition designed to put you in contact with organizations that offer solutions for your DMSMS and standardization challenges.

In addition, attendees have the opportunity of making a presentation during the technical sessions. Presenters may address DMSMS and total life-cycle management, standardization, GIDEP, parts management, joint and international service activities, industrial base, and value engineering and reduction of total ownership costs. Any attendees interested in making a presentation on one of these topics should submit an abstract to the review committee via the conference website at www.dmsms2009.com.

Events

Upcoming Events and Information

May 19–21, 2009, McLean, VA

PSMC Spring Conference

The spring conference of the Parts Standardization and Management Committee (PSMC) will be held May 19–21, 2009. The PSMC is a government/industry forum chartered by DSPO to improve weapon system supportability and reduce life-cycle costs by promoting commonality of parts and processes. The conference will begin with an Industry Day on May 19, followed by a day and a half of parts management presentations, tools demonstrations, and subcommittee breakout sessions.

For additional information, including the agenda, please visit the PSMC website at www.dscc.dla.mil/programs/psmc or call 703-767-6874 or 314-777-7181.

People

People in the Standardization Community

Welcome

Joyce Pezick of Defense Supply Center Philadelphia has assumed the duties of Lead Standardization Activity. She brings to the position 20 years of experience in the Defense Standardization Program.

In November 2008, **Joshua Civiello** joined the Active Devices Branch in the Document Standardization Division at Defense Supply Center Columbus (DSCC). An engineer, Mr. Civiello will be working in the printed wiring board area (FSC 5998). He was previously employed at The Ohio State University where his work included troubleshooting and repairing circuit card assemblies.

Edmund Wypasek joined the Interconnection Branch in the Document Standardization Division at DSCC in November 2008. He is serving on the rectangular electrical connector team (FSC 5935) as group leader. He brings a wealth of experience from private industry, having worked on Hewlett-Packard systems and high-voltage and programmable logic controllers. Mr. Wypasek's experience with automation systems includes running multiple projects, doing research, and collecting data. He has also worked with laser and fiber-optic systems.

Keith Powell joined the Electronics Devices Branch in the Sourcing and Qualifications Division at DSCC in November 2008. He returns having worked in the semiconductor area back in the mid-1980s. He is assigned in the printed wiring board area and will be trained as an auditor to verify compliance to applicable military specifications. Mr. Powell spent many years at Wright-Patterson Air Force Base, OH, as an engineer and an acquisition program manager in the Air Vehicle Directorate.

Farewell

Bruce Dickerson of DSCC left to work with another government agency. He worked in the Hybrid Microcircuits Branch, Sourcing and Qualifications Division. Mr. Dickerson had 21 years of experience as an engineer and as a qualified manufacturers list auditor in this division.

Tom Hood of DSCC left to work in private industry. He worked in the Electronic Devices Branch (Semiconductors), Sourcing and Qualifications Division. Mr. Hood had 18 years of experience as an engineer and as a qualified manufacturers list auditor in this division.

Dwight Cokain of DSCC retired in November 2008 after 29 years of federal service, including 11 years as a senior electronics technician in the Electronic Components Branch in DSCC's Document Standardization Division and 5 years in the U.S. Navy. He worked in the specification preparing activity function and completed hundreds of standardization projects for electronic relays (FSC 5945) and other miscellaneous electronic components (FSC 5999). Mr. Cokain was a key player in the effort to convert all the electronic relay specifications to performance specifications during the acquisition reform efforts.

Harriett Friedel, a senior food technologist at the Subsistence Directorate, Defense Supply Center Philadelphia, retired in July 2008. He worked on technical issues related to cataloging and specifications and on item reduction. Mr. Friedel worked on operational ration specifications, resolving many issues, including standardization of procurement, technical, packaging, and quality assurance requirements across the specifications.

Retired U.S. Air Force Major **Thomas Kasa** retired after 17 years as civilian chief entomologist, Operational Rations Division, Defense Supply Center Philadelphia. He served as the most knowledgeable quality assurance employee in the Directorate for Operational Rations. We will miss his experience in solving critical operational rations problems.

Emelia Altomari of Defense Supply Center Philadelphia (DLA-IS) passed away on October 31, 2008. A career federal employee, she had retired in June 2008 with more than 33 years of service. She started her career working for the Marine Corps. Ms. Altomari was a valued contributor in the standardization activities undertaken by DLA-IS and was a key contributor to military specification reform efforts, most notably the transition of some 800 military hardware standards to industry.

Upcoming Issues
Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme
January–March 2009	Non-Government Standards
April–June 2009	Interoperability
July–September 2009	Warfighter Support

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, Defense Standardization Program Office J-307, 8725 John J. Kingman STP 3239, Fort Belvoir, VA 22060-6233 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.

Defense Standardization Program
Journal
Government-Industry Data Exchange Program
Defense Standardization Program
Journal
DLA Standardization
Defense Standardization Program
Journal
Technology Standardization

DEFENSE STANDARDIZATION PROGRAM
dsp
MAKING SYSTEMS WORK TOGETHER