THE DOD BIOMETRICS PROGRAM

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-142
Course Content:	155 pgs
PDH/CE Hours:	8

OFFICIAL COURSE/EXAM
(SEE INSTRUCTIONS ON NEXT PAGE)

ENV-142 EXAM PREVIEW

<div align="center">**- TAKE EXAM! -**</div>

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. In the world of Identity Protection there is a statement that rings true, and is an important point to remember when describing the Identity Process: Identity/Authentication is a Universal Event, Assertion is a Local Event.
   a. True
   b. False
2. There are several separate and discrete parts to the Identity Process. Which of the following choices below match the description: The process of claiming an identity in order to obtain a privilege, or set of privileges, previously established for that identity?
   a. Identity
   b. Authentication
   c. Assertion
   d. Authorization
3. According to the FBI, no two persons have exactly the same arrangement of ridge patterns, and the patterns of any one individual remain unchanged throughout life, in which case, fingerprints offer an infallible means of personal identification.
   a. True
   b. False
4. _____ is a fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas.
   a. Loop
   b. Crossover
   c. Whorl
   d. Island

5. Biometrics are physiological features, fingerprint or iris pattern, that can be sensed easily by the system and are sufficiently unique to distinguish you from others in the population.
   a. True
   b. False
6. According to the FBI, among the terrorists and insurgents that we are fighting overseas, roughly 1 in _____ has a criminal record in the United States, which means that many of the people we are fighting today not only have been in America and in our hometowns but also have committed a crime while they were here.
   a. 100
   b. 1,000
   c. 10,000
   d. 20,000
7. The FBI has some ___ million fingerprint cards and its automated system topped 52 million records last July, with 6,000-7,000 new accessions per day. They handle 65,000 service requests per day.
   a. 180
   b. 200
   c. 350
   d. 500
8. According to the FBI, no two persons have exactly the same arrangement of ridge patterns, and the patterns of any one individual remain unchanged throughout life, in which case, fingerprints offer an infallible means of personal identification.
   a. True
   b. False
9. Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent only since _____.
   a. 1992
   b. 1994
   c. 1999
   d. 2001
10. According to the reference material, The FBI digitization standard of 500dpi yields a fingerprint record of __mb. Lossless compression, in practice, seldom does better than 2:1.
   a. 4
   b. 6
   c. 8
   d. 10

TABLE OF CONTENTS

LIST OF FIGURES

Executive Summary

A Defense Science Board Task Force was organized to address a number of issues relating to the use of Biometrics in the Department of Defense. The Terms of Reference (Appendix A) asked that specific organizational issues be addressed promptly and the Task Force provided an interim briefing that focused on these issues.

While the terms of reference refer to "biometrics," the Task Force is convinced that "identity management" is the more inclusive and the more useful construct. The Task Force holds two companion theses. First, while we can come up with an endless set of scenarios in which biometrics might be called upon to play a role, with analysis and a little abstraction without losing the essence, the endless array of scenarios can be reduced to a compact set of "use cases". This compact set of use cases will help us appreciate our companion thesis, that a common "back office" process (and associated "data model") can be envisioned to service all the biometric, and thus Identity Management, use cases.

That said, we clearly did not have either the time or the resources to study Identity Management (IM) conclusively, especially in terms of the broadened set of organizational associations, use cases and Defense applications, and even social issues, attendant to that sprawling field. The "common back-office process," and related architecture, to support biometrics, as alluded to just above, is itself a rich field of study that deserves and demands close attention and broader treatment than we were able to provide here. Another important aspect of the total subject of Identity Management is the whole universe of tokens and credentials. There are many of these, in as many different formats and standards as there are applications. Only some of them support, or are used in conjunction with, biometrics. We speak to some extent of the credential standard mandated for use across the federal government, called FIPS-201. Beyond that, however, this large and important topic will have to await a broader treatment of the whole of Identity Management, and we do recommend that such an effort be undertaken with a fully scoped charter.

What we have sought to do is to examine biometrics carefully, and we have placed those issues, both technological and "organizational," into the operational context of their use in strengthening IM processes. There remains, however, much to be done to understand and implement needed changes in organization, technology, and process before IM can achieve its full potential in the DoD or elsewhere. It is noteworthy that while significant progress is being made, both inside the DoD and across the federal government, to define and implement organizational approaches to biometrics, these efforts have yet to explicitly embrace the larger scope of IM, systemically. The Task Force holds that the enhancements to biometrics management we cite here are in the critical path to that outcome. However, it should be understood that such improvements in biometrics only, while necessary, are insufficient to the total need.

The Task Force finds that biometrics suffers from a characteristic of many "new" areas of technology and application. At the outset, biometrics had (it seems) as many advocates making unsupportable performance claims as it had detractors decrying its mystery, uncertainty and unacceptability on the basis of historic formulations of governance, privacy, etc. It is also true

that in biometrics the truth lies between these extreme positions, and for the most part, has yielded to thoughtful technical analysis and collaborative, inclusive, organizational effort. The Task Force will make several recommendations designed to advance these two parallel but associated lines of effort, the technological and the organizational.

Identity management, the output of the application of biometrics, and the real issue here, is vitally important to the success of many missions of the Department, and increasingly so. This growing importance, however, has not been reflected in the attention the Department has paid to the topic. At the outset of our study, the Department was neither well organized nor properly motivated for success in identity management, or biometrics. Since then, the Department has significantly improved its focus on management of the biometrics mission. Activities and responsibilities in the larger scope of Identity Management, however, remain broadly distributed across a number of Defense organizations, and we believe that the Department must embrace the larger construct. Several factors presage the increasing importance of identity management.

- Logical Access Control: The inexorable increase in information-based processes and increasingly critical dependence on the confidentiality, integrity and availability of information demand stringent controls on logical access which, in turn, stress authentication techniques.

- Physical Access Control: Increasing terrorist threats to our personnel, facilities and capabilities demands similarly stringent controls on physical access which too stresses authentication techniques. Likewise, criminal threats to our resources.

- Targeting: Our military and intelligence concerns in the Global War on Terrorism have largely shifted away from nation states and their facilities, and toward individuals.

The Task Force found need for clarifying and strengthening, perhaps reassigning, authorities and responsibilities for the full cast of DoD roles:

- Principal Staff Assistant (PSA): An empowered, dedicated Assistant Secretary-level individual who can provide and/or coordinate effectively the policy, strategic direction, oversight and evaluation; ensure sound programmatics and adequate resources within the Department; serve as "functional advocate" for biometrics (and eventually, identity management); and represent the Department in relevant interagency, intergovernmental and international processes.

- Joint Staff Advocate: A similarly empowered individual of status who would be designated as the primary focal point for staffing and coordination of biometrics issues on the Joint Staff.

- Combatant Commander: A designated commander responsible for developing and/or coordinating the requisite Concepts of Operations (CONOPS), joint experimentation and training, and joint and inter-agency doctrine for the military applications of biometrics.

- ▪ <u>Executive Agent:</u> A service, agency or field activity that can support the PSA in implementing, under PSA authority, Defense-wide programs for acquiring, fielding, sustaining and training, and in some cases operating, the biometric and related systems.

The Task Force stopped short of making recommendations about the assignment of these roles and responsibilities to specific Departmental entities with the exception of the role of Joint Forces Command in areas related to experimentation, doctrine and training, tactics and procedures (TTP). It did previously provide a list of obvious candidates with its assessment of their respective strengths and weaknesses. The Task Force also provided a number of interim findings and made several interim "process" recommendations.

Among the interim findings which have been substantiated and/or reinforced by subsequent study, the Task Force finds:

- ▪ The importance of identity management and the role of biometrics in the Department of Defense are underappreciated. Identity management and biometrics represent a key enabler in the Global War on Terrorism, can save lives, are essential to Information Assurance (which is key to Mission Assurance), and has international implications where our leadership is in question.

- ▪ The present management structure largely reflects pre-9/11 requirements: a "blue" focus inside DoD, and conceived in the context of information assurance. However, requirements and applications have grown with the emergence of "red" and "gray" requirements, HSPD/NSPD-driven requirements, increased inter-agency and international interests, and the growing importance of forensics on the battlefield.

- ▪ Urgent battlefield needs are not being met. The current "program" appears to lack the necessary warfighter customer orientation. The current execution appears to be inefficient and opportunities are being missed.

- ▪ Requirements will continue to grow as current business processes scale up, as new applications come on line, as the adversaries adapt and as new threats emerge.

- ▪ Technology is changing for the better. New technologies must be inserted rapidly. In some cases, technology will need to be stimulated to meet the most demanding military applications.

- ▪ There appears to be considerable benefit in a Department-wide authority for identity management and biometrics, accountable and responsible for its funding, policy, vision and direction, and sustainment.

Irrespective of the specific organizational "who," the Task Force found that certain actions were imperative and urged that, without further delay, the Department:

- ▪ Decide who is/will be the ID-Mgmt/Biometrics Principal Staff Assistant (PSA) and update the documentation to reflect that reality.

- Designate the PSA for biometrics as a "functional advocate" for biometrics issues within and across the Global Information Grid (GIG).

- Formalize and strengthen relationships between the Biometrics Fusion Center (BFC), the Defense Manpower Data Center (DMDC), and all other Defense entities with explicit and/or implicit biometric/identity management roles and/or missions.

- Decide promptly on a comprehensive (data) architecture for backup and disaster recovery.

- Identify and establish central OSD oversight of all Defense-wide Biometrics activities immediately, to include the Armed Forces Joint Identification Laboratory in Rockville, MD, and its DNA repository[1].

- Identify and establish management oversight of all biometrics programmatic activities within a consolidated program of record. Capture (interim) requirements in time to intersect the FY07 PDM; create a Defense-wide Biometric funding program and immediately put a "wedge" in the FY08 POM. Subsequently, consider a Defense-wide funding program for the larger Identity Management activities, including RDT&E, Procurement, O&M, personnel, and training.

- Create a permanent manning document for the Biometric Fusion Center (BFC) at/above current staffing levels; establish joint billets as appropriate, and designate the BFC as "critical infrastructure."

- Establish all required identity management CONOPS, doctrine, experimentation, training and education programs and processes.

We were gratified when, on 4 October 2006, the Deputy Secretary of Defense designated the Director, Defense Research & Engineering (DDR&E) as the Principal Staff Assistant (PSA) for biometrics[2], with responsibility for the authority, direction, and control of DoD biometrics programs, initiatives, and technologies. The Army was named in the same document as Executive Agent, with defined responsibilities under the direction of the PSA. Most of the specific recommendations contained in the report, then, are aimed at the PSA. These are distributed throughout the report and recapitulated in the last chapter, categorized according to whether they reflect: internal DoD issues; issues external to DoD; remaining organizational issues; R&D, materiel and technology issues; information management issues; and/or, legal and privacy issues.

---

[1] We call DNA out here specifically as there is, at present, definitional debate within the US government regarding the proper "status" of DNA as a "true biometric". Based on the range of DoD use cases involving DNA, the Task Force has chosen to define DNA as a "biometric modality," even while recognizing its unique character.

[2] See Appendix C of this report

Finally, although the art form of reports such as this often presages key recommendation in the Executive Summary, we do not. There are simply too many. Instead, we have chosen to recapitulate all the recommendations and their associated conclusions in Chapter 18. These are characterized according to the category of the recommendation: Information management and sharing; R&D and technology; Issues external to the Department of Defense; Internal issues; Organizational issues; and Legal and privacy issues. Where the recommendations fall into more than one category, they are duplicated for convenience and within each category the recommendations are treated in the order of their appearance in the body of the report.

Introduction—Identity Management and Biometrics

From its inception, this Defense Science Board Task Force on Biometrics understood that its job was to examine a topic which was urgent, complex, somewhat new and distinctly open-ended. "Biometrics" was and is seen as an emerging field of growing importance to the Department of Defense and the nation's security more broadly. The first and most important finding of the Task Force was that in order to understand the science and applications of biometrics, these must first be placed in context. The Task Force brought a variety of views to bear but there was unanimity that the "real" topic of discussion was "identity management" rather than simply "biometrics." Biometric identification supports identity management, which is a key to success in many mission areas in the Department of Defense and in the larger national and homeland security context both in the US and internationally.

Identity management is increasingly critical to the success of many missions of the Department of Defense, but this growing importance is not reflected in the attention the Department has paid to the topic in the past. The Department of Defense has been neither well organized nor properly motivated for success in identity management.

The recent appointment of the Director of Defense Research and Engineering (DDR&E) to act as the OSD Principal Staff Assistant (PSA) for biometrics[3] is a very positive step in this complex process. There is much work to be done in biometrics, and the DDR&E, working with organizations inside and outside the Defense Department, will be busy with it for some time. That said, the Task Force has sought to make the case that biometrics are inseparable from the larger field of Identity Management (IM), in almost any application or level of treatment other than pure science and research. Beyond that, Identity Management is itself linked intrinsically to Information Assurance (IA), in ways which have been described in some detail in recent DSB reports.

Pragmatically, we must conclude that it would be difficult to define, here and now, the proper organizational/technology approach to a *universally* biometrically-enabled, strongly-identified and assured, global information grid. However, that must be the procedural path along which we are looking and thinking, even now. Consequently, we must begin to structure our attention, and increase our understanding, within that expanded scope of interest.

As discussed throughout, the Task Force was clear that no examination of biometrics could fail to consider Identity Management (IM). However, it was just as clear to us that we did not have the time or resources to study the full scope of IM comprehensively, and that remains an unfulfilled need to be accomplished in the proper time and way.

In any very small group there is no need for identity management. However, whenever populations become more numerous, especially if they are not always or ever in physical contact

---

[3] Deputy Secretary of Defense memo dated 4 October 2006 -- See Appendix C. The same document defined the role of the Army as Executive Agent

with each other, distinguishing among individuals becomes steadily more important. In national security matters, as friend/foe distinctions such as clothing (uniforms) diminish in incidence and usefulness, this point is underlined. Differentiation based on sight, sound and smell provided the earliest distinctions, and the data management was initially based on "full path names"—*i.e.*, the "begats".

Today, identity management is more important than ever. Names carry less information today and are less unique, but biometrics have improved markedly as have our data management capabilities. Both are far from perfect, however, and set the agenda for our task force, as did the set of DoD missions that depend on identity management and therefore on biometrics.

To reiterate, biometrics is but a means to an end, while identification is the goal. Indeed, trying to define "biometric" in the current context is next to impossible without invoking the idea of identity, identity management, and/or identity management system.

An identity management system, here, is meant to include both algorithms, their instantiation in software/hardware, as well as data. The data are an organized collection of information about specific individuals. Indeed, when we ask "who are you," we are really asking "what are you" - *e.g.*, friend or felon?

It is easiest to think of an identity database as a relational database, rows and columns, where the rows ("entities" or "records") are individuals, where the columns (or "attributes") are characteristics or categories of information about individuals, and where the columnar entries (or fields) represent the particulars for that individual. Certain of the attributes serve principally to "identify" you, that is, to allow one to query (or "index into") the database and retrieve some or all of your record. Among traditional "identifiers" are name and social security number (SSN). Names may be our first impulse, but they are notoriously ambiguous and generally not sufficiently unique. SSN is more unique. All of these variables, however, suffer from the problem that they can be compromised relatively easily - bought, stolen, or invented. Thus, they are increasingly insufficient, by themselves, for identification. That brings us to biometrics.

The National Science and Technology Council (NSTC) subcommittee on biometrics defines biometrics as:

> *A measurable biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition.*

Their use of the qualifier "automated" reflects the practical utility of actual biometric systems, which otherwise would be generally inefficient and ineffective because of the uncontrolled/unknown error rates and biases that humans introduce. Read "recognition," per the preceding discussion, as the ability to retrieve with high confidence the identity record of the individual, *i.e.*, to index into an identity database. Their definition accords well with standard dictionary usage:

> *The term biometric is the name given a technology that is the measurement of a living, human characteristic. This process includes the ability to measure*

characteristics such as fingerprints, voice recordings, irises, heat patterns, keystroke rhythms, and facial images; comparing a person's unique characteristics against previously enrolled images for the purpose of recognition.

The unique pattern of a physical feature such as a fingerprint, iris, or voice as recorded in a database for future attempts to determine or recognize a person's identity when these features are detected by a reading device.

Identity vs. "Collateral Data"

It is useful to separate conceptually the "identity" and those "collateral data" which are pointed to by the identity, or which point to the identity. In one case, the identity is used to reference or retrieve or "index into" collateral data. In the second case, items of biographic data may simply be an explicit "back-pointer" or it may be implicit, *i.e.*, inferred from sufficiently unique items of biographic or privilege data.[4]

Furthermore, it is useful to conceptually separate the "biographic" from the "privilege" data. Biographic information, including established "roles" for the individual, provides the basis for the need and/or "suitability" decisions to confer a right or a privilege. Privilege information includes a description of the privilege granted and, perhaps, pointers to the biographic information on which the decision was based. Some form of "back chain" from the basis-information to the privilege would support dynamic reconsideration of the privilege by the grantor when basis information changes, which would otherwise require (frequent) periodic polling. The relationship of "identity" to "privileges," including the management processes related to both is an important one.

Collateral information also includes physiological data, those items of information common to all individual humans. We all were born at a time and in a place; we all have height, weight, hair and eye color, *etc*. Many of these characteristics are commonly used to "recognize" an individual, *i.e.*, to confirm an identity. Some, like fingerprints or DNA, are sufficiently unique and durable/unchanging to support strongly fixing an identity. It is these that we refer to as biometrics.

It is also important to define "identity." Strictly speaking "identity" is the "unit of analysis" (or record or row) in an identity management system. A particular identity is a particular record which (in a well-ordered system) has a unique "accession number," which one also might think of as "the identity." When associated with individual humans in a system, the concept of "root identity" emerges, as discussed below.

_____

[4] The bane of the privacy community is the ability to follow the logical threads using these pointers, which will disclose a lot of "peripheral" information from one or a few pieces of information. This is particularly troublesome when, in the eye of the individual, the peripheral information is not seen as germane to the legitimate purpose of conferring a right or a privilege. The more complete (and organized) the totality of the ensemble of information, the more inferential threads that can be pulled, and the more worrisome the process is to privacy advocates.

Identity Assurance

Digital identities have become critical in both civilian and federal enterprises. They represent a high assurance level that the identity of a person has been adjudicated by an enterprise or agency according to policy and therefore maintain a certain status of reliability. However, as with most attempts to create interoperability's between organizations, there is the reality that individual organizations or agencies will not trust the credentials issued by other organizations or agencies. It is generally true at present that there is no surety that the standards are common between them and therefore might not meet their standards. The effort to achieve cross-organizational management confidence, in root identity and authorities, is the stuff of Privilege Management, which we will discuss later.

HSPD-12[5] and its related technical standard, FIPS 201[6] is one example of many sets of initiatives to improve Identity Assurance. From our point of view, it is by far the most important, as it is mandatory across the entire federal executive enterprise. HSPD-12 specifically addresses the federal government and extends explicitly to certain commercial entities (federal contractors). It has been extended implicitly to state, local and tribal governments within the United States, in the form of assuring access to, and interoperability within, certain federal programs. The FIPS-201 technical standard developed under authority of HSPD-12 has been adapted in other current programs with even broader scope, such as the Transportation Worker Identification Credential (TWIC), and the First Responder Access Card (FRAC). We expect this trend to continue.

The FIPS-201 standard is a smart card based on common criteria to verify an individual's identity; is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitations; allows for personal identity to be rapidly verified electronically if visiting other facilities; and comes from a controlled set of issuers to assure quality and standards. The whole process is made more rigorous by the background checks conducted prior to issuance to ensure the applicant's eligibility and uniqueness within the database.

An Identity Management "System"

The real meat of a modern Identity Management system is not the front end, badges, tokens, and/or biometrics, but the information system in which they operate, the "IT backplane". This recognition represents a change in the attitude of program sponsors and the user population. Complex/expensive tokens (e.g. Smart Card) are useful and prescribed in many applications but,

---

[5] Homeland Security Presidential Directive (HSPD) 12 – *Policy for a Common Identification Standard for Federal Employees and Contractors* requires government-wide uniformity and interoperability to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card.

[6] Federal Information Processing Standard (FIPS 201) for Personal Identity Verification (PIV) of Federal Employees and Contractors: This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

if limited to local operation, are often impractical in situations where DoD seeks an ID solution. The geographic and organizational scope, plus the growth in size of enrollee populations, has made it clear that modern networked IT solutions offer the best hope of achieving mission success. The centralization in design, development, management and operation that usually accompanies networked systems provides economies of scale and allows us to amortize costs over a larger set of uses. It also is associated with improvements in interoperability.

Focusing for a moment on tokens and credentials, it is clear that there are currently many of these in important roles. Some of them, hopefully the best, almost certainly the most expensive, use biometrics either "on-card" or in conjunction with stored indices. A complete review of tokens and credentials, and their role within a total Identity Management system, is beyond the scope of this report, but it remains an important issue within that larger field of study.

Identity Management is a set of processes, policies, tools, connectivities, and social contracts protecting the creation, maintenance, use and termination of an identity. Figure 1 shows a simplified data flow diagram depicting the creation of a Digital Identity Record in a traditional enterprise environment. Not all processes are the same and all will vary. It is here that decision makers and stakeholders, with the proper authority, can modify, search, and delete digital identities based on policy and accepted practice.
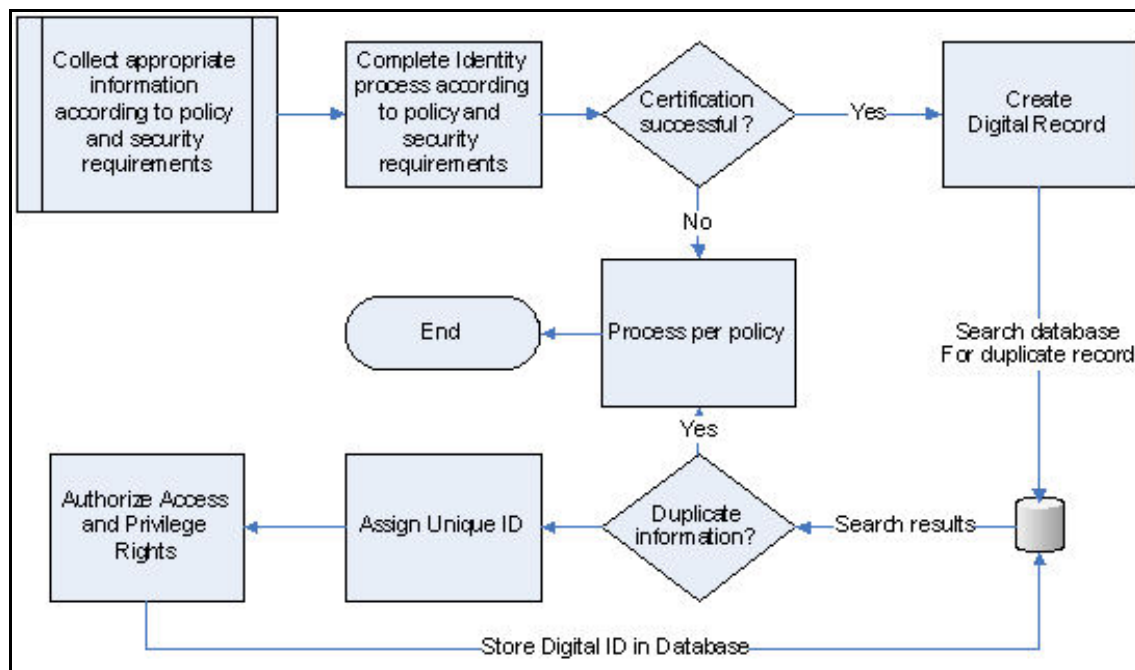
Figure 1: The Creation of a Digital Identity

Historically, the Department of Defense has had a number of different Identity Management "systems" of both large and small scale. Only very recently, with the advent of Presidential policy in the form of HSPD-12, has the federal government, and as such the Defense Department, moved toward a single, common and interoperable technology and policy approach to "Identity." The technological particulars of the design, implementation and operation of any such system, of course, depend on:

- The purpose of the system: What problem or problems is it attempting to address? What DoD/USG missions does it seek to enable?

- The population subtended by the system, and the way the identities of these individuals would be authenticated.

- The scope of the data, both "identifiers" and "collateral" data that would be gathered about individuals in support of "issuing an ID" - figuratively, *i.e.*, enrolling them in the system; and, literally, *i.e.*, issuing a token - and the way that identity would be correlated with (mapped to) data about the individual in any databases associated with the system.

- The users of the system, those who would be issued an ID, Department and OGA officers and, perhaps, non-federal authorities including the private sector.

- The types of use allowed, and under what circumstances: What types of database queries about individuals would be permitted?

- Required "interoperability" with other databases. The ability to retrieve information and make inferences across multiple datasets.
  - *The Task Force notes this important question appears to have been honored more in the breach than the observance as systems were fielded expediently in support of the warfighter.*

- Degree to which data mining or analysis of the information collected would be permitted. Who would be allowed to do such analysis? For what purposes?

- Degree to which enrollment in and/or identification by the system (even if the individual had not formally been enrolled) would be mandatory or voluntary.

- Legal structures that protect the system's integrity as well as the ID holder's privacy and due process rights: What structures determine the government and relying parties' liability for system misuse or failure?

Of all these features and considerations, HSPD-12 provides only the most basic, but this is the foundation upon which all else can be built. Put another way, absent the HSPD-12 foundation, all such effort would represent a house built on sand. As such, it defines the space within which remaining policy, technical, and organizational efforts are still required.

As has been pointed out,[7] implicit in the totality of these considerations is the notion of a "system" and not merely an ID card or biometric. The importance of the fact that identity management necessarily implies a "system" cannot be overstated. Such systems, at the scale that they would operate in the Department, necessarily imply the linking together of many social, legal, and technological components in complex and interdependent ways. The success or failure of such a system is dependent not just on the individual components (for example, the ID cards that are used or the biometric readers put in place) but on the ways they work, or do not work, together. For example:

- Are card enrollment/authentication devices located where they need to be? How well do the devices operate under various environmental and load scenarios?
- Who will operate the systems and how will they be trained and vetted?
- Do enrollment policies align with the security needs envisioned for the system? And so on.

How well these interdependencies are controlled along with the mitigation of security vulnerabilities and the unintended consequences of the deployment of a system, will be critical factors in its overall effectiveness.

In addition to the questions above, the reference outlines several cautions to bear in mind when considering the deployment of a large-scale identity system:

- Given the costs, design challenges, and risks to security and privacy, there should be broad agreement in advance on what problem or problems the system would address.
- The goals of the system should be clearly and publicly identified and agreed upon, with input sought from all stakeholders.
- Care must be taken to explore completely the potential ramifications of deploying a large -scale identity system, because the costs of fixing, redesigning, or even abandoning a system after broad deployment would likely be extremely high.

---

[7] *IDs—Not That Easy: Questions About Nationwide Identity Systems*, Statement of Stephen T. Kent Vice President and Chief Scientist, Information Security BBN Technologies and Chairman Committee on Authentication Technologies and Their Privacy Implications National Research Council The National Academies before the Subcommittee on Social Security Committee on Ways and Means U.S. House of Representatives March 16, 2006

Identity Processes

The Identity Process is one of the most interesting and technologically challenging parts of the Identity Protection environment because of the complexities of how we do business. There are several separate and discreet parts to this process. They include:

> Identity – Who you are[8]
>
> Authentication – The process which states that your identity and the activities that have been evaluated in your past meet the policy and integrity standards to be certified as a member of that organization or agency.
>
> Assertion — The process of claiming an identity in order to obtain a privilege, or set of privileges, previously established for that identity.
>
> Authorization – The act of granting a person permission to use, or have access to, specific physical or logical resources within that organization or agency.

In the world of Identity Protection there is a statement that rings true, and is an important point to remember when describing the Identity Process:

Identity / Authentication is a Universal Event, Authorization is a Local Event.

Translated, that means that you are, or should, always be the same person[9]. That is universal. However, you often have many different tasks and responsibilities that are unique to you, and which may be confined to specific situations or differing organizations/agencies. It is quite possible, or even probable that you might have differing permission sets assigned to you depending on where you are accessing either physical or logical assets. There is technology for the Identity Process to directly address that in a very granular and secure fashion. It allows permission sets to be created, modified, and deleted quickly and efficiently based on policy, law, social convention, and security requirements.

The "Root" Identity

Authenticated root Identities are needed to make ID-enabled applications work. One can only get to the payback at the application layer of an Identity Management system after having undertaken the cost and effort of establishing verifiably-unique root identity enrollment. This identity must be "transportable" over time and distance, in terms that benefit both the enrollee and sponsor. The enrollee must be able to convincingly assert his true ID to access resources or avoid sanctions. This aspect of the total IM strategy, the creation of root Identity to a strong and common standard, is the focal point of the prescriptive provisions of HSPD-12.

---

[8] An important distinction here is the difference between "true identity," a unique, provable, fact, for which the only real proofs are biometric in nature; and a "persona" that one may adopt as being appropriate to some kind of identity-sensitive activity, such as sending e-mail or conducting an online auction. The easy distinction is that an Identity is an irreducible core fact, while a Persona, if it to be trusted, should have recourse to a true or "root ID," whether or not that is visible to all parties, all the time.

[9] The converse, of course, is that nobody else can be "you".

The Role of Biometrics

There are numerous ID-sensitive applications extant today, especially in commercial practice, very many of which do not have an architectural/policy relationship to a true root identity. The contribution of biometric processes to the total ID enterprise is the offer of high assurance of uniqueness in initial registration, and added confidence to ID assertion in application. As such, while it is certainly possible to engage in ID-sensitive activities without biometrics, there can be no truly accurate Identity Management system without biometrics. In order to achieve, verify, and sustain that root identity, it is absolutely necessary to link the "legend," biographic information claimed by an enrollee (name, date/place of birth, address, etc), to the person making the claims at the bodily level. The emergence of this understanding has paced the growing role of IT networks in IM, as discussed above. Biometrics are difficult to verify in their original form, but they all lend themselves to codification, analysis and expression as IT files. Here the earlier point about social acceptance returns to the discussion. Public acceptance of biometrics has grown cautiously over time. Leading thinkers in the IM community have now been fielding applications that demonstrate and deliver real and practical benefits to consumers and managers, based on biometrics. At the same time, the subject of biometrics is being gradually demystified, even as the underlying science is more richly and broadly understood. Consequently, biometrics performance issues are being approached and examined more pragmatically, with fewer inflated expectations, and less unreasoning skepticism.

The maturation and availability of biometric capabilities within the Identity Management processes has added significantly to the power and reliability of Identity. Biometric technology involves the capture and storage of a distinctive, measurable characteristic, feature, or trait of an individual for subsequently recognizing that individual by automated means. The biological trait is unique to a specific person that, when intrinsically linked to the Identity Management process, creates an extraordinarily strong link between the identity credential, or token that is presented, and the person who has it in their possession.

The Identification Trinity

In the strongest identity formulation, we refer to "three factor authentication": something you know, something you have, and something you "are."

Something You Know

This includes passwords, PINs, pass-phrases, and answers to authentication questions such as the name of your first pet or car, your mother's maiden name, or other personally meaningful association. In the best case, such information is known only to you and "the system."

A selling point for such secrets as authenticators is that they are easily issued, invalidated in the event of compromise, and reissued upon authorized request. The down side is that, historically, they are readily compromised. Insofar as they tend to be meaningful to you, someone who knows you may know the secret or be able to guess the password or phrase. The more generally meaningful they are, the more susceptible to brute force "dictionary" attacks.

Attempts to strengthen the secret "key" generally make them less individually meaningful, harder to remember, easier to forget. The general response is to write them down somewhere, another avenue to compromise.

Because different systems issue/register their own secret identifiers, coupled with the drive to make them less easily compromised *i.e.*, less meaningful, the response for those who must access multiple facilities/systems is to use the same secret on more than one system. This means that any compromise propagates across those systems. It also opens the door to an "attractant" system obtaining your secret as you register in that system unaware of its nefarious purpose.

For these and other reasons, multi-factor identification is preferred for serious security.

Something You Have

No matter how pervasive today's digital technology, everyone has considerable experience with physical identity tokens, mainly social security cards[10], driver's license, passport, birth and/or baptismal certificate, employment-related badges, *etc*. Some of these tokens are often mistakenly referred to as "ID cards" but are, to a certain extent, vehicles for conveying "privilege." They are generally the property of, and/or controlled by the privilege grantor.

We have discussed HSPD-12, and its role in establishing strong root identity, its other major provision is the establishment of a common-format ID credential, which has become a technical standard known as FIPS-201. The DoD Common Access Card (CAC), which predates FIPS-201, has since migrated to a compliant standard. Some physical tokens may also contain digital certificates, crypto variables, and encoded biometric indices.

The Department of Defense has invested prestige and resources in its Common Access Card (CAC), sometimes referred to as CAC-card (*sic*) The fundamental goal of using the Common Access Card is to authenticate the identity of the cardholder (uniformed military, civilian DoD personnel and contractors) to a system or person that is controlling access to a protected resource or facility. This end goal may be reached by various combinations of one or more of the following validation steps.

Card Validation - The process of verifying that a CAC is authentic and has not been subjected to tampering or alteration. Card validation mechanisms include:
- Visual inspection of the tamper-proofing and tamper-resistant features of the CAC;
- Use of cryptographic challenge-response schemes with symmetric keys;
- Use of asymmetric authentication schemes to validate private keys embedded within the CAC.

---

[10] Never really intended to be an identity token or credential in the modern sense, it has no anti-tamper or ID authentication, as expressly stated on the card: "not to be used for identification purposes."

Credential Validation - The process of verifying the various types of credentials (such as visual credentials, CHUID[11], biometrics, CAC keys and certificates) held by the CAC. Credential validation mechanisms include:

- Visual inspection of CAC visual elements (such as the photo, the printed name, and rank, if present);
- Verification of certificates on the CAC;
- Verification of signatures on the CAC biometrics and the CHUID;
- Checking the expiration date;
- Checking the revocation status of the credentials on the CAC.

Cardholder Validation - The process of establishing that the CAC is in the possession of the individual who is the legitimate holder of the card. Classically, identity authentication is achieved using one or more of these factors: a) something you have, b) something you know, and c) something you are. The assurance of the authentication process increases with the number of factors used. In the case of the CAC, these three factors translate as follows: a) something you have - possession of a CAC, b) something you know - knowledge of the PIN, and c) something you are - the visual characteristics of the cardholder, and the live fingerprint samples provided by the cardholder. Thus, mechanisms for CAC cardholder validation include:

- Presentation of a CAC by the cardholder;
- Matching the visual characteristics of the cardholder with the photo on the CAC;
- Matching the PIN provided with the PIN on the CAC;
- Matching the live fingerprint samples provided by the cardholder with the biometric information on file at the Defense Manpower Data Center (DMDC).

Something You "Are"—Biometric Indices

Biometrics are physiological features, fingerprint or iris pattern, that can be sensed easily by the system and are sufficiently unique to distinguish you from others in the population. Your biometrics are not something you have to remember and might forget, so you don't need to write them down. Biometrics indices are generally harder to compromise than other authentication factors, so biometric-based identification is harder to repudiate.

In the previous discussion of the Common Access Card, biometrics are part of the multi-factor process in validating both the credential and the credential holder.

---

[11] CHUID -Card Holder Unique Identifier

Biometric Authentication Model

The workflow for biometric authentication involves a two-stage process, as depicted in Figure 2 below:

- Initial registration of the individual, preferably "face-to-face," which, in turn, involves:
  o User identification
  o Feature capture
  o Template construction
  o Inserting a record in the database which, logically, contains at least an accession number, and the user identification

- User authentication, which may be local or remote, and involves:
  o Identity assertion
  o Feature capture
  o Retrieval of the registration template from the asserted-identity record
  o Scoring against the registration template
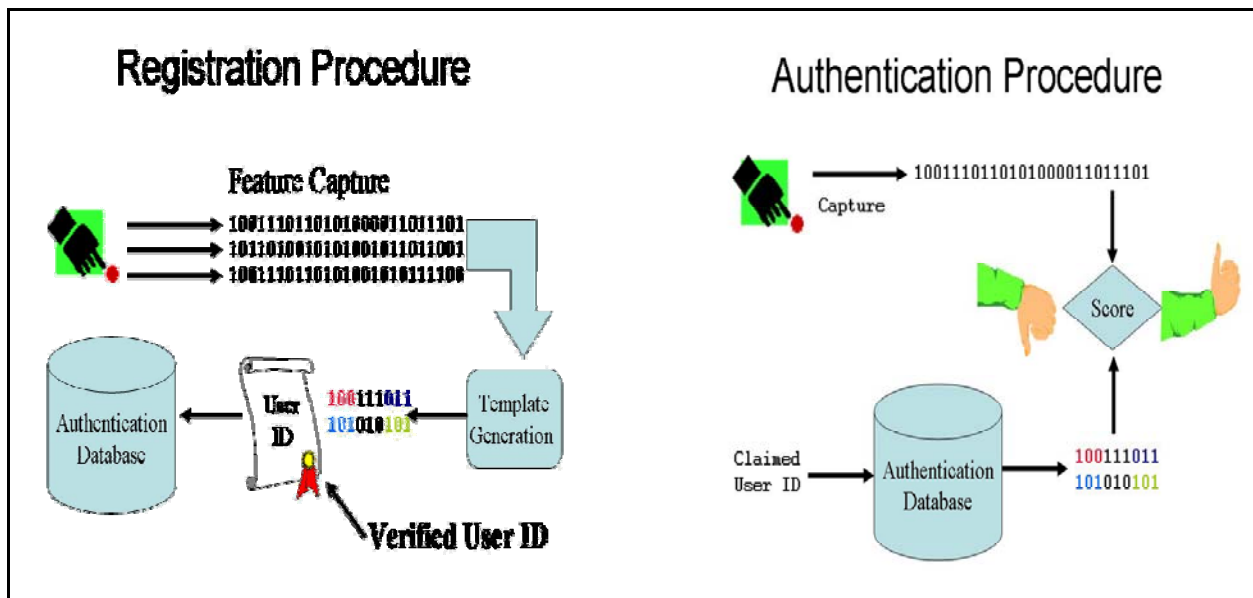
Figure 2: Registration and Authentication Procedure

Data Management Issues

It's not really who you are, it's what you are. Identity management systems inherently contain, store and manage, sometimes very dynamically, masses of data. These range from raw biometrics, to templated versions of the same, to associated biographic information. Associated privilege information may be involved, and also perhaps digital signatures, certificates and other architectural and security features. Establishing a good data architecture is essential to effective identity management. Being able to retrieve related data and cross reference across relevant data sets is really the point of it all.

Observation: The Department of Defense does not appear to have a comprehensive data architecture for identity management in its various aspects, nor does it appear to have anyone responsible for creating and maintaining such an architecture. This is especially important because the various relevant data sets across which one might wish to operate (*i.e.*, cross reference) are scattered and under "local" control. Indeed, many of the relevant datasets are outside the Department itself. It is very difficult at present, and institutionally resisted to at least some extent, to recognize and accept credentials issued by other federal agencies. The "fix" for this suboptimal situation is broadly embraced within "Privilege Management" concepts, discussed in detail later in this report.

Recommendation 1: The PSA for Biometrics, in the absence of a PSA for identity management, should identify the responsible actor in the Department and ensure that a data model/architecture is developed and maintained. The PSA should become the "functional advocate" for biometrics and identity management, in terms of their use in the Global Information Grid (GIG).

The Power of ID-Sensitive Applications

The value of any Identity Management system exists in the *Applications*. Simple ID enrollment, in and of itself, never pays off in terms of a demonstrated, measurable and attractive "return on investment". The processes of establishing programs, gathering and maintaining data, conducting investigations to verify enrollee claims, and issuing badges, all represent costs, and all are fronted-loaded within an Identity Management implementation. No matter how you measure it, the value is found in the practical use of the Identity Management system. These applications include a broad and ever-expanding range of enhancements to personnel and information security, force protection, intelligence and other important missions. The good news for the DoD is that given all historic effort in developing and fielding the CAC, not to mention HSPD-12, there is already a sunk-cost investment in the necessary foundation upon which an applications architecture can be built.

It is possible to envision an expanding set of ID-sensitive applications in work and society, collectively comprising what one author has termed an "Identiverse," within which security and functionality are enhanced, privacy as well, if designed and managed properly. Benefits may take the form of increased efficiency in workflow, access to resources, convenience, *etc*.

The "Back Office" Process

Much of the focus in the application of biometrics in support of identity management is vested in the "front end" or "point of sale."

- The lance corporal who fingerprints, and thereby identifies a "high value target," or his counterpart police officer on the beat who nabs and identifies one of the "ten most wanted" or;

- The guard at the turnstile of a sensitive facility who prevents the would-be terrorist from entering the facility under false pretenses or the immigration control officer or transportation safety worker who identifies a known terrorist.

However, the real work is being done by the servers in the back office that maintain, compare and retrieve the relevant data on which action can be taken. In Figure 3, the work flow is shown for the Integrated Automated Fingerprint Identification System (IAFIS) run by the FBI's Criminal Justice Information Services Division (CJIS)[12].
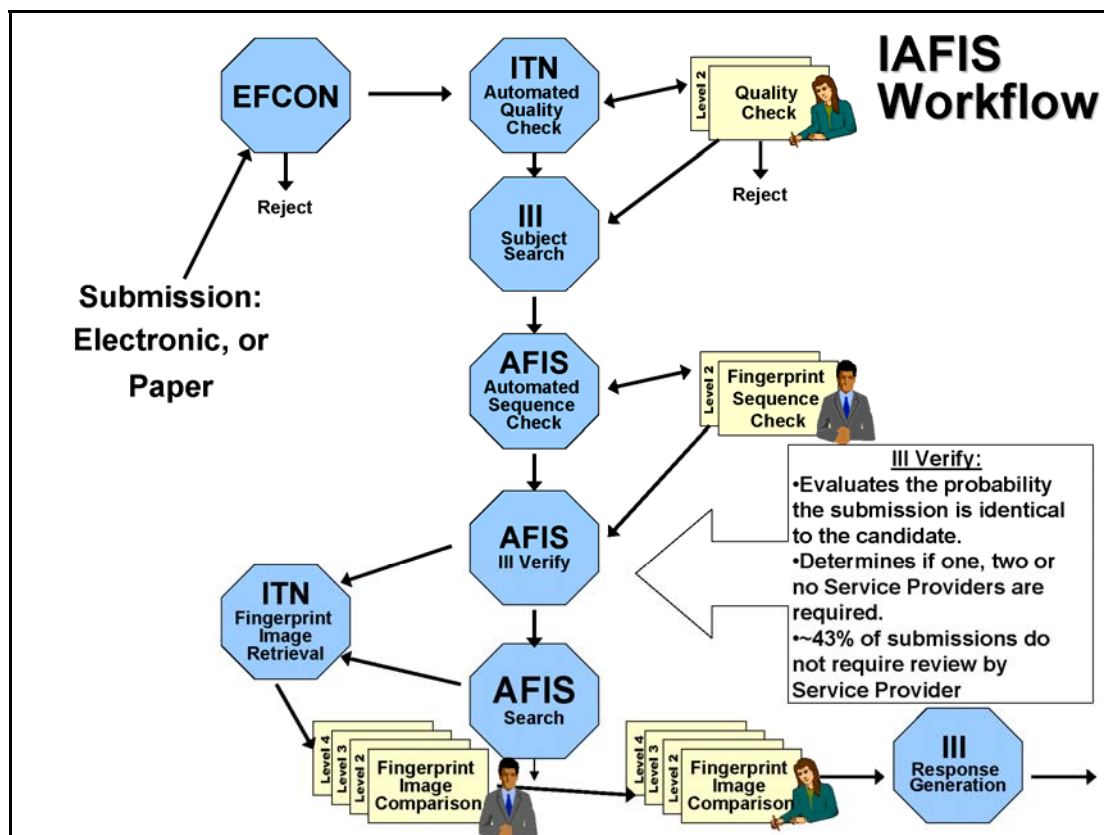
Figure 3: IAFIS Workflow

_____

[12] See Glossary for long titles and definitions used in this model.

In the DoD cases, the work flow is more complicated still because there is a diaspora of datasets that could inform the actions, some of which are under disparate management within the Department, and some outside the Department, as well. As we observe elsewhere the data models/architectures for the identity management system are critical, as are the hardware and software systems architectures in which the data are embedded. Moreover, for most critical biometric-enabled processes today, there are humans in the loop responsible for quality assurance.

Observation: Enterprise-wide systems analysis has not yet been brought to bear on the identity-management processes that support DoD missions. The business and work-flow processes are neither documented nor fully understood, it seems, and it is not clear where the accountability for these lies.

Recommendation 2 : The PSA for biometrics, in lieu of a PSA for identity management, should assign the accountability for analyzing, documenting, and refining the business and work-flow processes and systems architecture(s).

Biometric Indices

Biometric indices have unique characteristics. Different applications of biometrics, different "use cases" or scenarios, place different demands on the biometric indices. Some biometrics are better suited than others to a specific use case. Figure 4 suggests a relevant set of attributes by which the suitability of the array of biometric indices might be judged.
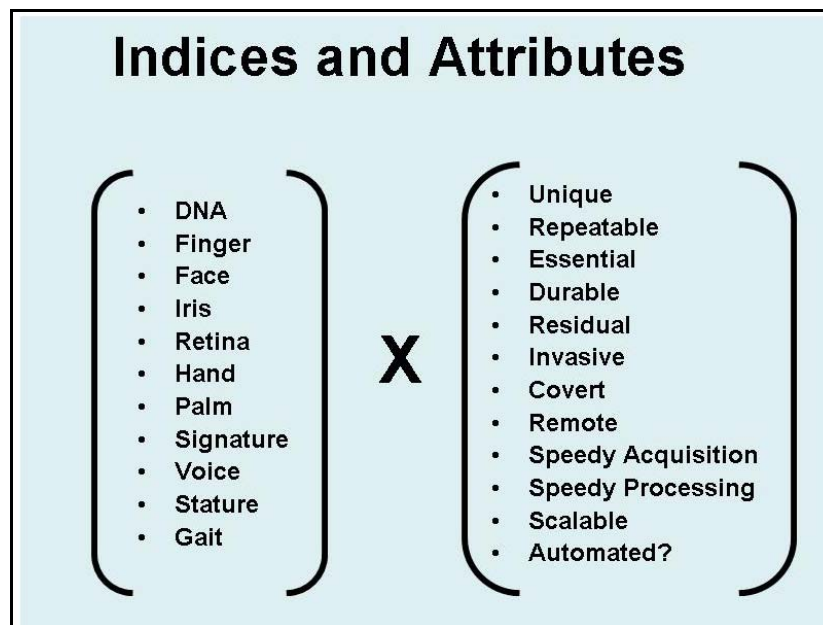
Figure 4: Biometric Characteristics

In the table at Appendix O, Biometric Modalities Matrix, we evaluate a relevant subset of possible biometric indices against a set of appropriate attributes according to our understanding of their state of maturity as of this writing[13]. Some of these modalities that are of most relevance to DoD activities are discussed in further detail in the following sections.

Facial Recognition[14]

Facial recognition is clearly something that humans rely on daily, yet experience tells us that either we are not perfect at it, or faces/facial features are not all that unique. Both are likely true, and until recently, humans were about as good at facial recognition as computers,

---

[13]. It is important to note that there are a number of such short-form analyses extant, and all of these are somewhat different in format and/or content. The Task Force drew from existing work, personal knowledge and experience to derive the issues deemed to be of greatest relevance to the DoD, as reflected in the format here. See, *inter alia*, www.biometrics.gov/referenceroom/introduction.aspx; also www.biometrics.gov/docs/biooverview.pdf

[14] Additional information about face recognition technology can be found at www.biometrics.gov//docs/facerec.pdf

Facial recognition is vulnerable to disguise. Everyday experience suggests that if we are trying to avoid recognition, disguise can be moderately effective, but if we are trying to impersonate someone else, disguise is likely to be somewhat less effective. Notwithstanding, it is a convenient biometric because it is one of the few that is both "machine-readable" and "human-readable" so it is generally used for identification cards and badges, although it should generally be used in combination with other biometrics, *i.e.*, multi-modal. The ubiquity of surveillance cameras means that, in a sense, a face can leave a trace and therefore be useful forensically, as are DNA and fingerprints. As the resolution and other performance characteristics of these improve, Facial Recognition (FR) will become increasingly viable as a reliable identification tool.

Obviously, FR is also attractive from the standpoint of the opportunity it represents to detect, verify and track at some distance. It is not alone in this attribute, and performance is not yet optimal, but we may highlight this aspect of FR as an important avenue of future research effort. (See chapter 12).

Man Against Machine

Humans are not used to matching fingerprints, or DNA, but we do have a lot of practical experience at recognizing and recalling human faces[15]. How good are we compared to the current state of computer facial recognition?

Recent research, sponsored by several interested federal organizations[16], suggests that we are not all that bad at it. Or, said differently, computers aren't all that much better. Figure 5 maps the probability of a correct recognition against the probability of a false acceptance in identity matching of "difficult face pairs."[17] While there were two or three machine algorithms that surpassed the performance of the humans, we humans did quite well, and managed to beat out the majority of the machine algorithms. In this same paper, most face systems easily beat human performance on "easy face pairs."

---

[15] Studies have shown that individuals are good at recognizing faces they are familiar with (family, friends, celebrities, etc.), but not so good with unfamiliar faces. Individuals also tend to be better at distinguishing faces within ethnic groups that they have the most contact with (someone that doesn't personally know someone from a particular ethnic group will have difficulty distinguishing faces from that ethnic group).

[16] Federal Bureau of Investigation, National Institutes of Justice, Department of Homeland Security and the Technical Support Working Group.

[17] Alice J. O'Toole, The University of Texas at Dallas, *Human vs. Machine Performance*, research sponsored by the TSWG, USG.
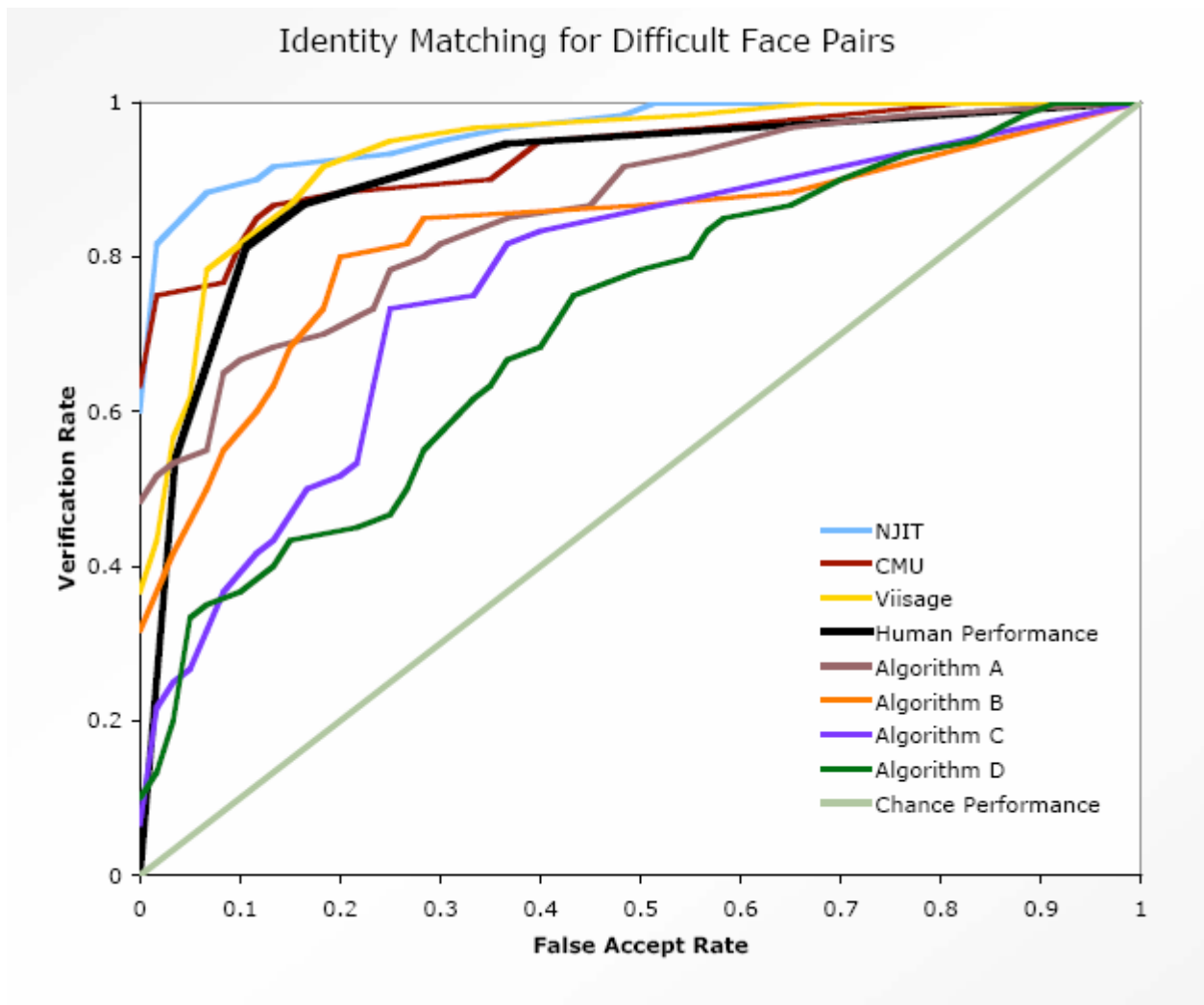
Figure 5: Facial Matching Performance Curves

Of course, the computer is significantly faster, but the same research did show that humans aren't all that slow; our performance did not improve if we took longer than two seconds to contemplate the faces. Human performance did decline noticeably if the faces were only shown for a half second or less. Ultimately, though, computers will be increasingly fast and powerful, increasingly small and inexpensive, and have access to ever-improving matching algorithms. In the Task Force's view, this is the key insight: At the same time, collection devices (cameras) will also increase in ubiquity and performance. Taken together, these conditions are expected to lead to strong advances in the prevalence and performance of automated FR applications. The emergence and refinement of "3D imaging," as discussed later, will only serve to accelerate this trend. The "Rubicon" will be the acceptance of FR, given these enhancements, as an operationally-practical modality for accurate, high-volume and high-speed search, which it is not today.

Fingerprints[18]

Fingerprint Identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips. One can hardly be unaware of the fact that criminal Identification by means of fingerprints is one of the most potent factors in apprehending fugitives.

According to the FBI, no two persons have exactly the same arrangement of ridge patterns, and the patterns of any one individual remain unchanged throughout life, in which case, fingerprints offer an infallible means of personal identification.

Fingerprints can be recorded on a standard fingerprint card or can be recorded digitally[19] and transmitted electronically to an authoritative service provider such as the Biometrics Fusion Center, or the FBI for comparison. Alternatively, they can be compared locally.

A Fingerprint Vendor Technology Evaluation (FpVTE) 2003 was conducted by the National Institute of Standards and Technology (NIST) to evaluate the accuracy of fingerprint matching, identification, and verification systems[20]. Additional evaluations include the testing of the FBI IAFIS system, the US-VISIT IDENT system and SDKs (Software Development Kits) from several vendors. Eighteen different companies competed in FpVTE, and 34 systems were evaluated. Different subtests measured accuracy for various numbers and types of fingerprints, using operational fingerprint data from a variety of U.S. Government sources. The most accurate systems were found to have consistently very low error rates across a variety of data sets. The variables that had the clearest effect on system accuracy were the number of fingers used and fingerprint quality. An increased number of fingers resulted in higher accuracy. The accuracy of searches using four or more fingers was better than the accuracy of two-finger searches, which was better than the accuracy of single-finger searches. The test also shows that the most accurate fingerprint systems are more accurate than the most accurate facial recognition systems, even when comparing the performance of operational quality single fingerprints to high-quality face images.

Iris Recognition[21]

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent only since 1994.[22] As shown in Figure 6, the iris is a muscle within the eye that regulates the size of the

---

[18] Additional information about fingerprint recognition can be found at www.biometrics.gov/docs/fingerprintrec.pdf.

[19] For "how-to" information on fingerprinting, see http://www.fbi.gov/hq/cjisd/takingfps.html

[20] http://fpvte.nist.gov/

[21] Additional information about iris recognition can be found at www.biometrics.gov/docs/irisrec.pdf

[22] John Daugman, "Iris Recognition for Personal Identification," The Computer Laboratory, University of Cambridge <http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html>.

pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Iris recognition has long been dominated by a single vendor, but with the recent expiration of the iris recognition concept patents, additional options now exists. The multi-agency Iris Challenge Evaluation[23] was developed to assist their development and to independently assess their capabilities.
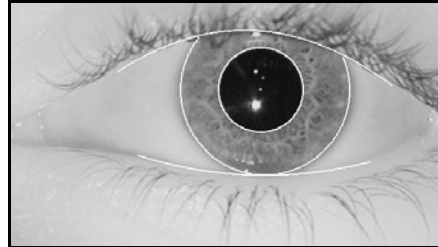
Figure 6: The Human Iris

White outlines indicate the localization of the iris and eyelid boundaries.[24]

Before recognition of the iris takes place, the iris is located using landmark features. These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance.

Iris imaging requires use of a high quality digital camera. Today's commercial iris cameras typically use infrared light to illuminate the iris without causing harm or discomfort to the subject.

Iris recognition is a biometric modality with unfulfilled promise. While widely recognized for having several desirable traits (such as uniqueness and stability), iris recognition is still considered to be risky due to limited market competitiveness/maturity and difficulties with usage for some individuals or in some environments (enrollment failures and user accommodations).

Most tests of iris recognition products have yielded indications of very high performance in terms of matching error rates, particularly the false acceptance rates (FAR). However, the results also indicate that some sensors are very difficult to use, resulting in high failure to enroll (FTE) rates and slow transaction times. Iris recognition has difficulty operating in outdoor environments, and some adverse lighting conditions can induce significant levels of false reject rates (FRR).

---

[23] rris.nist.gov/ice

[24] John Daugman, "University of Cambridge: Computer Laboratory: Webpage for John Daugman" <http://www.cl.cam.ac.uk/users/jgd1000/>.

Additional RDT&E is needed in making easier to use and extended-range sensors, hyper-range sensors (that can collect face and iris imagery at once), statistically-relevant assessment of iris system capabilities, and developing iris image quality metrics to aid in enrollment and/or recognition decisions.

Vascular Recognition

Vascular recognition[25], a relatively new biometric modality, takes advantage of the fact that the network of vessels in each person's hand forms a pattern that reportedly can be distinguished from anyone else's. The leading manufacturers of these vascular pattern recognition devices, TechSphere, of Seoul, South Korea, and Japan's Fujitsu and Hitachi, claim to have sold tens of thousands of them in Asia and Europe.

Reportedly, vascular recognition has wide acceptance in banking, especially in Japan where ATMs featuring vascular sensors are in operation. These meet the country's Personal Information Protection Act, April 2005. Vascular sensors, in preference to fingerprint scanners, cater to certain cultural sensibilities: users prefer not to have to touch the sensors in order to conduct transaction, a concern in some Asian countries where hygiene is an exceptionally important cultural value. The user simply holds a hand near an infrared light source, paired with a charge-coupled device. As the near-IR passes through the body tissue, it is reflected by the hemoglobin in the blood. This reflected light, picked up by the CCD, reveals an image of the blood vessels. Subsequently, as with other biometric sensors/systems, a template is developed and enrolled or matched to a reference.

DNA[26]

DNA encodes sufficient information for those defining characteristics of the organism that trace to "nature" as opposed to "nurture." While neither quick nor cheap to process, DNA must be the most unique of biometric indices. Another endearing trait of DNA is the fact that, as with latent fingerprints, residual traces of DNA can frequently be found "at the scene." The residue, or on common articles of use, means that we do not require the subject's cooperation or even awareness to "enroll" said individual. DNA also contains pointers to forebears, offspring and other relations; and DNA can betray certain medical conditions of interest. These last two characteristics of DNA are a bit of a mixed blessing for us. Genealogy is quite interesting in a variety of intelligence scenarios, but raises high the "privacy" flag, as does the collateral medical information.

A growing awareness of Identity Management by the medical community is leading to the convergence of medical biometrics capabilities for medical treatment, with Identity Management.

---

[25] See, for example, *IEEE Spectrum*, Nov. 2006, p. 16

[26] As previously noted, DNA is not universally accepted as a biometric modality at present. However, the TF has chosen to treat it as such in this report.

For the last fifteen years, DNA has played a significant role in the mortuary affairs of the Department of Defense. At that time, The Assistant Secretary of Defense for Health Affairs was authorized to:

> "…establish policies and requirements for the use of DNA analysis to aid in the identification of remains … [and to] establish a registry to carry out those policies and meet those requirements. The registry may include a DNA identification laboratory and an appropriate specimen repository."[27]

In 1993 the US Army Surgeon General became the Executive Agent and overseer of the Armed Forces DNA Identification Laboratory (AFDIL) and the Armed Forces DNA Repository, more precisely, the Armed Forces Repository of Specimen Samples for the Identification of Remains (AFRSSIR)[28], from which specimen samples can be extracted when required. The repository currently contains nearly 5 million specimens inside freezers kept at -20^C. The repository is held strictly to its military mortuary purposes except on court order or with permission of the "owner" of the specimen.

Original purpose notwithstanding, the world-class expertise of the Identification Laboratory (distinct from the "blue force" repository) has been used effectively for DoD forensic counterterrorism purposes and, in February 2001, the "Black Helix" concept surfaced:

> "A secure repository and interactive database, which will focus on archiving, retrieving, and interpreting bio-molecular data for the identification and tracking of terrorist suspects."

Historically and at present, AFDIL has a unitary medical reporting chain, notwithstanding the convergent trends cited above between the medical DNA and IM communities generally. In AFDIL's case, it has been determined that the counterterrorism mission, no matter how important, is not a "medical mission," and in many cases "not a military mission" so AFDIL must operate as an "Economy Act Contractor Only". What are the "use cases?"

- Prison Escapees/Released Detainees – Red Force
- Relatives of persons of interest (insofar as DNA permits familial searches, not just one-to-one.
- Evidence from IED incidents (TEDAC)
- Personal effects and LCN DNA (Single Cell Laser Capture)
- Human remains from suicide bombings (AFME)
- Force Protection – Gray Force access and employment – "DNA analysis in the field"
- Force protection – Blue Force – personnel recovery

Who are the customers/partners in this line of work?

---

[27] Donald J. Atwood, Deputy Secretary of Defense, 16 December 1991.

[28] Per: 10 USC 176 and 177; DODD 5154.24; DODI 5154.30.

- National Detainee Reporting Center (NDRC)
- National Ground Intelligence Center (NGIC)
- Defense Intelligence Agency (DIA)
- Terrorist Explosive Device Analytical Center (TEDAC)
- Combined Explosives Exploitation Cell (CEEC)

This is a growth area. The workload is significant and has already resulted in a database, the Joint Federal Agencies Intelligence DNA Database (JFAIDD). The JFAIDD contains 15,000 DNA profiles, with 17,000 samples processed (turning up 2, 000 duplicates); a queue of 30,000 new samples in the laboratory; and 400 requests for DNA profiles, searches, or comparisons: 75% by DoD; 5% by the Intelligence Community; 5% by Law Enforcement; and 15% from TEDAC—FBI/DoD, and counter IED.

Currently, the field operational utility of DNA is held back by the delays inherent in the physical transport of the specimens to the lab, and the costly and lengthy processing. All of this should yield to technology some day, the sooner the better.

Recommendation 3: The PSA for biometrics should undertake to develop field-deployable DNA collection and matching equipment that requires less skill to achieve operationally worthy results, and the data architecture for accessing repositories for match should be designed and deployed apace. Additionally, the PSA, in coordination with appropriate authorities, should investigate options related to organizational, physical and/or data collocation with other/larger elements of the total DoD biometrics/IM enterprise.

The Task Force also validates the AFDIL need for:
- A DoD charter, policy and strategic vision, and military medicine is unlikely to be a sufficient champion for DoD biometrics;
- A durable funding stream—funding is currently non-DoD economy act transfers—and/or a working capital fund, as well as accurate projected workload;
- Policy and interagency agreements for sharing DNA biometric data and casework with other federal agencies and allies;
- DoD (and other) consumers of DNA biometrics identified, trained and interconnected; connectivity required, *inter alia*, with BFC, NFIC, DIA, and COCOMS;
- Access to foreign populations of interest for "baseline."

Recommendation 4: DoD should formally assign to Armed Forces DNA Identification Laboratory (AFDIL) the ancillary forensic/counterterrorism intelligence mission(s) and provide oversight, policy and fiscal guidance, and connectivity as required.

Biometric "Residue"—Forensics

A special characteristic of some biometrics is that an individual can leave traces of his or her being "at the scene". Latent fingerprints are the common example, along with DNA. In this modern, surveillance-happy world, voice and face can also be a part of the record at the scene, generally with the advantage of being time-date stamped. To the trained canine, human scent, too, can remain at the scene for some considerable time after the subject has left. And, in addition to these figurative "footprints" there are always literal footprints which can sometimes yield information about body characteristics such as height, weight, sex and gait.

While it is difficult to imagine new biometrics that might leave a similar identity residue, the value of such could be high for certain DoD and law enforcement missions.

Processing the Biometric

Compression Losses

Consider for a moment the process of extracting information, the biometric, from an organism. The individual presents a body part; the "system" illuminates, stimulates, or passively receives energy; transduces it into a convenient form and extracts relevant information. Almost always, there is some "compression" of the originally sensed information. For example, in an image, the original pixelization, color mapping, and perhaps subsequent jpeg encoding provide compression. Beyond the "imagic" representation, the "system" extracts and encodes "features," facial landmarks, fingerprint "minutiae," *etc*., which provides additional compression.

In the information domain each of these steps reduces to a more manageable size the number of bits necessary to represent the relevant information, *i.e.*, "compression." Sometimes the compression is thought to be entirely reversible, a "lossless" compression. More often the compression is not entirely reversible, a "lossy" compression. Figure 7 demonstrates these relationships.
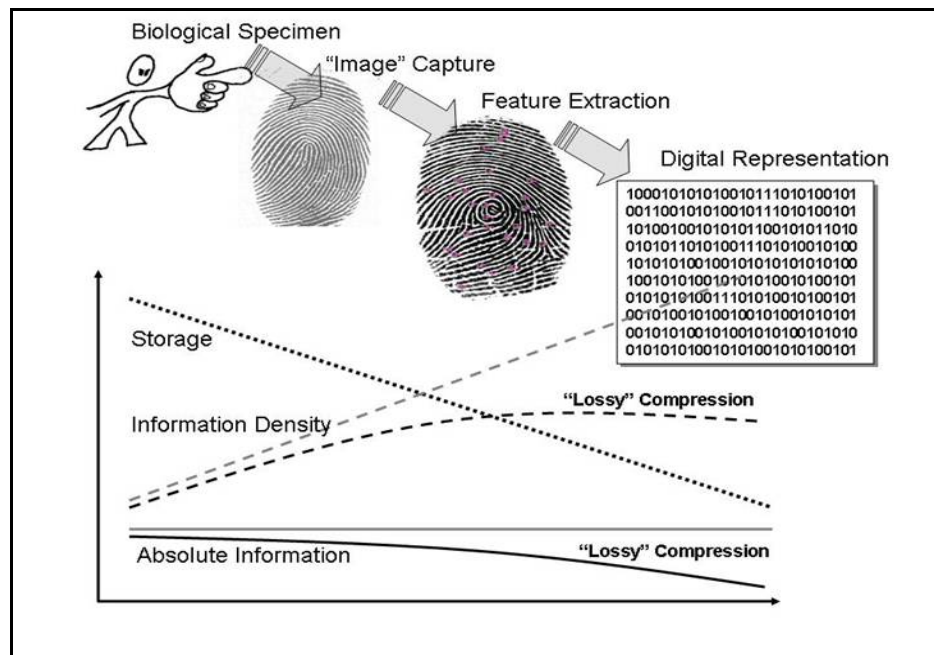
Figure 7: Compression Curves

In the world of digital imaging, going from, say, a NEF to a TIF, to a JPEG represents lossy compressions; you cannot recover fully the original image from the JPEG. A simpler example: we "round" numbers. Once rounded up or down we can no longer retrieve the original number.

We strive to ensure that in processing the biometric our compression algorithms do not lose "vital" information. In practical terms, this means that we hope that the encoded information is

functionally as unique as the original, and as easily processed, *i.e.*, compared. Almost inevitably, information is lost. If we fail to save the original, we may be frustrated at a later date when a newer and better algorithm is developed and our previous encoding has inadvertently discarded now-essential information, which we now can no longer recover. If so, the value of our legacy repositories of identity information is devalued.

Finding: A decision to save only the extracted information and discard the "original" entails future risk and serves only to conserve computer storage and processing, each of which is getting cheaper and cheaper. Because the value of a legacy identity database grows non-linearly with the number of individuals, that is, the utility grows faster than the size of the database, discarding the "original" is likely a false economy. It is, however, sobering to "do the math". The FBI digitization standard of 500dpi yields a fingerprint record of 10mb. Lossless compression, in practice, seldom does better than 2:1. The FBI has some 200 million fingerprint cards and its automated system topped 52 million records last July, with 6,000-7,000 new accessions per day. They handle 65,000 service requests per day.

Recommendation 5 : Department of Defense policy should tilt toward saving the "original" biometric (in high resolution) rather than relying only on the processed metric/template.

Quite incidentally, the business process of maintaining a database of DNA for the identification of remains entails saving the original biological specimen. Here, the business case argues that, today, the processing is expensive and, anyway, most specimens will not need to be processed, ever. The underlying principle, however, is consonant, namely that processing techniques are bound to improve in the future.

Another "Compression" Danger

We rely on certain biometrics because they are acceptably unique. When, however, we rely on a transform of the biometric we run the risk that the transform may no longer maintain the same uniqueness properties. While it may remain true that the original biometric, transformed, may still map uniquely, there is the possibility that other, non-biometric presentations, purposefully constructed to deceive, may be able to map to a target identity, that is, generate the template that will match the target identity.

Hits and False Alarms—Costs and Benefits

Taking a biometric measurement is a "noisy" business as is the process of comparing it to samples in a database. In each instance where a "target" biometric sample is compared to a biometric record in the database(s) we can entertain two hypotheses: (1) the comparison corresponds to an actual match, the "ground truth" or (2) the comparison does not, in fact, correspond to an actual match. The "system"[29] makes its best guess according to its (decision) rules as to whether the two samples, the target and the record, match. The system may have decided that there was a match, or not.

In Figure 8, there are two possible ground-truth inputs to the system, true match, or not, and two possible responses accordingly, match, or no match.

Figure 8: Identification Decision Matrix

The values in the payoff matrix can vary. Sometimes, the cost of a false alarm is very high while the cost of a miss is relatively inconsequential. In this case, the (rational) "system" will adjust its behavior, *i.e.*, bias its "response" toward "no-signal" (when it is uncertain). The effect is to vary the criterion, which can "bias" the system's response toward signal or non-signal and, therefore, change the ratio of hits and false alarms (also known as "Type II errors"). Our system of criminal justice, for example, purports to be biased against false alarms, "…beyond a reasonable doubt."

Another factor also comes into play in determining performance under any given set of costs and benefits, the *a priori* probability that a true match or non-match will be presented.

---

[29] Note that the "system" can be totally automated, or be a "man-machine" system, or be totally manual, it matters not for this discussion.

A familiar example sad, but understandable, is the guard at the entrance to a facility looking at picture badges. Overwhelmingly the individuals are presenting their own badges and the pictures match the faces to a first approximation. Result: a cursory, "rubber stamp" examination and a casual wave-in. The exception might be under a heightened threat condition which says, in effect, the *a priori* probabilities have changed, we are expecting trouble, perhaps in the form of an intruder, and, perhaps, the costs and values in the payoff matrix have changed likewise so that we don't mind annoying and delaying the innocent.

The traditional way of visualizing the system performance is a "Receiver Operation Characteristic" (ROC curve), as shown in Figure 9, where "signal" represents "match" and "noise" represents "no-match".
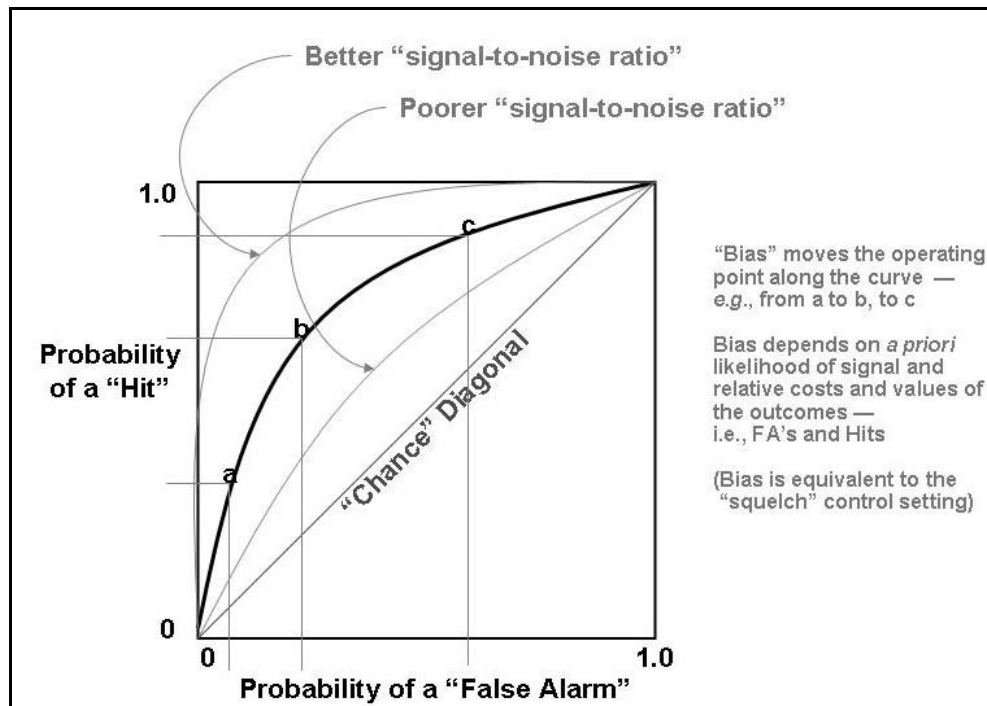
Figure 9: Receiver Operation Characteristic Curve

In the real world, some biometric indices are simply not sufficiently accurate for the intended application, no matter how we adjust the criterion. This may be because our implementation of the biometry is poor, or because the biometric is simply not sufficiently unique in the population of interest. In the real world, too, the biometric system may be additionally stressed by having to render its decision "hastily" (or "promptly" depending on whether you are the designer or the user.) If more exhaustive processing could improve sufficiently the quality of the match, then the inexorable Moore's law gives us hope.

Biometrics Goes to War

As Fran Townsend[30] observed, the transformation of our armed forces to counter the threats of asymmetric warfare introduced a new military mission: the collection of biometric information from the foes we face on the battlefield. Figure 10 illustrates an obvious case. "The U.S. government is building a comprehensive biometric screening regime to detect terrorists before they attack. Our border security, visa screening, and law enforcement systems are based primarily on fingerprints: permanent and unique identifiers that are difficult, if not impossible, to counterfeit or alter. So when a terrorist is captured in the field or a safehouse is raided, it is important to "freeze" the terrorist's identity so that he can always be identified as an enemy and a potential threat. False names, passports, and nationalities cannot mask the data found in fingerprints or DNA. The Department of Defense, with the full support of the White House, has recognized the collection of biometric identification as a basic warfighting capability, especially when fighting insurgent enemies who hide among the civilian populations."

Figure 10: Criminal Enrollment

According to the FBI, among the terrorists and insurgents that we are fighting overseas, roughly 1 in 100 has a criminal record in the United States, which means that many of the people we are fighting today not only have been in America and in our hometowns but also have committed a crime while they were here. [31]

As Townsend emphasizes, "it is important that every biometric identifier: every fingerprint, photograph, DNA swab, or iris scan, is collected correctly and precisely the first time because there may be only this opportunity to ensure the safety of our troops, families, and nation."

As we have pointed out elsewhere, it was the sudden introduction of this new mission that appeared to fragment the Army's ongoing biometrics program, which was then oriented toward information assurance and (peacetime) access control.

---

[30] Frances Fragos Townsend is Assistant to the President for homeland security and counterterrorism.

[31] See: Paul J. Shannon, *Fingerprints and the War on Terror, An FBI Perspective*, JFQ, 43, 2006.

Scenarios ("Use Cases")

We can come up with an endless set of scenarios in which biometrics might be called upon to play a role. Our thesis is that with a little analysis and a little abstraction without losing the essence, the extensive array of scenarios can be reduced to a compact set of "use cases." This compact set of use cases will help us appreciate our companion thesis, that a common "back office" process services all the biometric use cases and thus fully describes "identity management," writ large. The first major dichotomy in the taxonomy of biometric use cases is the distinction between "recognition" and "identification" or "verification."

Identification vs. Verification vs. Recognition

Identification is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database (identification is sometimes referred to as a one-to-many comparison). One possible outcome, of course, is that the sample is found to be new/unique, which is the desired outcome in initial registration/enrollment of a "friendly" population.

Verification is a task where the biometric system attempts to verify an individual's asserted identity. In this case, a new biometric sample is captured and compared with the template stored previously with the asserted identity (verification is sometimes referred to as a one-to-one comparison). If the two samples match, the biometric system confirms that the applicant is who he/she claims to be.

Recognition is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled.

The same four-stage process, biometric capture, feature extraction, feature comparison, and decision, match/non-match, applies equally to identification and verification. As stated, identification/recognition involves matching a sample against a database of many, whereas verification involves matching a sample against a database of one. The key distinction between the two centers on the questions asked by the biometric system and how these fit within a given application.

> During **identification**, the biometric system asks, **"Who is this?"** and establishes whether a biometric record exists, and, if so, the identity of the enrollee whose sample was matched.

> During **verification**, the biometric system asks, **"Is this person who he/she claims to be?"** and attempts to verify the identity of someone who is using, say, a password or smart card.

Intellectually, the distinction can be made to disappear in a more expansive regimen: an individual presents himself/herself to the "system."

A biometric is captured, and implicitly or explicitly the system asks, "Who are you?"

- If (a registered) identity is asserted by the individual or imputed from a token, the system uses that identity information to index into the database(s) to retrieve a sample and compare.

    o If, however, the identity asserted is not found in the database(s) we can conclude:

        - The individual has not previously been "enrolled," in which case

            • We might then enroll the individual, collecting collateral data, an imputed identity, and associating that in the database(s) with the biometric, or;

        - The asserted/imputed identity is "suspect," either not the identity under which the individual was enrolled or the individual was never enrolled, in which case;

            • We should choose to proceed as if no identity was asserted or imputed.

- If no (registered) identity is asserted - an uncooperative subject - and/or no collateral information from, say, a token is available; the system performs a one-to-many search through the database(s).

- If no (satisfactory) match is found we conclude that we did not "know" the individual and, logically, we would "enroll" that individual.

Several things should be noted. The cost in time and resources to do a non-indexed exhaustive search and compare our "one-to-many" case is high and the delay may be intolerable. That is why, when circumstances permit, we prefer to (first) do an indexed retrieval and a single comparison, our "one-to-one" case. This is a concession to (current) reality. Note also the mutually-supporting roles of biometric and biographic information within an IM system. The biometric processes described here are of particular value in resolving potential confusion, or possibly even claims, of "one identity," based on biographic characteristics, by two people.

It would be logically simpler, and actually preferable, to always do the end-to-end search and compare the individual's specimen to all samples in the database(s). Note that otherwise, we are implicitly assuming that the database(s) are "de-duped" *i.e.*, that there does not exist (unknowingly) two different "identities" with the same biometric.

This means, of course, that each sample, at some time in its lifetime, should have been compared with all other samples (our old, one-to-many case) and every newly enrolled identity should be compared with all the identities in all database(s). The saving grace is that these exhaustive comparisons can be done in the "background" when time is not of the essence.

Scenarios and Vignettes

The Task Force solicited "use cases," in the form of scenarios or vignettes of biometrics in action, from all its government advisors and added its own experience and imagination. Perhaps the most comprehensive and authoritative set are provided as "operational vignettes" in the

Capstone Concept of Operations For DoD Biometrics In Support of Identity Superiority[32], which are presented in their entirety in Appendix E.

Interestingly, the military medical community provided two biometric-use scenarios, only one of which was identity management. Lest we forget, medical diagnoses also make use of biometrics—*e.g.*, pulse rate, blood pressure and blood type. The medical and mortuary scenarios are also presented in their entirety in an appendix.

Appendices E through N of this report detail the use cases identified by the Task Force, including those sourced from other elements of the federal government in which Defense missions are impacted or DoD capabilities evoked.

---

[32] *Capstone Concept of Operations (CONOPS) For DoD Biometrics In Support of Identity Superiority* (DRAFT, version 2.0 dated 8 JUL 06)

Research, Development, Testing & Evaluation: Needs, Opportunities and Capabilities

It is clear that certain demanding scenarios require, and all benefit from, improvements in biometrics: their capture and their algorithmic processing and matching. Traditionally, the government research funding establishment follows one or more of three strategies: broadcast the needs and buy from among the offerings; find the competent researchers and ensure that they are properly motivated and resourced; and ferret out good ideas and pursue them. The Task Force prefers the last, but good ideas are traditionally hard to come by.

It is important, however, that any federally sponsored research be in touch with the commercial marketplace. Any fruits of the research must translate promptly into products that are producible by the US industrial base and broadly marketable by the US commercial sector. Accordingly, federally-sponsored research must be linked into the federal acquisition process, so that when these products are available, government is able to procure them. This requires involvement of acquisition professionals throughout the research planning and implementation processes.

Not surprisingly, this is not the only study of biometrics ongoing. In addition to this DSB study and the ongoing joint Study of the Naval Research Advisory Council and the Army Science Board, the National Academies' Computer Science and Telecommunications Board (CSTB)[33] has an ongoing project, *Whither Biometrics.*[34] In a 2005 workshop, they provided their sense of the challenges for biometric technologies and systems, as:

1. Improving accuracy of biometric technologies and related performance evaluations through research on sensor resolution and ergonomics; algorithms and techniques for biometric fusion; characteristics of biometric feature spaces; and scientific methods to better quantify performance under realistic conditions.
2. Systematically and thoughtfully integrating biometric systems with other security systems.
3. Interoperability of biometric systems, especially internationally, through a framework of standards, test methodologies, and independent evaluations.

The Workshop also made several recommendations for improving research in the field of biometrics:
1. Improve the consistency of review policies by using a peer-review process (such as is used for journals) to facilitate repeatability, documentation of experiments, and executability.

---

[33] The **Computer Science and Telecommunications Board** (CSTB) established in 1986 provides independent advice to the federal government on technical and public policy issues relating to computing and communications.

[34] http://www7.nationalacademies.org/cstb/project_biometrics.html

2. Provide access to large data sets and different types of data, such as multimodal data, to measure performance improvements and find ways to increase the amount of data used in biometric performance studies.

3. Develop challenge problems to guide academic research and to create a baseline for comparisons and independent evaluations.

4. Increase the documentation of government-funded and proposed research

Each recommendation is quite straightforward and the Department could not err in accepting all of them.

One view holds that the impact of R&D, in many cases, has diminished over the past few years. There is no more low-hanging fruit; USG multi-year research efforts are virtually non-existent, and the priority problems require "multiagency" focus. Fortunately, there is recent progress in just this area.

In August 2006, the National Science and Technology Council Subcommittee on Biometrics, the established federal interagency lead for biometrics matters, published the *National Biometrics Challenge*[35] (NBC). The reader is directed to this document for general, up-to-date information and, in the context of this section of this report, two specific sections: *Biometrics Challenges; Research Focus and Benefit*; and the *Federal Government's Role in Biometrics Advancement*. The NBC states that "significant progress is required for the U.S. to realize fundamental improvements across all biometric modalities and thereby enable more advanced operational systems."

The NBC establishes four "primary driving forces" in the broad pursuit of biometrics capabilities:

- National Security
- Homeland security and law enforcement
- Enterprise and e-government services
- Personal information and business transactions

The Task Force notes that although the first named item, National Security, is clearly the premier mission of the DoD, all four of these "forces" impact on the missions and operations of the DoD, now and increasingly in future. This point even applies to "law enforcement," based on the assigned role of DoD under HSPD-13/NSPD-41, *Maritime Security Policy.*

Consideration of these driving forces led to the identification of four "preeminent challenges" in the NBC document: sensors, systems, interoperability, and social issues of communications and privacy.

---

[35] *The National Biometrics Challenge,* National Science and Technology Council, Subcommittee on Biometrics, August 2006, http://www.biometrics.gov/nstc/publications.aspx

The subcommittee's agenda for sensors focuses on: rapid collection of face, finger and iris data under harsh field conditions; quality collection of non-cooperative users at a distance; and biometrics templates that can be revoked and replaced when compromised. An interesting approach proposed is development of sensors that automatically recognize the operating environment and adjust to deliver optimal data.

On the systems' side, the subcommittee would focus research, *inter alia*, on enhanced matching algorithms and integration of multiple sensors, matching algorithms and modalities in a single system. Two other systems issues of note, besides the usual call for standards and interoperability, are: modeling the return on investment (ROI) for applications of special interest; and analysis of the scalability of biometrics systems.

As previously discussed, the DDR&E has assumed the lead in coordinating biometrics RDT&E efforts across the interagency. This important role will permit DoD, the largest investor in this class of research, to be cognizant of related efforts in other federal organizations. At the same time, as DoD seeks to meet its own current and future biometrics mission needs, it can be attuned to opportunities to support the total government biometrics effort through technology migration, and sharing of research data as appropriate. It is important for the Department, having accepted the interagency research lead, to endorse research across the broad spectrum of biometric opportunities and needs. Notwithstanding, the PSA should ensure the Department's own unique needs, mission specific applications, have first claim on DoD research resources. Beyond satisfying expressed warfighter requirements, the PSA should anticipate emergent "urgent needs" and seek new opportunities for "battlefield biometrics." Our premise is that very much of this DoD work will find value and application elsewhere in government, for all the reasons we cite throughout this report, regarding interoperability, the growing scope/span of biometrics and IM applications, etc.

The Task Force has tried to shape a research agenda that would fully support the NBC's goals, and yet be relatively specific to the needs of the Department. The specific areas singled out include:

- Multi-modality
- "Spoofability"
- Standoff
- Covertness
- New Measures
- Speed of Response
- Environmental Effects
- Race, Ethnicity and Gender Effects
- Residual Indices other than Fingerprints and DNA
- Measurements, Statistics, Testing & Evaluation
- Technology Insertion
- Product Assurance
- Return-on-Investment (ROI) Modeling
- Scalability

Each is described briefly in the subsequent subsections, including one or more specific developmental priorities recommended by the Task Force. The recommendations are *generally* ranked from highest to lowest, as appearing here. As the lead for biometrics R&D, all recommendations for action in this chapter are directed toward the PSA for Biometrics.

Multi-Modality—the Power of Two or More

The Task Force believes that DoD missions supported by biometrics would benefit substantially by using not just one but a combination of biometric indices. Not only would the accuracy be improved, by as much as the square root of N in the case of completely independent indices, but the ability to cross-reference across databases of collateral information would be too. The Task Force anticipates that the development of doctrine, tactics, techniques and procedures (TTP) that we recommend be undertaken by USFORCECOM will endorse the use of multiple biometrics.

> When an individual presents, never miss an opportunity to collect multiple biometric measures as well as a standard set of biographic information.

For most operational scenarios, "face" will probably be one of the measures because among all the standard biometric measures, it is most useful for human interpretation. Leading contenders, today, appear to be fingerprints, iris, and DNA, and perhaps the vascular patterns of the hand which, as described elsewhere, is favored in Asian nations.

A good starting point for our multi-modal doctrine might be the "13-biometric" collection standard (10 fingers + 2 irises + 1 face), toward which our leading allies are leaning. There is also an opportunity to serendipitously capture data made available by other collection. An example would be to use sclera information from some iris scan data. Our basic premise, don't throw data away, supports this principle. Beyond that, focused research into new modalities, especially those closely related to other, existing collection and records may operationalize this approach.

Irrespective of the particular measures, there are certain issues pertaining to the way in which multiple indices are combined, searched, and compared to achieve the desired combination of speed, accuracy, and conservation of bandwidth and computation. There is a good deal of experience in "single-mode" biometrics and a fair understanding of the performance of matching algorithms used in the various systems. We do not yet have that wealth of experience in, and understanding of, multi-modal biometrics. Because processing in multi-modal systems may become a pacing item in their development and deployment, and their interoperability with allied systems, this should rank high in the research agenda established for the OSD PSA for biometrics.

Recommendation 6.: Conduct research focused on defining, verifying, quantifying and improving biometrics collection/matching performance in multi-modal systems. Evaluate alternative methods for comparing and weighting results of matching algorithms of different biometric modalities within a single system; seek to establish optimal mixes/combinations of modalities in various applications and scenarios. Examine issues specifically related to multi-modal data storage and system architecture.

Spoofing

Biometrics add strength to identity management as a means to control access to privileges, but biometric systems also have vulnerabilities, if they can be either evaded (as suggested in Figure 11) or deceived. System vulnerabilities include attacks at the biometric sensor level, replay attacks on the data communications, and attacks on the database, among others.

Figure 11: Access-Control Evasion

For certain national and homeland security missions, there may be serious, well-supported attempts to confound person-identification by the Department that could jeopardize force protection and compromise information security, *inter alia*. State sponsorship of would-be imposters complicates this issue, as do the economic incentives that inspire and fund civilian enterprises to spoof biometrics. Of course, one way to invalidate identity controls is to bypass the biometric "front end" and attack the system elsewhere.

In a strong information assurance setting, this is likely to be the state-supported impostor's preferred method. Because such attacks are not unique to biometrics, although their probability would likely increase as a result of strong biometrics at the front end, we do not discuss these here and suggest that research in this area is the province of the DoD NII/CIO and DIRNSA wearing their information-assurance caps.

Much progress has been made in this area of biometrics technology since a time, several years ago, when published articles[36] [37] were calling attention to the spoofing vulnerabilities of biometric devices.[38] These flaws are, of course, historical and may be mitigated by today's technology. But they exemplify the biometric "arms race," and demonstrate the constant need for "red teaming" and up-to-date intelligence on what a potential adversary is doing, and demand continuing research.

Today, "liveness detection" is commonly employed for anti-spoofing in new systems design, to the extent possible. The goal of this is to determine if the biometric being read is an actual measurement from the authorized, live person who is present at the time. The technology for liveness detection varies with the biometric modality and, in the case of fingerprints, for example, currently works well and should be required, including the back-fitting of such capability in currently-deployed systems that are not so equipped. Where such schemes are practical they have the added advantage of providing some protection to the owner of the real finger or iris. This and other anti-spoof measures are a field ripe for research and experimentation and DoD sponsorship in this area seems warranted.

Recommendation 7.: Conduct continuous "Red-Team" efforts to defeat biometric sensors and systems in use in the DoD (collaboration with intelligence agencies is recommended). Incorporate insights gleaned from these processes into improved systems designs. Incorporate anti-spoofing technology into all practicable DoD biometrics applications, including backfit into existing systems where indicated by operational risk and importance. Maintain visibility into emergent-modality research to seek to spot spoofing vulnerability/opportunity early.

Standoff

Especially in cases where the impostor might pose a physical threat, it would be desirable if biometric identification could be made at a distance. Of course, this can be done in a cooperative setting, where the scanner/reader could be at a "safe" distance but this does not describe the most intense situation, where the need is the greatest.

Standoff also supports our next topic, covertness. With a little imagination, one can extend the standoff notion to identifying suspect individuals traversing a choke point or, better yet, in a crowd. And, wouldn't it be nice to be able to do this from a reconnaissance platform like an Unattended Aerial Vehicle (UAV) or, better yet, from a sensor/seeker on a weapon. Even short of such fanciful goals, the more standoff the better, and force protection scenarios would benefit sufficiently, therefore the Task Force commends this area for research. Logical partners in such research would include the Department of Homeland Security, the FBI, and the Intelligence Community.

---

[36] T Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proceedings of SPIE, vol. 4677, January, 2002

[37] L Thalheim, J Krissler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test," c't magazine, November 2002.

38 http://people.clarkson.edu/~biosal/research/spoofingliveness.html

It is important to recognize that standoff works two ways: we seek to detect and track others at a distance, and we also seek to assert our own identities over similar distances, to obviate "friendly fire," for example. While the two functions may seem similar, the respective biometric techniques are likely to differ.

Recommendation 8.: Support research efforts by DARPA and others into extended-range human biometric identifiability and tracking. Explore feasibility of "unattended surveillance" of larger areas. Examine applicability of biometrically-based capability for long-range identity assertion in operational scenarios.

Covertness

The ability to identify an individual unaware (closely related to the previous topic of standoff identification) would enhance several military as well as law enforcement scenarios. And, non-intrusive, standoff, covert biometric indices appear, on the face of it, to be important in detecting deception in an individual as, for example, in the polygraph.

> Note that latent fingerprints and traces of DNA are certainly part of a covert identification, although enrolling the individual may have been overt. Our research recommendation in the area of covertness, however, goes well beyond trace evidence of an individual's presence and identity.

In passing, we mention here, and expound at greater length in a subsequent section of privacy, that this particular attribute of biometric identification, its covertness or lack thereof, particularly troubles the "privacy community." The lesson to be drawn is that the Department should execute any such research smartly (but not necessarily secretly). As with standoff, logical partners in such research would include the Department of Homeland Security, the FBI, and the Intelligence Community.

Recommendation 9.: Explore and develop technical means to conduct strong-biometric collection under apparently innocuous conditions. This should be possible both within controlled environments (e.g. offices) and otherwise.

New Measures and Applications

While the Task Force has no credible new measures to suggest at this time, it is essential that the research community be attuned to any opportunities, here. Depending on their characteristics, they could complement or supplant measures on which the Department is planning to rely.

Other than the discovery of completely new indices of human biometric measurement, the most promising areas seem to be those looking at new ways to measure and compare human features by using multiple looks, multiple look angles (bistatic collection/matching), and multiple segments of the spectrum. An example is moving from a two-dimensional to a three-dimensional model of the human face. The claims here include a significant improvement in speed of capture and processing, and a significant reduction is subject involvement. Historically, improved accuracy required more time and more subject involvement, *e.g.*, positioning the body part(s) with some care. Although 3D facial technology has the potential to combine high

accuracy with minimal subject participation, the technology is clearly not yet fully developed, and some performance testing has shown uneven results. Nonetheless, this is deemed an important area of future research and development effort.

The technology is based on a structured light method working in the invisible near-infrared range, projecting a light grid onto the face so that the grid is distorted by the individual's facial geometry. These distortions provide the 3D facial template, 40,000 data point are sampled in one proprietary instantiation. Currently, matching engines and algorithms are proprietary.

Another interesting extension of facial recognition is to include not only 3D facial shape, but also facial vasculature by imaging in the visible, near IR and thermal IR bands, thus combining geometry with underlying physiology.

At the same time, it is clear that the Department has only just begun to recognize, develop, and act on the full potential of biometrics to enhance processes of many different kinds, across the entire Defense enterprise. The Task Force recognizes that it will be necessary to maintain an agile, adaptive and continuously-learning technology organization, to ensure that new biometric-application opportunities are spotted and acted upon appropriately.

Recommendation 10.: Quantify, operationalize and improve upon 3D imagery as a basic biometric modality. Explore development of coherent, bistatic 3D imagery collection capability, with cameras separated over some distance. Conduct an ongoing, basic-research (6.0/6.1) effort in biometrics, seeking to discover new modalities, and previously-unknown insights from existing collection and operational biometrics. Seek to identify and operationalize promising new areas of biometrics application, appropriately.

Speed of Response, etc.

In many of the DoD-relevant scenarios, the time-to-identify, and, in most, to retrieve relevant collateral data, is a window of vulnerability we would like to close. For such mission-critical uses of biometrics, there should be a good baseline of the time budget in identification (and retrieval of collateral) *i.e.*, how much time is allotted for acquisition of the biometric, its transduction/reduction, its communication, search time, collateral retrieval time, and return communications. Pieces of the budget that logically fall to the NII/CIO (and the Services, normally thought responsible for the "last tactical mile") should be pursued by them. Emphasis, here, should be on algorithms and device characteristics. These, coupled with dividends from Moore's and Metcalfe's Laws, should improve the timeliness of biometric identification insofar as the Department has a strategy for technology insertion.

Recommendation 11.: The OSD PSA for biometrics should work with ASD/NII, DoJ/FBI and the Services to identify and achieve time-based performance requirements for biometrics data transmission, comparison/analysis and return of results, all in the context of operational needs in the various use cases. Establish programs to develop or modify existing biometrics collection and/or data-routing systems to achieve required timeliness.

Environmental Effects

Relatively unique to the Department of Defense is the need to operate anywhere, in any climate and in any weather. This can, indeed does, put serious constraints on the design, development, acquisition and deployment of military materiel. In many scenarios, the biometric capture device is subject to the same constraints.

A well-rounded research agenda in biometrics, shaped by DoD-centric needs, must include research and development efforts to counter adverse environmental effects.

Recommendation 12.: Given the expected expansion of biometrics applications and use-case scenarios, ensure that field-use biometrics collection and analysis systems are designed to function effectively across the whole range of physical environments. If there are cases where the basic science involved prohibits or inhibits this, identify and document these for the benefit of operational planners.

Race, Ethnicity and Gender Effects

Again, because of the global nature of the DoD mission, it is essential that biometric identification measures be immune to idiosyncrasies of segments of the population(s) it might encounter, or at least that such variances be understood, and their effects measured and accounted for, before the fact.

Any research efforts in biometrics sponsored by the Department must be attuned to the race, ethnicity and gender variables, as well as other prevalent medical/physiological anomalies. Here, of course, the worldwide adoption of biometric based authentication for civilian/commercial applications will drive out these variables, to some extent. Notwithstanding, this area deserves special attention.

Recommendation 13.: Define and measure ethnologic and/or regional differences in performance of biometrics modalities which effect large groups or whole populations. Ensure that these insights are known to operational planners. In cases where such differences can be accounted for by adjustments or controls in collection or matching processes, provide for the means to adjust such settings in field-deployable equipments.

Residual Indices other than Fingerprints and DNA

Here, the scenarios of interest are forensic and/or those which might involve tagging, tracking or locating (including the particularly vexing "naked hostage" problem). Beyond human chemical effluvia (body odors) few ideas spring readily to mind. Still, there are DoD, intelligence and civilian law-enforcement scenarios where this would have high payoff, which suggests partnerships with the FBI and the Intelligence Community.

Recommendation 14.: Support multi-agency research to identify and refine possible new biometric modalities related to residual/latent information.

Measurement, Statistics, Testing, And Evaluation

Measurement, statistics, testing and evaluation are strong supporting players in any research agenda. As the CSTB was presented in their summer workshop, a part of their ongoing project, *Whither Biometrics*:

- Evaluating biometric systems serves three purposes: to guide and support research and development, to assess the readiness of a system for deployment, and to monitor performance of a system in the field.
- As in many other domains, appropriate experimental design and solid statistical underpinnings are needed to produce effective testing and evaluation regimes. There is no one-size-fits-all solution given the many types of systems that are deployed.
- Data and data selection choices, which include understanding the reference and expected user populations, can have a large impact on the accuracy and effectiveness of testing and evaluation.

Recommendation 15.: Ensure that testing and evaluation processes are available and used, as appropriate to the nature and needs of biometrics systems design and modification.

Technology Insertion Strategy

Tthere are some examples where the Department seems unable to realize the benefits of research because of programmatics and/or a flawed/conservative acquisition and deployment strategy. This principle may be extended into the search for new areas of opportunity to field identity-sensitive applications, and/or strengthen existing systems through biometric verification.

Recommendation 16.: Ensure that there is an aggressive technology insertion strategy to complement the research agenda.

Biometric Product Assurance

To support critical national/homeland security and law enforcement missions, federal users of standards-based biometric components and systems require a high level of assurance that the products they acquire conform to selected biometric standards in order to ensure subsystem compatibility and interoperability of their biometric implementations. Proper system planning involves a battery of tests: performance and operational impact assessments (technology/scenario/operational evaluations); standards conformance analyses; systems integration; and interoperability assurance. Vendor claims of conformance via first-party (i.e., vendor) testing are not sufficient in the near term since there is no mature or proven conformance testing infrastructure in place. With the emergence of standards-based test tools for biometric standards, there is now a window of opportunity for the DoD to collaborate within the interagency process to promote the development of a national biometric conformity assessment program. Such a program could utilize second-party conformance testing (e.g., a single government testing laboratory) or third-party conformance testing (e.g., multiple accredited testing laboratories) as the means to produce validated product lists for use in procurements.

The community-wide level of sophistication for each of these tests varies considerably. The DoD should continue to support intergovernmental and community-wide efforts to raise the

sophistication of these test efforts, and to advocate and support advanced efforts to develop those capabilities most critical to DoD-specific needs.

Recommendation 17.: The OSD PSA for biometrics should examine the technical capabilities of the department for biometrics conformance testing capabilities, in cooperation with other federal authorities/capabilities in this area. Upon appropriate coordination, the PSA should support programmatic efforts to establish, maintain and support testing capabilities to support DoD's needs, and role(s) in the total federal biometrics effort.

Modeling Return on Investment (ROI)

Often overlooked in the Department's research portfolios is the need to better model the costs and benefits of success in a research thrust: how do you value the newly enabled capability in terms commensurate with the resources expended and/or other capabilities foregone? As was pointed out by the NSTC subcommittee on biometrics, we have already done the easy, inexpensive stuff, what's left is the hard, expensive stuff. Is it worth it? While sometimes poor at estimating prospectively the costs, the nature of the Department is to be concerned and precise about the costs once incurred. The S&T components of the Department are pretty good as assessing the technical risks. Where there is a weakness, is on the value side: what will the return be?

Recognizing our habitual weakness, the NSTC subcommittee on biometrics argues for the development of modeling tools and techniques, and models of ROI in specific applications. The Task Force agrees.

Recommendation 18.: That the OSD PSA for Biometrics with the USD/Comptroller and Chief Financial Officer, support the development and use of Return-on-Investment (ROI) modeling for significant biometrics applications in the Department.

Scalability

With biometrics (really, identity management) systems as with many others, what works well in small, bounded applications does not necessarily extend gracefully or efficiently to much larger cases. Almost never are there economies of scale in data systems, although there may be in the acquisition hardware, software and communications components, and training.

Data systems tend to scale, at best linearly and generally much worse, non-linearly so that the limits of affordability/workability are quickly reached. We hope to extend key identity management applications across the entire Department and, in many cases, across the federal government; to state, local and tribal authorities; key commercial sectors, to allies and partners; and even globally.

The NSTC subcommittee is correct in citing this area of research as an important one, and the Task Force echoes their sentiments.

Recommendation 19.: The OSD PSA for Biometrics, with the ASD/NII should ensure that scalability issues are addressed specifically in anticipation of scaling key identity management systems and processes globally.

DoD Organizational Issues

The Task Force discovered that even within the relatively narrowly defined field of biometrics, there are a number of DoD organizations performing missions based on historic sponsorship and organizational constructs, arrangements which now should be reexamined in the context of the recent PSA appointment. The goal, of course, is not to suppress the efforts and initiative of DoD organizations, but to achieve a level of visibility, coordination, review and control. This will permit efficient management and realization of economies of scale, while avoiding redundancy to at least some degree.

Recommendation 20.: The OSD PSA for biometrics should create a sub-working group of the DoD Biometrics Executive Committee, focused on biometrics information/data sharing. This group should be co-chaired by the PSA and representatives from USD/P, with additional members to include at least ASD/NII, USD/I, USD/PR and the Office of the General Counsel (OGC). An early task for this group should be an effort to survey and map the total, DoD-wide biometrics/IM data environment, for all applications, as a baseline analysis to support further architectural efforts.

Recommendation 21.: The OSD PSA for biometrics, in coordination with the USD/I, should assume control and direction of the DIA-based National Signatures Program human biometrics effort. He should decide whether or not to continue this new effort; if so on what basis, and with what goals.

Recommendation 22.: The OSD PSA for biometrics should define, with the ASD/Health Affairs and the USD/Intelligence, the creation of Command and Control reporting and programmatic relationships in identity management for the Armed Forces DNA Identification Laboratory (AFDIL) in Rockville, MD.

Policy and Doctrine within and beyond DoD

Many of the policy and doctrinal concerns with biometrics and identity management transcend the Department of Defense and involve "the inters": inter-agency, inter-governmental, international, as well as the commercial sector. For the Department to realize its goal as a visionary, proactive, model organization of biometrics management across the spectrum of defense roles and missions, it must bring into central visibility, if not direct control, the many external activities, equities and organizations which depend on the DoD and on which the DoD depends.

The Task Force validates the need for the Department to be an active participant, stalwart partner, and in many cases leader, in the various external fora: interagency, intergovernmental, joint, allied and coalition, and international as well as industry fora.

DoD Participation in the Biometrics Interagency Process:

The task force strongly advocates active engagement, and leadership, as appropriate, by the Department of Defense in the interagency process related to biometrics because:

- DoD biometrics activities cannot be performed without reliance on data and capabilities resident in other federal departments and agencies, *e.g.,* the FBI's Criminal Justice Information Services Division (CJIS);
- Key DoD missions that depend heavily on biometrics are shared with other federal departments and agencies, *e.g.*, National Strategy for Maritime Security, where DoD partners with the Department of Homeland Security (DHS);
- By policy and technical design, new and emergent federal biometrics/identity management programs overarch, and are mandated to be interoperable across, the entire federal establishment, *e.g.*, HSPD-12[39]-based identity management policies;
- The power of biometrics increases non-linearly with the span of the enterprise, organizationally and geographically, and to achieve such global connectivity, interoperability, standardization and security requires inter-agency and international collaboration;
- The absence of universally understood and agreed upon interpretation of law and policy related to biometrics has led to disparate local interpretation and/or implementation, which is inefficient and ineffective;

---

[39] Homeland Security Presidential Directive (HSPD) 12 – *Policy for a Common Identification Standard for Federal Employees and Contractors* requires government-wide uniformity and interoperability to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card.

- In order for the international policy and technology environment related to biometrics to remain favorable to US security interests, the nation must speak with a single, powerful voice in relevant fora, and as a major US stakeholder, DoD's needs must be fairly represented in the US position.

The goal is an interoperable identity and collateral data exchange environment that embraces the entire US national security establishment. Key factors that affect realization of the goal include:

- Policy & Governance
- Technical standards
- Data-sharing
- Research & Development coordination

These key factors have been recognized by the Executive Office of the President, and early efforts are underway to organize and coordinate the interagency process for biometrics management along these lines.

Policy & Governance:

While it is axiomatic that the federal interagency process is managed by the Chief Executive, the process permits delegation of specific tasks to defined agencies or departments. At present, the Office of Science and Technology Policy (OSTP) leads the efforts of the Executive Office of the President in biometrics policy and governance, and manages the process via the National Science & Technology Committee (NSTC), Subcommittee on Biometrics.

Within this subcommittee a senior-level group is working to develop a USG-wide governance structure so that future agency biometric systems are seamlessly and appropriately interoperable, rather than agency systems being built individualistically and then requiring an interoperability appliqué. This requires continued interagency collaborations at the technical as well as at the policy level.

The OSD PSA for biometrics is an appropriately-senior official to represent DoD interests in this area at present. However, a preliminary analysis is underway to expand the scope of this area of interagency coordination, to embrace all of Identity Management, as it becomes more obvious that providing interoperable systems involves much more than collaboration on biometric-specific items. In such case, DoD may need to re-examine its representation.

The Task Force notes that this is yet another manifestation of what it sees as the need for OSD to move conceptually beyond biometrics to identity management.

It is clear that the OSD PSA for biometrics faces a formidable challenge vis-à-vis biometrics, alone. Notwithstanding that, we urge the Department to begin planning to address the larger identity management issue(s).

Recommendation 23.: The OSD PSA for biometrics should establish and maintain its position as the focal point for all DoD biometrics activities at the interagency level.

Recommendation 24.: The OSD PSA for biometrics should establish the policy and technology basis for associating biometrics with the broader field of Identity Management, in the whole range of DoD applications and requirements, and support interagency efforts to do the same.

Recommendation 25.: The Secretary of Defense should consider the establishment of a dedicated, senior-level position on the OSD staff. This official should have cognizance over all Identity Management activities across the Department, and should also represent the department's total interests in this area externally, coordinating appropriately with other US governmental departments and agencies, and international partners. The PSA for Biometrics would report to this office.

Recommendation 26.: Working with and through established interagency lead organizations and processes, the OSD PSA for biometrics should contribute to the development of strategic national objectives of the United States as regards biometrics and identity management, in support of international engagement on these topics.

Technical Standards

Historically, DoD scientists and engineers have been involved in both the national and international standards bodies in areas of interest to the Department. However, over the past decade or two, there has been a significant decline in this participation. There are at least two factors that have driven this change. First, DoD's role as the lead customer in many technology areas has declined as our acquisition system has focused on COTS products and the size of the commercial market has increased. Second, as the funding structure of the DoD laboratories has shifted toward shorter term projects and industrial funding models, the incentive to work in the long term standards process has decreased. While in many technical areas the need and potential value of working with the standards bodies to ensure DoD interests are identified and met is recognized, funding of these activities is required to ensure effective and continuous representation.

Biometrics, however, is a "good news" story as regards standards and collaboration. Good progress is being made within the US government to correlate and consolidate standards across the field of biometrics, and to some extent, Identity Management. The work is being conducted under the auspices of the National Science and Technology Council[40] (NSTC), and DoD has performed a valued, leading role in these efforts to date. Heretofore, these efforts have focused solely on coordinating USG positions in standards development activities. At present, efforts are in progress to expand that approach to monitor and drive the adoption of these standards in federal programs, with supporting conformity assessments.

---

[40] The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

Standards development and testing have largely followed, rather than led, program development. Standards need to be developed to create an environment conducive to efficient architectural design and system development, anticipating future capabilities to the extent possible. As always, rigorous, tested and interoperable standards are on the critical path for large-scale biometrics implementations, especially across organizations and jurisdictions.

Biometric standards-setting bodies exist at both national and international levels:

- At the national level, the INCITS/M1 committee has cognizance over all biometric standards, and along with the OASIS effort to incorporate web-based interfaces, is leaning toward the expansion in scope to embrace all of Identity Management, under the name of BIAS.

- Internationally, M1 represents the United States in the ISO SC37 committee, which focuses on biometrics standards. Two other ISO committees, SC17 (cards and ID tokens) and SC27 (IT security) are also engaged, and the three committees together are addressing IM standards issues more broadly.

There are other domestic and international standards bodies engaged in biometrics in which DoD does not have as strong a role:

- Terrorist Data Interchange Formats (TDIF) (Intelligence Community lead)
- International Civil Aviation Organization (ICAO) (DHS/DoS lead)
- Organization of Economic Cooperation and Development (OECD) (DoS lead)

Importantly, there is a DoD-internal standards body, the Biometrics Standards Working Group (BSWG), which actually predates organized interagency effort in biometrics. This group includes liaison representatives from OSTP, DHS and DoJ. It supports the domestic M1 committee and has proven a useful forum to focus technical attention on DoD-specific issues of biometrics standards and their implementation.

As standards work gains momentum, it will be increasingly important for DoD to remain fully engaged. We expect the various coordination groups to evolve in scope and topical focus, leading to a seamless and mutually-supporting grid, with cross-membership in important areas.

Recommendation 27.: The OSD PSA for biometrics should ensure that the DoD maintains strong support for, and participation within, domestic and appropriate international biometrics standards bodies. DoD technical centers of excellence and the PSA should ensure that organizational resources and individual incentives are provided. If other DoD entities are empowered to represent the department at any such fora, they should fall under PSA authority and guidance in all matters under consideration.

Recommendation 28.: The OSD PSA for biometrics should assume the Chair of the DoD Biometrics Standards Working Group (BSWG). The PSA should manage the work of that group to address and consider relevant areas of technical and policy concern, while continuing to maintain full visibility towards, and participation of, US government partner organizations.

Recommendation 29.: The OSD PSA for biometrics should ensure that DoD continues to co-chair (with NIST) the interagency standards and adoption coordination process through the NSTC subcommittee on biometrics.

Privilege Management

As we have discussed, the seminal federal activity to date in enabling wide-spread and interoperable identity management (IM) was the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in 2004[41]. This established requirements leading to the adoption of common procedures for registration, enrollment and credentialing of federal employees, and others. The technical standard for the credential, designed by NIST, is called FIPS-201. This standard has become the basis for an expanding range of IM programs across federal, state and local government, with an increasing number of private citizens enrolled in FIPS-201-based IM programs. The association of biometrics features within this standard, including on-token biometrics storage, and 1:N biometrics checking upon enrollment to ensure uniqueness before cards are issued, makes our attention to these related issues of IM and biometrics indivisible.

It also explains our treatment of the subject in this section. With the FIPS standard now being embraced for an increasingly-diverse set of applications, across an ever-broadening scope, it naturally demands cross-organizational management attention. The adoption of "privilege management," as the next major phase of wide IM implementation, will be a process which must be front-loaded with enabling policy(ies). These will be required to establish the scope of participation, define certain technical standards, arbitrate the "ownership" of such processes within the government, and broker the government-civil interface, to the extent such processes extend in those directions.

It is important to understand that however impressive, indeed indispensable, the HSPD-12 initiative has been in the process of biometrics and identity management, it is not, in and of itself, a complete policy or standards basis to support federal needs in biometrics or IM. When fully implemented HSPD-12 will provide a point of departure for pursuing efficiencies, economies and enhanced functionality in many ID-sensitive applications. Earlier in this report we discussed in some detail the relationships between root identification (for which HSPD-12 accounts) and other key aspects of mature and successful Identity Management systems. The policy basis for that total enterprise, beyond the root ID and associated credentialing, remains a need. This applications-focused piece of the total Identity Management system can be described grossly as the "Privilege Management" process.

> A biometrically fixed, relatively universal, root-ID would permit the "root authority" to offer ID services to any application that would manage privileges, allowing that application to enforce the association of the privilege with the assured identity-granting or denying the privilege to that identified individual.

---

[41] Biometrics matters related to that policy were subsequently published as Special Publication (SP) 800-76.

Biometrics can provide the non-repudiable basis for this process which could never be achieved using only tokens and/or PINs/passwords. By creating a common format and interoperable root-ID environment (as mandated by HSPD-12), it becomes possible to extend and manage such activities across organizational boundaries, as the various privilege-holding authorities all have recourse to a common and trusted basic ID. The term for such cross-organizational functionality is "privilege management".

Recommendation 30.: The OSD PSA for biometrics should support and participate in interagency efforts to develop a cross-government policy framework for the implementation of a Privilege Management architecture, within, across, and building upon the scope of National Implementation Plans and the HSPD-12-directed Identity universe.

Data Sharing

Sound identity management, supporting privilege management, is the key to sharing sensitive data at acceptable risk. The collateral data associated with a firmly fixed identity, biographic data, assigned roles[42] and official personae, informs sensible decisions as to suitability and need-to-know.

Of course, the information system must have adequate protection measures designed, implemented and maintained, but the strongest system would fail were it not able to avail itself of the strongest identity management services.

Now and in the past, formalized identification systems have involved various tokens and credentials, PINs and passwords, issued and recognized by individual sponsoring organizations. Within their respective administrative fiefdoms, various identity-based "privileges" were granted and managed. This approach is dated and falls far short of what the Department requires to support both its joint, allied and coalition operations globally, and its enterprise-wide business processes.

In all such cases, the pre-existence of a common/standard, HSPD-12-based root ID and credential universe is foundational and permits development of complementary policy and architectural structures for Privilege Management (PM). Such a structure would permit enrolled/credentialed persons across an organizationally-horizontal workflow (e.g. at an international transportation portal) to interact as if they had been sponsored and empowered (i.e. "provisioned" with role-based authorities and access privileges) by a single authority. As such, the military joint C3 processes are a natural beneficiary of this kind of capability, if it were to be created. The point is made even more strongly in recognition of the increasing tendency of US military missions and authorities to interact with increasingly-diverse organizational players, at home and abroad.

---

[42] Note that an acknowledged role is really shorthand for a pre-determined basket of privileges.

Sharing Identity-Related Information

DoD has any number of relationships for the sharing of identity-related data. Many are bilateral, many are *ad hoc*. There is currently no complete or consistent catalog of these relationships, or the authorities under which they operate. A substantial information-gathering and analysis effort is in order.

Recommendation 31.: Under PSA auspices, a comprehensive registry should be developed and maintained cataloging any and all arrangements for sharing identity-related data. The PSA should clarify authorities for entering into such relationships.

Recommendation 32.: The OSD PSA for biometrics should work within the interagency environment to support the identification of relevant data repositories and organizations across government, which will collectively comprise an integrated data environment (architecture) for biometrics use and storage.

Sharing identity-related information exists at the conjunction of policy and technology. So, to provide maximum operational flexibility to respond to any contingency within the DoD mission space, technical architectures should be as organizationally indifferent, topically comprehensive, and operationally adaptive as possible; and policies should facilitate sharing within and across organizations in response to any need. Here, the PSA for biometrics, working in concert with other DoD authorities, has much to do.

By the nature of the defense mission, it has long been necessary to share information between and among government agencies, selected international partners, and non-governmental organizations and contractors. However, these arrangements have often been conducted at the level of personal coordination and/or paper-based exchange while the nature of biometrics data sharing argues for an interoperable IT architecture.

There are already US government mandates for large-scale sharing of the basic biometric data itself. One such example is the National Strategy for Maritime Security, laid out in HSPD-13/NSPD-41, which requires extensive data sharing between the DoD and DHS, as well as other federal and state/local authorities. The policy also mandates information exchange with international partners and allies. Implementation must provide for use of biometrics information, whether associated with government personnel seeking to verify accesses and privileges; known or suspected bad actors; or screening info collected from unknown persons. The CJIS is almost certain to be involved, broadening the scope and complexity of the information-sharing architecture.

Moreover, the need for the individual departments and agencies to provide for continuity of operations opens the way for disaster recovery planning (data and processing backup) that will encompass the total data environment, across the Departments of Defense, Justice and Homeland Security.

Recommendation 33.: The OSD PSA for biometrics should work with other authorities across the federal government, towards a goal of creating a disaster-recovery and backup-site

architecture that encompasses the total biometrics data enterprise upon which the performance of DoD missions is dependent.

Another motivation for cross-departmental data sharing is section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), which mandates the "Information Sharing Environment" [43], that combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information), of federal, state, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively. The IRTPA requires the President to designate an individual to serve as the Program Manager (PM) responsible for information sharing across the federal government. In June 2005, the President directed that the PM be part of the Office of the Director of National Intelligence (ODNI). Although reporting to the DNI, the PM's mandate covers access to terrorism information across federal, state, local and tribal governments and the private sector.

Reportedly, the PM is actively seeking candidate projects to demonstrate and advance cross-organizational architecture and data sharing, and this is an opportunity the Department should not miss. Since the ISE is the long-term approach for enabling and managing the interagency exchange of terrorist information, terrorist-related biometrics data are part and parcel of the ISE.

Recommendation 34.: The OSD PSA for biometrics should propose a DoD-sponsored, cross-organizational biometrics pilot program to the Program Manager for the Information Sharing Environment (ISE) for inclusion in the ISE implementation road map. The importance of organizational roles and responsibilities defined in the National Strategy for Maritime Security suggests a DoD/DHS sharing effort, focused on functions required by HSPD-13/NSPD-41.

---

[43] See www.ise.gov for details of organization and charter.

Manpower and Training Requirements

There do not seem to be any highly unusual or demanding training requirements in the operation of identity management systems and the field applications of biometrics. Of course, any system development/acquisition should consider training requirements and developments should, as always, seek to minimize the requirements for training (and maintenance, too). This is not to say that training, today, is adequate. It is not. Notwithstanding the fact that training needs may not be extraordinary, there is an evident shortage of skilled personnel.

At the level of equipment familiarity and operational proficiency, deficiency in training is cited as a leading cause of unsatisfactory biometrics sample collection in operational environments at present. This situation underlines the current shortage of military training facilities keyed to producing skilled military and civilian personnel of the types, and in the numbers, required to meet operational needs.

While there is some early progress in defining the biometrics mission at the highest levels[44], much more needs to be done in areas of operational concepts, doctrine and planning, across the entire defense establishment. Currently-fielded operational systems do not employ common tactics, techniques and procedures (TTP), either individually or as a system of systems. This deficiency is made even more stark in a coalition-force environment.

Recommendation 35.: Establish a focused identity management and biometrics doctrine effort at the Joint Forces Command, to identify and manage operational needs of the combatant commanders in this area. This organization must also develop TTP for biometric use in coalition/international force operations, where additionally, complex issues of data sharing and differing national perceptions of, and rules regarding, "privacy," etc apply.

Recommendation 36.: The OSD PSA should work with USD/P&R to establish an "Identity Management Community" within the DoD to establish, support and manage a career-long continuum of training, education and professional development in this field.

Recommendation 37.: Create a program of formalized biometrics training, addressing the need at multiple levels:
- Senior awareness and orientation to expose uniformed and civilian seniors to the high-level issues, implications and applications of ID Management;
- S&T education to keep up with, and even advance, the state of scientific development of biometrics within the DoD;
- Theater/Operational level, for uniformed managers and specialists;
- Equipment-level operations.

---

[44] Capstone Concept of Operations for DoD biometrics in support of Identity Superiority, draft dated 8 July 2006.

If the Department applies itself, it can design and deliver training to operational personnel. This would not, by itself, remedy the shortage of skilled professionals necessary for design, development and management of such systems.

Today, there is a very narrow community of institutions of higher learning that offer relevant technical education in biometrics science and application at the Bachelor's and Master's Degree levels, and very few of their graduates find their way into the Defense Department. If we hope to meet the projected need for skilled staff, we must encourage the emergence of a broader and deeper choice of available and relevant undergraduate and graduate-level education in biometrics and identity management.

Recommendation 38.: The OSD PSA for biometrics, in coordination with and supported by the USD/P&R, should examine the model used to support and encourage the emergence of Information Assurance (IA) as a recognized and accredited academic discipline in the 1990's, in terms of its possible relevance for reproduction and application to IM/biometrics. In the IA case, the National Security Agency provided technical advice and oversight; sponsored conferences, papers and some basic research; established standards for accreditation; and awarded recognition and other resources to qualifying institutions. This strategy is perceived to have been instrumental in accelerating the definition and emergence of IA as a specific professional field, just in time to support the Department's, and the nation's, rapidly-expanding needs. We believe the current circumstances related to biometrics, and especially to identity management, demonstrate many similarities.

Securing Identities

We have described such concepts as "root identity," the various steps in enrollment and credentialing, and "privilege management," all as applied to biometrics. We turn now to a discussion of the social issues, primarily behavioral and attitudinal, that underlie IM and especially biometrics. We have suggested throughout that there is more to be done, beyond this report, to achieve a deep and broad understanding of IM in DoD, now and in the future. That is nowhere more true than in the area of understanding and responding to the "soft science" issues surrounding biometrics and their use.

In our discussion of "security," we operate from the premise that there is (will be) a single, biometrically-verified and recorded "identity." This must be strongly protected, although it can, and should, be segregated by strong protections from any application-specific context, or privilege. In so doing, we hope to support goals of privacy and security, in policy, procedure and architecture/technology.

The goals of "security" of this identity then must protect both the individual, and the organization(s) within which he/she operates. Confident, unique identifiability serves both of these purposes. Thus, we seek to ensure that:

- No person can be enrolled with a root identity more than once; and conversely;

- No person can adopt the root identity of a previous enrollee.

This compact, the institution undertakes to protect a person's unique identity through technology and process and that person is thereby prevented from manipulating their identity for malicious purposes, is at the core of our concept of IM and biometrics in support of national security needs.

Given the degree to which this part of the discussion is conducted as much in the "gut" as in the head of the average person, here again we cite the essential role of education, technical effort to support rigorous conclusions and wise program development. Effective security safeguards for storage and use of biometrics information are simply indispensable, and security breaches in this area will prove much more than embarrassing. Due to the enormous importance that the Task Force attaches to biometrics generally, the future in this area is simply too important to risk negative social (or legislative!) reaction to avoidable errors.

Finally, we suggest that the modern history of biometrics and IM in America has been dominated by programs which "worked," in a technological sense, but which were deemed unacceptable in the "court of public opinion." We must learn from these experiences, and pay close attention to these "social science" aspects of the total biometrics topic, as we seek to design, develop, field and operate biometrics programs that "work" in every respect, here and in forward operating areas.

Privacy

Large scale identity systems can raise serious privacy concerns, if not singly, then jointly and severally. Throughout most of our discussion, we acted as if there was a unitary, single-purpose identity system, which paired uniquely an individual and some select information. In the "real world," however, there are multiple systems that contain various pieces of information and, frequently, some variable or variables that permit cross-referencing an identity across the several systems. Heretofore, an identity in a system would commonly include a Social Security number that enables cross referencing and the association of more information with the identity than any of the individual systems intended.

Observation: This ability to cross reference and draw new, previously unimagined, inferences is, at once, the strong selling point for identity management and the bane of privacy advocates. The privacy challenge is real, even when any or all of the individual systems have been designed and are operating securely and in a manner consistent with applicable law and sensitive to privacy and other considerations.

In many applications the linking of identities with collateral information need not be exact, *i.e.*, one-to-one, because the application only requires population statistics. Strong measures can (and should) be taken to veil the individual data in these cases. In other cases, the individual's data are the point, and for these policy and administrative measures, augmented by technology, to minimize exposing such data.

Ultimately, the Department of Defense must find ways to respond better to the public's expectations of privacy, shaping those expectations to a prudent extent, and responding better to negative media exposure, which is not only embarrassing but can set back important policies, technologies and systems.

To offset privacy concerns related to the establishment of a consolidated biometrics data universe, the department should emphasize the opportunity for improved security and audit controls in a centralized architecture; and the ability to create search architectures that focus on query/response within defined scope, rather than necessarily searching "all data all the time." The good news here is that this policy approach will support enhanced system technical performance and improve scalability, relative to current methods. An interesting framework[45] for understanding the concerns of the "privacy community" is presented in Figure 12.

---

[45] http://www.bioprivacy.org/bioprivacy_main.htm
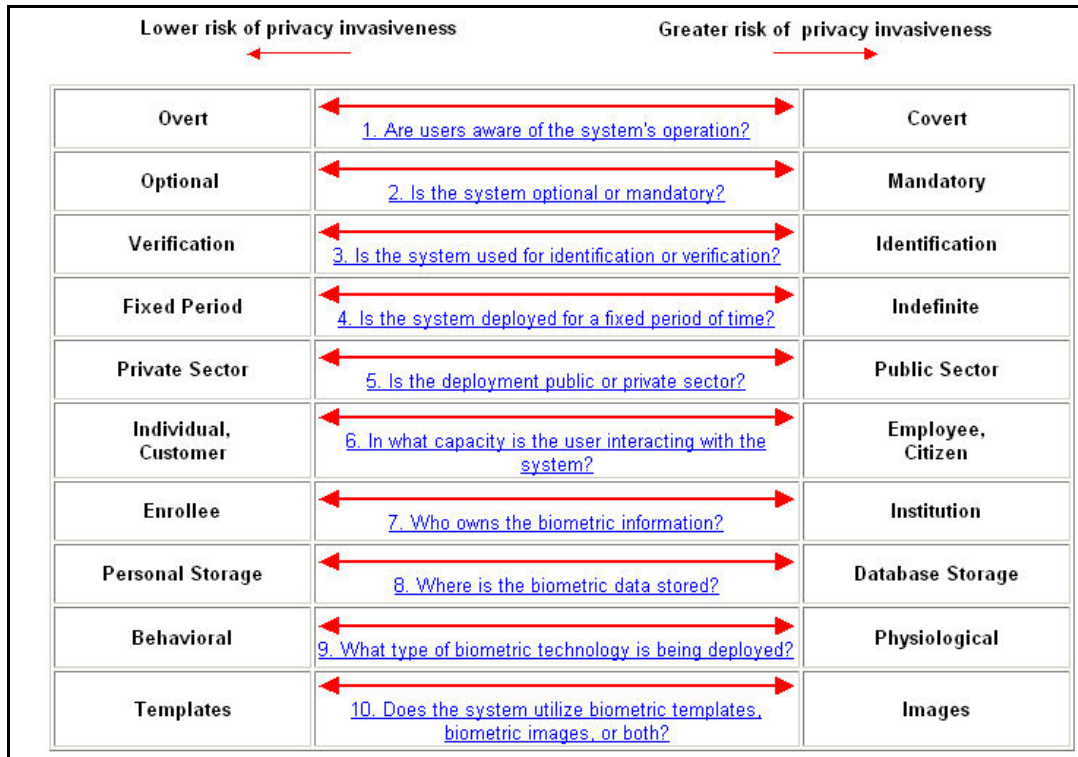
Figure 12: Privacy Considerations

Sadly, but not unexpectedly, for most DoD applications of biometrics in support of identity management, the more desirable characteristics are all "to the right," *i.e.*, involve a greater risk of privacy invasiveness, according to this characterization. Those who, as recommended above, will represent the DoD's biometric/identity management efforts should pay close attention to the framework.

Integration of privacy principles into biometric system design, development, and operations is critical to system success but absent comprehensive, authoritative and published DoD-wide positions in this area there will be local interpretation of law, policy and implementation, with some disruptive effect. The Department of Homeland Security has taken the lead in this area, creating a primer to help an implementing department or agency approach the complex privacy implications of biometrics use[46]. There is a clear need for the establishment of uniform constructs in complex areas of unsettled law and policy related to biometrics, and privacy is a good place to start. Work in this area should be coordinated with ongoing interagency efforts (currently led by the DHS Privacy Office, as chartered by the EOP).

Recommendation 39.: The designated PSA for biometrics (and, ultimately, for identity management) should ensure that privacy considerations are brought to the fore early in the requirements and design phase of any system; and the scope of the considerations must extend beyond the individual system to include other systems with which a user might interact. Policies

---

[46] Privacy & Biometrics: Building a Conceptual Foundation, dated 14 April 2006

and procedures, ideally implemented in technology, may be required to enforce undesirable commingling of sensitive data.

Recommendation 40.:   The Department of Defense, if not the USG, must seek to engage responsible advocates of privacy early in the design and application of identity management systems; the serious purpose of the system must be communicated and understood; and, the data must be limited to that purpose.

Recommendation 41.:   The OSD PSA for biometrics should request a broad review by the Office of General Counsel (OGC) of the privacy implications of biometrics use within the Department, which should be coordinated with the Department of Justice. Based on the results the PSA, in coordination with the Defense Privacy Board and the OGC, should create comprehensive biometrics privacy policies and strategies as required to support the range of defense missions, consonant with interagency efforts.

Identity Theft and Biometrics

Identity theft has been popularized by the media, of late. Biometrics are designed to reduce its frequency but biometrics are but a part of a larger identity management system, which can be suborned in a number of ways, all of which must be defended against. While DoD's circumstances differ in some specifics from the popularized examples, it is important to understand the techniques and their impact, economic in the popularized cases, but threatening mission success in the DoD context. The Department benefits from all measures undertaken to curb these abuses.

Identity theft encompasses a myriad of criminal activities including "true name" fraud, account takeover, and fraudulent applications fraud. What these and other approaches have in common is that they succeed (readily) by attacking the "identity infrastructure" via its soft underbelly, the various "pseudo-identity" mechanisms that proliferate today. As we have discussed, these may be either issued by government (e.g. birth certificate), or actually represent some sponsor's token providing access to a privilege under their control (this is the model in most commercial "ID applications" at present, including credit cards).

Simply stated, almost all "ID applications" today represent "privileges," as we have discussed the term, most of which do not have recourse or reference to a strong root ID. To that extent, they represent houses built on sand, and are open to the kinds of attacks described here. We have spoken previously of the role of biometrics in establishing strong root ID, thereby mitigating many current deficiencies, as detailed below. As such, we see biometrics as being the technology and process "force" which will *eventually* turn around identity theft, but not immediately, and not at the Defense Department's instigation. We have included this discussion here, including the basic characteristics of identity theft as at present, due to its obvious relevance to biometrics generally, and because of DoD's role in coordinating all biometrics RDT&E across the federal government.

Definitions of Identity Theft

"True name" identity theft involves acquiring a person's identity to establish new financial accounts or loans, obtain employment, create fraudulent identification, or to commit other crimes. Account takeover identity theft refers to the acquisition of a person's existing credit card or bank account or an existing non-credit card account. The account takeover can consist of utilizing an existing account with the intent to obtain money, goods, services, or any other thing of value that can be used to initiate a transfer of funds. Fraudulent application fraud occurs when a criminal uses an identity other then his/her own to apply for credit or services. These three broad categories of identity theft encompass a range of criminal activities, from simple fraud to complex global schemes.

The term identity theft conjures many different definitions within the federal and state government, the law enforcement community, the private sector, and financial community. Prior to the Identity Theft Assumption and Deterrence Act, which was passed by Congress in 1998, legislation did not treat identity theft as a federal crime, and federal and state statutes did not distinguish between identity theft and other types of fraud. The act defined identity theft as the knowing transfer or use, without lawful authority, of any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[47] Interpretation of the legislation has found this definition of identity theft to be consistent with true name identity theft, account takeover, and credit card fraud.

With the 2004 passage of the Identity Theft Penalty Enhancement Act, Congress redefined identity theft, expanded the range of criminal sanctions, and established the crime of aggravated identity theft. The new definition of identity theft replaced the phrase "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual" with the phrase "a means of identification of another person." The purpose of this change was to define the term so that it would encompass all victims. Congress interpreted the phrase "means of identification" to include the name, social security number (SSN), date of birth, address, and telephone number of a specific person; biometric data, such as fingerprints, voice prints, and retina or iris images; and access devices, account numbers, personal identification numbers, and other means of account access. According to this interpretation of the definition, true name fraud and account takeover are forms of identity theft.

The definition of identity theft varies according to the mission and the customers of affected agencies and businesses. The FBI and the FTC broadly interpret the identity theft statutes to include any financial or non-financial account takeover and true name fraud as identified in 18 U.S.C. 1029 (e)(1). The FTC Identity Theft Clearinghouse collects consumer identity theft information on true name, account takeovers, and credit card fraud. The American Banking Association (ABA) defines identity theft as financial account takeovers and true name fraud for deposit accounts only. Major credit card companies such as MasterCard and Visa categorize

---

[47] 18 U.S.C. 1029(e)(1)

identity theft as account takeovers and fraudulent applications but *exclude* most other forms of credit card fraud (use of lost, stolen, or never-received cards; counterfeit cards; and mail order/telephone order fraud) from the definition. The most significant difference in these definitions is the *means* by which an account takeover is defined. MasterCard and Visa do not consider the fraudulent use of a credit card as account takeover because the perpetrator of the fraud has not fully assumed the identity of the victim. However, the FTC and the FBI consider credit card numbers to be a means of identification, and any use of the account numbers constitutes identity theft-related account takeover.

Impact of Identity Theft

In the commercial sector, there is increasing concern with identity theft, and with good reason. It is all too prevalent, usually associated with thievery. While the inconvenience can be intense and personal, much of the economic consequence, as with all theft, is borne by society at large, through insurance premiums and other business costs which are passed on to all consumers. Of course, things are different for the Department of Defense, indeed, for the USG. More important than the immediate economic consequences, identity theft can threaten mission success. The threats which the DoD faces are different from those faced by general commerce and we emphasize, below, the importance of a formal threat model.

Identity theft is especially important in the case of centralized databases or systems used for multiple purposes. Not surprisingly, the more useful or "powerful" an ID is, the more tempting a target it becomes.

As others have pointed out: "one reason for the problem is the expanded use of SSNs for purposes that were not originally intended coupled with the assumption that they are 'secret' or should act as a 'key.'" Not so long ago, before identity theft became "computerized," SSNs were used promiscuously as a unique identifier, to resolve name conflicts. In fact, police departments concerned with material theft made engravers available to the public and encouraged them to label their valuables with their SSN.

A problem with use of SSNs in combination with publicly available personal information (e.g., mother's maiden name) as an identifier, or "key," to gain access to an individual's credit records and other authoritative credentials is their lack of secrecy, given the ease with which they can be shared, sold, and compromised. As use of computers has matured, keys or passwords are kept secret to prevent access to the system by an unauthorized user. While keeping information secret may be a common practice for online and other remote applications, it must also underpin the process of establishing credentials in the physical world. Otherwise, fake identities can be created by using SSNs and other personal information that is (mistakenly) presumed secret or private to acquire so-called "breeder" documents (*e.g.,* driver's licenses) that can be used to gain access to an individual's personal or financial information. Such "breeder" documents should be bolstered by biometric indices.

The "How To" of Identity Theft

Identity thieves use many techniques to target victims and obtain sensitive personal information. These methods range from conventional tactics, such as identity theft facilitated through a

personal relationship with the victim, to advanced schemes using technology and the Internet. The furtive methods employed by perpetrators of identity theft often allow criminals to remain anonymous and prevent consumers from detecting the theft before significant damage is inflicted.

Surrendered Identities

Identity thieves target vulnerable and destitute persons willing to surrender their identities in exchange for nominal sums of money, homeless and unemployed persons tend to be the most complicit victims because they seldom report fraudulent use of their identities to law enforcement authorities. Financial institutions inadvertently sustain a loss that they do not acknowledge as identity fraud. Consequently, identity thieves may be able to perpetrate fraud over an extended period of time with a decreased risk of detection. In contrast, drug addicts and low-income individuals who engage in surrendered identity fraud are more likely to report the theft to avoid financial obligations for fraudulent charges to accounts created or taken over in their names.

Creating Identities

Criminals may create identities or assume the identities of deceased persons in furtherance of fraudulent schemes. The false identities facilitate the production of counterfeit identification documents, which may be sold to illegal immigrants seeking access to employment, housing, health, and financial services. The targeting of victims for identity creation is frequently an arbitrary process that depends upon which documents the identity thief can obtain. Criminals may access sensitive personal data through compromised open source records or through publications such as the Social Security Administration's death index, which contains the Social Security Numbers of deceased Americans. As with surrendered identity theft, the creation of new identities using personal data of deceased individuals greatly diminishes a criminal's risk of detection and extends the length of time over which the fraud may be perpetrated.

Stolen Identities

The most common method through which criminals obtain identities is theft, and criminals use a variety of creative approaches to target victims. The most popular methods to steal identities are through the exploitation of personal relationships and insider access; pilfering of personal information via dumpster diving or stealing mail; the abuse of computer technologies; and the perpetrator's misrepresentation of his purpose in seeking access to confidential documentation.

Insider Access

Approximately 50 percent of identity theft victims claim to know the identity of the perpetrator, who is usually a relative, neighbor, or acquaintance of the victim. Although conducted on a less visible scale than high-profile mass thefts of consumer information, the prevalence of identity theft committed through a personal relationship can prove especially detrimental to victims. Criminals often have access to bank account and credit card information, property deeds, and identifying documentation.

Employees with access to confidential customer records may pilfer SSNs, addresses, account numbers, and other identifying information for use by accomplices or for sale to criminal organizations. Employees of banks and financial institutions have unique access to a wealth of information such as income, credit score, account balances, and available credit that may be used to select favorable targets for victimization.

Public Records

Many identity theft victims are seemingly targeted at random. Criminals exploit public data, such as state and local records, property ownership records, marriage certificates, and the Social Security administration's death indices for personal identifying information. SSNs are prohibited from display in federal agency records, but that does not apply to federal court records.

Individuals and criminal organizations also exploit data aggregators by opening fraudulent accounts, say by posing as legitimate debt collection companies, for the purpose of obtaining personal information to conduct fraudulent activity. Data aggregators compile in-depth personal information on individuals from many sources to include court records; property tax assessor files; professional license applications; vehicle registration forms; bankruptcy filings; and credit reporting agencies. The unauthorized use of this information can be used to change mailing addresses; redirect telephone numbers; access financial institution records; open checking accounts, credit cards, or lines of credit; and transfer property or assets.

Dumpster diving or rummaging through trash is the most readily available avenue to obtain personal information. A wealth of personal information can be discovered in the garbage. The collectors of the information target documents discarded by hospitals, financial institutions, hotels, medical offices, accounting firms, law firms, mortgage brokers, and other organizations that have carelessly discarded personal information. While businesses formulate security procedures, they are only effective if they are enforced by all employees with access to personal information. If a customer service representative writes a customer's SSN on a piece of paper and discards it in the trash, the information is vulnerable to identity thieves.

Mailbox theft is another common method to obtain personal information. Mailboxes yield valuable information from bank account statements and credit card bills to credit card marketing offers. In apartment buildings, the mailboxes are typically located in one central area. This is an excellent target for collectors of information. The criminal can access multiple mailboxes within minutes. In single family communities, mailboxes located at the end of the driveway are easily accessible for an identity thief to steal incoming or outgoing mail. It is common for the resident to drop outgoing mail in their mailbox and put the flag up signifying that mail is in the mailbox. Although this flag signals a mail pickup to the mail carrier, it is a "red flag" for an identity thief to steal the mail. Typically, the outgoing mail will contain checks for payment to credit card and utility companies. Bill payments may contain an account number, the name, address, telephone number of the person, and the checking account number. Identity thieves have enough information to constitute an account takeover.

Internet-Related Theft

New technologies and the Internet provide identity thieves with innovative tools for acquiring large amounts of personal identifying data with minimal effort. For example, identity thieves use credit card skimming devices known as Magstripe Readers to collect encoded data from magnetic strips on credit cards. Magstripe Readers, as well as credit card processors, are readily available for purchase on the Internet and can be used to create counterfeit credit cards.

Identity thieves use spyware technology, which tracks a user's Internet activity without the individual's knowledge or consent, to obtain sensitive personal information. The software can record a user's keystrokes and send the captured information, which may include passwords and account numbers, to remote locations or users for criminal exploitation. Another form of Spyware is robot networks or "botnets," which is a group of computers compromised by malicious code and centrally controlled by the hackers. Often, the malicious code contains a keystroke logger that records all personal and account information typed on that computer.

In recent months, several computer intrusions have occurred at institutions of higher education nationwide. Colleges and universities maintain a vast amount of personal identifying information on past and current enrollees, including SSNs, dates of birth, addresses, telephone numbers, parental information, bank account numbers, loan disbursements, and pictures. The exposure of this data is extremely damaging as identity thieves can exploit the personal information by applying for new student loans and altering current student loans' disbursement dates, remittance addresses, receivers' addresses, and direct deposit accounts.

Criminals target customers of financial institutions, Internet service providers (ISPs), online auctions, and other businesses via "phishing" scams, in which victims receive fraudulent e-mail directing them to websites "spoofing" legitimate businesses and government agencies. The phishing scams deceive Internet users into disclosing personal identifying and account information. The text of the e-mail instructs victims to immediately respond with their account information for 'verification purposes,' or their account will be disabled. The e-mail frequently directs victims to open a hyperlink that appears to be the legitimate Web site of the business or government agency. Criminals who engage in phishing often employ spamming techniques to send the fraudulent e-mail to thousands (or millions) of potential victims nearly simultaneously. Thus, phishing can be a lucrative criminal mechanism even if only a small percentage of the recipients are deceived into disclosing their personal financial and/or other sensitive information.

In a new variation on phishing known as "pharming," identity thieves redirect users' web requests to a bogus Web site, even though the users have entered the correct domain address. Users unwittingly believe they are connected to a legitimate Web site and feel secure in sharing their personal information. The perpetrators of this scheme conduct the fraud by planting malicious software into users' computers via e-mail attachments or by poisoning the server that directs traffic on the Internet.

Job Postings

Identity thieves also use employment advertisements to deceive individuals into relinquishing personal information. In this scheme, the perpetrator posts a job advertisement online or contacts

the victim through a spam e-mail. The victim responds to the job posting through an online job application. This application requests sensitive information including date of birth, SSN, employment history, and contact information. In some instances, the victim's identity is immediately exploited; in others, the victim may actually become an employee of the subject, often agreeing to receive and resend money or products to the subject before their identity is compromised.

Fraudulent Documents

The use of stolen identities to create fraudulent identification documentation represents a significant national security threat. Document fraud encompasses the counterfeiting, sale, or use of false documents, such as birth certificates, passports, or visas to evade the US immigration laws. Fraudulent identification documents allow criminals and terrorists to assume new identities to evade detection and surveillance, obtain legitimate employment, to enter the United States, and gain access to secure facilities and confidential information. With false identification, perpetrators can easily open bank and credit accounts to steal money and finance further illicit operations.

> In September 1992, one of the conspirators in the World Trade Center bombing entered the United States with a fraudulent Swedish passport in which the photograph was substituted. The suspect did not expect to be challenged during the INS inspection, but an INS inspector suspected that the passport had been altered. A search of the luggage revealed instructional materials for making bombs. In March 1994, the subject was convicted for his role in the World Trade Center bombing. This terrorist was in possession of numerous false identification documents, such as photographs, bank documents, medical histories, and educational records that could have been used to create numerous false identities.

Criminals use many methods to obtain or create fraudulent identification documents. High-quality fraudulent identification documents, such as social security cards and birth certificates, can be used to acquire subsequent identification documents, such as passports and driver's licenses. Blank documents stolen from legitimate sources, such as the DMV, may be impossible for law enforcement officials to detect as counterfeit. Technological advances and sophisticated computer graphics programs enable criminals to create high-quality fraudulent driver's licenses and passports complete with holograms and other security features. Many fraudulent documents appear so realistic that they escape the detection of highly-trained individuals. Fraudulent documents present a significant national security threat to the United States and preclude law enforcement from verifying an individual's true identity.

(The difficulty in) Establishing an Identity

The status quo as regards the establishment of an identity in an identity-system is another challenging but critical part of the process.[48]   There is a tangled web of government-issued identity documents used as foundational documents that allow the government and other organizations to issue other identity documents.   Many of these foundational documents, used to acquire an SSN or Passport, for example, are subject to fraud and forgery themselves.   Birth certificates are particularly problematic, in that they are issued by thousands of different jurisdictions across the country, making them both easy to forge and difficult to verify and thus very poor to use as an identification document from a security perspective.   Moreover, no aspect of a birth certificate binds it to an individual in any strong security sense." The types of possible attacks on identity documents vary and include the following:

- An individual acting as an imposter;
- Forged or fraudulent documents;
- Tampering with existing documents;
- Compromise of confidential information (for example, in an identity system database) that is then used to create a false identity;
- Modification of computerized records to support a false identity.

The debate continues regarding the efficacy and acceptability of moving to, say, digital credentials or biometrics for these purposes. As we have noted, this is a debate which the DoD will observe, and should be attuned to, but which will necessarily be resolved at higher levels. As technology and perhaps ID cards become ever more sophisticated, the issuing process will remain extremely important. All the security in the world cannot overcome deficiencies in this step, the system will only be as good as the data that goes into it.   The best that any system can provide is a compelling connection with some *previous* verification of identity.   Essentially, trust in the integrity of the system is based not so much on any single verification when an individual presents a claim of identity as it is on increasing confidence when multiple transactions happen over time and all previous transactions with that particular individual have worked out.

The bottom line in this part of our discussion must be that while biometrics can seal a given human being to a set of biometric indicators, nothing can underwrite the claims made by the enrollee or anybody else regarding the "TRUE identity" underlying the enrollment. A person may perhaps succeed in enrolling with a false biographic story – once. What we must hope they can never do is to discard that "root ID" in favor of any other at a whim, and fail to be detected in so doing. In fact, current procedures associated with HSPD-12 seek to mitigate just that threat, by requiring background investigation before permitting biometric enrollment for root ID.

---

[48] See, *inter alia*, *IDs—Not That Easy: Questions About Nationwide Identity Systems*, Statement of Stephen T. Kent Vice President and Chief Scientist, Information Security BBN Technologies and Chairman Committee on Authentication Technologies and Their Privacy Implications National Research Council The National Academies before the Subcommittee on Social Security Committee on Ways and Means U.S. House of Representatives March 16, 2006

Biometrics Are Forever—the Down Side

There was one area in which the Task Force did not find itself of one mind: the question of using biometrics for authentication across a wide, general purpose, network like the Internet. In 2002, The National Academies National Research Council's *Committee on Authentication Technologies and Their Privacy Implications* concluded that it was not appropriate to remotely authenticate over such networks using biometrics. Their logic was:

- Remote authentication across, say, the Internet, for myriad uses, means that the "libraries" of reference biometrics would be stored at many places on the net and, eventually, some library could be compromised, no matter how strong the safeguards.

- This is, of course, the case with passwords, PINs, *etc*., and instances of compromise are legion. In the case of passwords, PINs, *etc*., however, a new identifier/authenticator can be issued. Think, for the moment, about the impracticality of issuing a new fingerprint.

- Their recommendation was that the biometric identifiers be stored locally, even, say, on a card/token normally in the individual's physical possession and it, in turn, could be used to unlock an otherwise secret key or crypto variable which would support the remote authentication. A new key variable could, if necessary, be issued.

- Why, they argue use the biometric, itself, as the remote authentication variable? According to their calculus, the reward was nil and the risk real.

The Task Force was divided on whether this recommendation was (still) valid. Some felt it had been made in an earlier time and that the information assurance technology/understanding on which the recommendation was based was dated.

A somewhat different formulation would stipulate that biometrics are forever, but their association with either an identity or with a privilege is not forever.[49] Biometrics should never be used by themselves; when used as a reference, they need to be digitally signed, and their association with a privilege or identity must be revocable.

When used for remote authentication, according to this formulation, there are three requirements:
1. The reference biometric (biometric at rest) must be digitally signed to detect tampering, and the association of the biometric with either identity or privilege must maintain a mechanism for revocation. A biometric used for privilege should be traceable to the biometrics used for establishment of identity, and must also be revocable.

---

[49] This distinction is captured, as we frame the case here, in the admonition to call out "Privilege Management" as an embedded aspect of "Identity Management."

2. The proffered biometric (for authentication) must be protected from tampering or detection during the transit (biometric in motion). This should combine encryption and digital signature.

3. The collection mechanism for the biometric must be trusted and revocable. In local operations, the collection is observed by a security person (example, 10-print collection), and the equipment is trusted because it is under local control. Revocation of the equipment is just replacement. In remote operations, there must be a remote trusted biometric reader, associated with the biometric to be read, and the trust of the biometric reader must be revocable in case of tampering (self revocation), or in case of loss.

Finally, there is much to be gained by a properly constructed authentication with a biometric, in conjunction with PIN and keys. This is "three factor authentication": something a person has (private key on token), something they know (PIN or other private key releaser), and something they are (biometric taken by a trusted, revocable reader).

In such a system, there are three revocation mechanisms:

1. Revocation of the certificate represented by private key, denoting loss of the key/token.
2. Changing of the PIN, effectively revoking the access of the old PIN.
3. Revocation of the link between a specific reference biometric and a specific private key.

Even though one cannot revoke a biometric, one can revoke the relationship between a specific biometric, and a specific instance of privilege or identity. The effectiveness of the revoked biometric can be re-established by re-linking it to a new instance of the specific identity or privilege.

Recommendation 42.: That the PSA for biometrics cause this issue of using the biometric, itself, for remote authentication across a broad multi-use network to be re-examined. Participants in the re-evaluation would include, inter alia, the CIO(s), the ASD/NII, and the DIRNSA.

Making a (Black) Market in Identities

After sensitive personal data has been obtained, an array of Internet sites are available to facilitate the criminal operations of identity thieves. Internet chat rooms provide another avenue for criminals to collect sensitive personal information or recruit unwitting participants for identity theft purposes. Chat rooms provide a more personal method of communication than mass e-mail or web postings. Identity thieves use chat room interactions to recruit employees with access to sensitive insider information to participate in their schemes. The current nature and, as discussed here, the limitations of identification technology and associated tokens have given rise to some level of organized commerce in the process. There are web sites that openly market themselves as "fake ID" resources. All efforts of the Department, the federal government and our allies, indeed all law abiding nations, must proceed with a clear understanding that there are strong, sophisticated, well organized opposition forces engaged.

The Internet also provides a convenient venue for global criminals to communicate without meeting in person and collaborate with accomplices. Chat rooms not only provide access to

gather sensitive personal data, but provide a forum as a means to communicate with co-conspirators. Identity thieves use chat rooms, bulletin boards, and Web sites to share knowledge about tactics and techniques of their tradecraft.

The Need for a Threat Model

Perpetrators of identity theft can be grouped into three distinct categories: organized criminal groups or networks, terrorist organizations and sympathizers, and individual criminals. Criminal networks may use identity theft to facilitate financial fraud and other criminal activities and to avoid law enforcement detection. Terrorist organizations and affiliates use identity theft for fundraising, information gathering activities, and to disguise the identities of their operatives. Identity theft, when perpetrated by a terrorist organization or affiliate, constitutes a significant threat to national security. Generally, the individual identity thieves, who may have access to sensitive consumer and personal data through their positions of employment or ability to gain unauthorized access to computer systems, seek an easy way to make money. These categories are not mutually exclusive. For example, individual criminals may form business relationships with other criminals and terrorists organizations for the purpose of obtaining, selling, and using personal information.

As with any information assurance undertaking, a logical first step is to understand the threats with which one must cope. In the case of biometrics and identity management, such formal threat models are not in evidence. It is missing from the *Capstone Concept of Operations For DoD Biometrics in Support of Identity Superiority*, a serious omission.

Recommendation 43.: The PSA for biometrics should commission development of appropriate threat model(s) and assign responsibility for maintaining currency of the model(s). The Task Force considers such threat modeling to be at the nexus of Intelligence and Information Assurance. Threat model(s) should inform and condition the design, development, acquisition and/or operational deployment of biometrics and identity management systems. __

Identity as the Bedrock of Security…or shifting sands?

We base the entire national security information protection system on personnel security, which is based, in turn, on a vetting process. For our most treasured secrets, *e.g.*, Specially Compartmented Information (SCI), Special Access Programs (SAP), and Restricted Data (RD), we perform an extended background investigation (EBI), and (usually) a "technical interview," aka polygraph examination. But, how do we fix the identity in question? How do we know that the person whose background we investigated, whose polygraph we administered, is the selfsame person who shows up to partake of the secrets? True, we require submission of a fingerprint card and run it through IAFIS, but it is only loosely connected to the polygraph examination, if at all, or to the issuance of subsequent credentials, say, a "badge," which also has a picture on it, but that picture is generally not part of the background investigation. This is, of course, just a particular instance of the difficulty in establishing a (root) identity.

If ever there was a need for firm fixed identity, you might think this would be it, to stiffen the personnel security that underlies our national security information controls. Insofar as biometrics can help bind that identity, you would think we would institute their use. Our unassailable conclusion is that biometrics, here, are a terrific idea.

Recommendation 44.: We recommend that biometrics be used to bind together (a) the identity aspects of background investigation, (b) polygraph and any other vetting techniques, and (c) the issuance of credentials of trust or the conferring of other rights.

In the course of our incidental review of biometric-related security practices in the Intelligence Community, the Task Force did find one commendable practice at one Agency: fingerprinting visitors, trades-people, *etc.*, who come to the headquarters facility and are not cleared, *i.e.*, no background vetting is evident. The prints are then run through the "FBI system" to see if the individual has come in contact with the national criminal justice system. With a significant population processed to date, the "yield" is remarkably high. Nearly one-third of such individuals are known to the national criminal justice system. The reason they have come in contact with the system may be more or less significant. The processing turn-around presently is overnight, so it is more relevant for repeat visitors (although even of interest *ex post facto* for a one-time visitor, depending on the collateral information revealed). Of course, technology and economics will make near-real-time information increasingly affordable. Notwithstanding, an Agency that takes its security seriously, as we might expect of the Intelligence Community, should be interested in such history of a visitor.

Recommendation 45.: Those who manage access to sensitive DoD facilities for uncleared, otherwise unvetted, individuals should be directed to evaluate the cost-benefit of taking fingerprints or other biometrics when such individuals first present themselves and doing a biometric-conditioned "national agency check," and subsequently (at least) a local-store reconfirmation of identity. This non-repudiable entry log would supplement or supplant current paper logs. Pilot programs should be encouraged. The Task Force notes that, ultimately, a cross-facility database might have additional counterintelligence analytic value.

Often, it is wise to protect, sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This is a classic feature of intelligence and military operations; it also potentially applies to biometrics. In all such cases, established procedures are employed to weigh and balance the perceived benefits of disclosing a capability after some "coup" is achieved, versus withholding such information, lest the avenue of that success be jeopardized for future use. We may expect that biometrics-based tools and techniques will be increasingly deployed in sensitive applications, and used to achieve important successes in support of national objectives. In so doing, we must seek to preserve the security of what the intelligence community calls "sources and methods," even while being able to headline the outcomes of such use when otherwise deemed appropriate.

Recommendation 46: The OSD PSA for biometrics, in coordination with appropriate authorities, should seek the creation of comprehensive security policy or policies for biometrics. Such policy should embrace all phases of developmental and operational use, and all other relevant considerations.

Recommendations Summarized

This section recapitulates the recommendations, and where necessary, the supporting observations and conclusions, to be found in-line in the report. They are grouped, non-disjunctively, according to topic. For a fuller understanding of the recommendation the reader is referred to the body of the report where it originated.

Information Management & Information Sharing Issues

Observation: The Department of Defense does not appear to have a comprehensive data architecture for identity management in its various aspects, nor does it appear to have anyone responsible for creating and maintaining such an architecture. This is especially important because the various relevant data sets across which one might wish to operate (i.e., cross reference) are scattered and under "local" control. Indeed, many of the relevant datasets are outside the Department, itself. It is very difficult at present, and institutionally resisted, to at least some extent, to recognize and accept credentials issued by other federal agencies. The "fix" for this suboptimal situation is broadly embraced within "Privilege Management" concepts, discussed in detail later in this report. (Page 19)

Recommendation 1: The PSA for biometrics, in the absence of a PSA for identity management, should identify the responsible actor in the Department and ensure that a data model/architecture is developed and maintained. The PSA should become the "functional advocate" for biometrics and identity management, in terms of their use in the Global Information Grid (GIG). (Page 19)

Observation: Enterprise-wide systems analysis has not yet been brought to bear on the identity-management processes that support DoD missions. The business and work-flow processes are neither documented nor fully understood, it seems, and it is not clear where the accountability for these lies. (Page 24)

Recommendation 2: The PSA for biometrics, in lieu of a PSA for identity management, should assign the accountability for analyzing, documenting, and refining the business and work-flow processes and systems architecture(s). (Page 24)

Finding: A decision to save only the extracted information and discard the "original" entails future risk and serves only to conserve computer storage and processing, each of which is getting cheaper and cheaper. Because the value of a legacy identity database grows non-linearly with the number of individuals, that is, the utility grows faster than the size of the database, discarding the "original" is likely a false economy. It is, however, sobering to "do the math". The FBI digitization standard of 500dpi yields a fingerprint record of 10mb. Lossless compression, in practice, seldom does better than 2:1. The FBI has some 200 million fingerprint cards and its automated system topped 52 million records last July, with 6,000-7,000 new accessions per day. They handle 65,000 service requests per day. (Page 36)

Recommendation 5 : Department of Defense policy should tilt toward saving the "original" biometric (in high resolution) rather than relying only on the processed metric/template. (Page 36)

Recommendation 19.: The OSD PSA for Biometrics, with the ASD/NII should ensure that scalability issues are addressed specifically in anticipation of scaling key identity management systems and processes globally. (Page 56)

Recommendation 20.: The OSD PSA for biometrics should create a sub-working group of the DoD Biometrics Executive Committee, focused on biometrics information/data sharing. This group should be co-chaired by the PSA and representatives from USD/P, with additional members to include at least ASD/NII, USD/I, USD/PR and the Office of the General Counsel (OGC). An early task for this group should be an effort to survey and map the total, DoD-wide biometrics/IM data environment, for all applications, as a baseline analysis to support further architectural efforts. (Page 57)

Recommendation 30.: The OSD PSA for biometrics should support and participate in interagency efforts to develop a cross-government policy framework for the implementation of a Privilege Management architecture, within, across, and building upon the scope of National Implementation Plans and the HSPD-12-directed Identity universe. (Page 64)

Recommendation 31.: Under PSA auspices, a comprehensive registry should be developed and maintained cataloging any and all arrangements for sharing identity-related data. The PSA should clarify authorities for entering into such relationships. (Page 65)

Recommendation 32.: The OSD PSA for biometrics should work within the interagency environment to support the identification of relevant data repositories and organizations across government, which will collectively comprise an integrated data environment (architecture) for biometrics use and storage. (Page 65)

Recommendation 33.: The OSD PSA for biometrics should work with other authorities across the federal government, towards a goal of creating a disaster-recovery and backup-site architecture that encompasses the total biometrics data enterprise upon which the performance of DoD missions is dependent. (Page 65)

Recommendation 34.: The OSD PSA for biometrics should propose a DoD-sponsored, cross-organizational biometrics pilot program to the Program Manager for the Information Sharing Environment (ISE) for inclusion in the ISE implementation road map. The importance of organizational roles and responsibilities defined in the National Strategy for Maritime Security suggests a DoD/DHS sharing effort, focused on functions required by HSPD-13/NSPD-41. (Page 66)

Recommendation 42.: That the PSA for biometrics cause this issue of using the biometric, itself, for remote authentication across a broad multi-use network to be re-examined. Participants in the re-evaluation would include, inter alia, the CIO(s), the ASD/NII, and the DIRNSA. (Page 81)

R&D, Materiel and Technology Issues

Recommendation 3 :   The PSA for biometrics should undertake to develop field-deployable DNA collection and matching equipment that requires less skill to achieve operationally worthy results, and the data architecture for accessing repositories for match should be designed and deployed apace.   Additionally, the PSA, in coordination with appropriate authorities, should investigate options related to organizational, physical and/or data collocation with other/larger elements of the total DoD biometrics/IM enterprise. (Page 32)

Recommendation 6.:   Conduct research focused on defining, verifying, quantifying and improving biometrics collection/matching performance in multi-modal systems.   Evaluate alternative methods for comparing and weighting results of matching algorithms of different biometric modalities within a single system; seek to establish optimal mixes/combinations of modalities in various applications and scenarios.   Examine issues specifically related to multi-modal data storage and system architecture. (Page 48)

Recommendation 7.:   Conduct continuous "Red-Team" efforts to defeat biometric sensors and systems in use in the DoD (collaboration with intelligence agencies is recommended). Incorporate insights gleaned from these processes into improved systems designs.   Incorporate anti-spoofing technology into all practicable DoD biometrics applications, including backfit into existing systems where indicated by operational risk and importance.   Maintain visibility into emergent-modality research to seek to spot spoofing vulnerability/opportunity early. (Page 50)

Recommendation 8.::   Support research efforts by DARPA and others into extended-range human biometric identifiability and tracking. Explore feasibility of "unattended surveillance" of larger areas.   Examine applicability of biometrically-based capability for long-range identity assertion in operational scenarios. (Page 51)

Recommendation 9.:   Explore and develop technical means to conduct strong-biometric collection under apparently innocuous conditions.   This should be possible both within controlled environments (e.g. offices) and otherwise. (Page 51)

Recommendation 10.:   Quantify, operationalize and improve upon 3D imagery as a basic biometric modality. Explore development of coherent, bistatic 3D imagery collection capability, with cameras separated over some distance. Conduct an ongoing, basic-research (6.0/6.1) effort in biometrics, seeking to discover new modalities, and previously-unknown insights from existing collection and operational biometrics.   Seek to identify and operationalize promising new areas of biometrics application, appropriately. (Page 52)

Recommendation 11.:   The OSD PSA for biometrics should work with ASD/NII, DoJ/FBI and the Services to identify and achieve time-based performance requirements for biometrics data transmission, comparison/analysis and return of results, all in the context of operational needs in the various use cases. Establish programs to develop or modify existing biometrics collection and/or data-routing systems to achieve required timeliness. (Page 52)

Recommendation 12.: Given the expected expansion of biometrics applications and use-case scenarios, ensure that field-use biometrics collection and analysis systems are designed to function effectively across the whole range of physical environments. If there are cases where the basic science involved prohibits or inhibits this, identify and document these for the benefit of operational planners. (Page 53)

Recommendation 13.: Define and measure ethnologic and/or regional differences in performance of biometrics modalities which effect large groups or whole populations. Ensure that these insights are known to operational planners. In cases where such differences can be accounted for by adjustments or controls in collection or matching processes, provide for the means to adjust such settings in field-deployable equipments. (Page 53)

Recommendation 14.: Support multi-agency research to identify and refine possible new biometric modalities related to residual/latent information. (Page 53)

Recommendation 15.: Ensure that testing & evaluation processes are available and used, as appropriate to the nature and needs of biometrics systems design and modification. (Page 54)

Recommendation 16.: Ensure that there is an aggressive technology insertion strategy to complement the research agenda. (Page 54)

Recommendation 17.: The OSD PSA for biometrics should examine the technical capabilities of the department for biometrics conformance testing capabilities, in cooperation with other federal authorities/capabilities in this area. Upon appropriate coordination, the PSA should support programmatic efforts to establish, maintain and support testing capabilities to support DoD's needs, and role(s) in the total federal biometrics effort. (Page 55)

Recommendation 18.: That the OSD PSA for Biometrics with the USD/Comptroller and Chief Financial Officer, support the development and use of Return-on-Investment (ROI) modeling for significant biometrics applications in the Department. (Page 55)

Recommendation 19.:: The OSD PSA for Biometrics, with the ASD/NII should ensure that scalability issues are addressed specifically in anticipation of scaling key identity management systems and processes globally. (Page 56)

 Recommendation 34.: The OSD PSA for biometrics should propose a DoD-sponsored, cross-organizational biometrics pilot program to the Program Manager for the Information Sharing Environment (ISE) for inclusion in the ISE implementation road map. The importance of organizational roles and responsibilities defined in the National Strategy for Maritime Security suggests a DoD/DHS sharing effort, focused on functions required by HSPD-13/NSPD-41. (Page 66)

Recommendation 42.: That the PSA for biometrics cause this issue of using the biometric, itself, for remote authentication across a broad multi-use network to be re-examined. Participants in the re-evaluation would include, inter alia, the CIO(s), the ASD/NII, and the DIRNSA. (Page 81)

Issues beyond the Department of Defense

Recommendation 23.: The OSD PSA for biometrics should establish and maintain its position as the focal point for all DoD biometrics activities at the interagency level. (Page 60)

Recommendation 24.: The OSD PSA for biometrics should establish the policy and technology basis for associating biometrics with the broader field of Identity Management, in the whole range of DoD applications and requirements, and support interagency efforts to do the same. (Page 61)

Recommendation 26.: Working with and through established interagency lead organizations and processes, the OSD PSA for biometrics should contribute to the development of strategic national objectives of the United States as regards biometrics and identity management, in support of international engagement on these topics. (Page 61)

Recommendation 27.: The OSD PSA for biometrics should ensure that the DoD maintains strong support for, and participation within, domestic and appropriate international biometrics standards bodies. DoD technical centers of excellence and the PSA should ensure that organizational resources and individual incentives are provided. If other DoD entities are empowered to represent the department at any such fora, they should fall under PSA authority and guidance in all matters under consideration. (Page 62)

Recommendation 29.: The OSD PSA for biometrics should ensure that DoD continues to co-chair (with NIST) the interagency standards and adoption coordination process through the NSTC subcommittee on biometrics. (Page 63)

Recommendation 30.: The OSD PSA for biometrics should support and participate in interagency efforts to develop a cross-government policy framework for the implementation of a Privilege Management architecture, within, across, and building upon the scope of National Implementation Plans and the HSPD-12-directed Identity universe. (Page 64)

Recommendation 32.: The OSD PSA for biometrics should work within the interagency environment to support the identification of relevant data repositories and organizations across government, which will collectively comprise an integrated data environment (architecture) for biometrics use and storage. (Page 65)

Recommendation 33.: The OSD PSA for biometrics should work with other authorities across the federal government, towards a goal of creating a disaster-recovery and backup-site architecture that encompasses the total biometrics data enterprise upon which the performance of DoD missions is dependent. (Page 65)

Issues within the Department of Defense

Recommendation 2 : The PSA for biometrics, in lieu of a PSA for identity management, should assign the accountability for analyzing, documenting, and refining the business and work-flow processes and systems architecture(s). (Page 24)

Recommendation 18.: That the OSD PSA for Biometrics with the USD/Comptroller and Chief Financial Officer, support the development and use of Return-on-Investment (ROI) modeling for significant biometrics applications in the Department. (Page 55)

Recommendation 20.: The OSD PSA for biometrics should create a sub-working group of the DoD Biometrics Executive Committee, focused on biometrics information/data sharing. This group should be co-chaired by the PSA and representatives from USD/P, with additional members to include at least ASD/NII, USD/I, USD/PR and the Office of the General Counsel (OGC). An early task for this group should be an effort to survey and map the total, DoD-wide biometrics/IM data environment, for all applications, as a baseline analysis to support further architectural efforts. (Page 57)

Recommendation 24.: The OSD PSA for biometrics should establish the policy and technology basis for associating biometrics with the broader field of Identity Management, in the whole range of DoD applications and requirements, and support interagency efforts to do the same. (Page 61)

Recommendation 28.: The OSD PSA for biometrics should assume the Chair of the DoD Biometrics Standards Working Group (BSWG). The PSA should manage the work of that group to address and consider relevant areas of technical and policy concern, while continuing to maintain full visibility towards, and participation of, US government partner organizations. (Page 62)

Recommendation 35.: Establish a focused identity management and biometrics doctrine effort at the Joint Forces Command, to identify and manage operational needs of the combatant commanders in this area. This organization must also develop TTP for biometric use in coalition/international force operations, where additionally, complex issues of data sharing and differing national perceptions of, and rules regarding, "privacy," etc apply. (Page 67)

Recommendation 36.: The OSD PSA should work with USD/P&R to establish an "Identity Management Community" within the DoD, to establish, support and manage a career-long continuum of training, education and professional development in this field. (Page 67)

Recommendation 37.: Create a program of formalized biometrics training, addressing the need at multiple levels: (Page 67)
- Senior awareness and orientation to expose uniformed and civilian seniors to the high-level issues, implications and applications of ID Management;
- S&T education to keep up with, and even advance, the state of scientific development of biometrics within the DoD;
- Theater/Operational level, for uniformed managers and specialists;
- Equipment-level operations.

Recommendation 38.: The OSD PSA for biometrics, in coordination with and supported by the USD/P&R, should examine the model used to support and encourage the emergence of Information Assurance (IA) as a recognized and accredited academic discipline in the 1990's, in terms of its possible relevance for reproduction and application to IM/biometrics. In the IA case,

the National Security Agency provided technical advice and oversight; sponsored conferences, papers and some basic research; established standards for accreditation; and awarded recognition and other resources to qualifying institutions.   This strategy is perceived to have been instrumental in accelerating the definition and emergence of IA as a specific professional field, just in time to support the Department's, and the nation's, rapidly-expanding needs. We believe the current circumstances related to biometrics, and especially to identity management, demonstrate many similarities. (Page 68)

Recommendation 43.: The PSA for biometrics should commission development of appropriate threat model(s) and assign responsibility for maintaining currency of the model(s). The Task Force considers such threat modeling to be at the nexus of Intelligence and Information Assurance. Threat model(s) should inform and condition the design, development, acquisition and/or operational deployment of biometrics and identity management systems. (Page 82)

Recommendation 45.: We recommend that biometrics be used to bind together (a) the identity aspects of background investigation, (b) polygraph and any other vetting techniques, and (c) the issuance of credentials of trust or the conferring of other rights. (Page 83)

Recommendation 46:   The OSD PSA for biometrics, in coordination with appropriate authorities, should seek the creation of comprehensive security policy or policies for biometrics. Such policy should embrace all phases of developmental and operational use, and all other relevant considerations. (Page 84)

DoD Organizational Issues

Recommendation 4:   DoD should formally assign to Armed Forces DNA Identification Laboratory (AFDIL) the ancillary forensic/counterterrorism intelligence mission(s) and provide oversight, policy and fiscal guidance, and connectivity as required. (Page 32)

Recommendation 21.: The OSD PSA for biometrics, in coordination with the USD/I, should assume control and direction of the DIA-based National Signatures Program human biometrics effort. He should decide whether or not to continue this new effort; if so on what basis, and with what goals. (Page 57)

Recommendation 22.:: The OSD PSA for biometrics should define, with the ASD/Health Affairs and the USD/Intelligence, the creation of Command and Control reporting and programmatic relationships in identity management for the Armed Forces DNA Identification Laboratory (AFDIL) in Rockville, MD. (Page 57)

Recommendation 25.:   The Secretary of Defense should consider the establishment of a dedicated, senior-level position on the OSD staff. This official should have cognizance over all Identity Management activities across the Department, and should also represent the department's total interests in this area externally, coordinating appropriately with other US governmental departments and agencies, and international partners. The PSA for Biometrics would report to this office. (Page 61)

Recommendation 46:   The OSD PSA for biometrics, in coordination with appropriate authorities, should seek the creation of comprehensive security policy or policies for biometrics. Such policy should embrace all phases of developmental and operational use, and all other relevant considerations. (Page 84)

Legal and Privacy Issues

Recommendation 20.: The OSD PSA for biometrics should create a sub-working group of the DoD Biometrics Executive Committee, focused on biometrics information/data sharing. This group should be co-chaired by the PSA and representatives from USD/P, with additional members to include at least ASD/NII, USD/I, USD/PR and the Office of the General Counsel (OGC). An early task for this group should be an effort to survey and map the total, DoD-wide biometrics/IM data environment, for all applications, as a baseline analysis to support further architectural efforts. (Page 57)

Recommendation 31.: Under PSA auspices, a comprehensive registry should be developed and maintained cataloging any and all arrangements for sharing identity-related data. The PSA should clarify authorities for entering into such relationships. (Page 65)

Observation: This ability to cross reference and draw new, previously unimagined, inferences is, at once, the strong selling point for identity management and the bane of privacy advocates. The privacy challenge is real, even when any or all of the individual systems have been designed and are operating securely and in a manner consistent with applicable law and sensitive to privacy and other considerations. (Page 70)

Recommendation 39.:   The designated PSA for biometrics (and, ultimately, for identity management) should ensure that privacy considerations are brought to the fore early in the requirements and design phase of any system; and the scope of the considerations must extend beyond the individual system to include other systems with which a user might interact. Policies and procedures, ideally implemented in technology, may be required to enforce undesirable commingling of sensitive data. (Page 71)

Recommendation 40.:   The Department of Defense, if not the USG, must seek to engage responsible advocates of privacy early in the design and application of identity management systems; the serious purpose of the system must be communicated and understood; and, the data must be limited to that purpose. (Page 72)

Recommendation 41.:   The OSD PSA for biometrics should request a broad review by the Office of General Counsel (OGC) of the privacy implications of biometrics use within the Department, which should be coordinated with the Department of Justice. Based on the results the PSA, in coordination with the Defense Privacy Board and the OGC, should create comprehensive biometrics privacy policies and strategies as required to support the range of defense missions, consonant with interagency efforts. (Page 72)

Appendix A — Terms of Reference

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

APR 1 3 2006

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board Task Force on Defense Biometrics Program

You are requested to form a Defense Science Board (DSB) Task Force on Defense Biometrics Program.

The Department of Defense (DoD) created a biometrics management approach defined by pre-9-11 documentation. As a result, all activities in the post-9-11 period are reactive with ad hoc resources and management teams responding to warfighter applications that attempt to leverage emerging developments in biometric technologies. Today, DoD must develop a cogent plan of action to institutionalize biometrics as a vital element of the Department's identity management capability.

DoD needs include: (1) development of an effective management plan comprising aspects of the Office of the Secretary of Defense (OSD), the Joint Staff (JS), Military Departments and Combatant Commanders; (2) establishment of an effective approach to resource activities to support emerging warfighter biometric needs in the Global War on Terrorism; (3) establishment of biometric measures of effectiveness; (4) establishment of science and technology activities that promote biometric advancement; and (5) establishment of effective operational support to the warfighter.

The Task Force should address the following:

1. Define the role of biometrics technologies and capabilities within DoD's Mission Space. The Mission Space should identify new customers and partners developed since 9-11 and the ability of biometric technologies to adapt to the changing Mission Space. As a minimum the evolving Mission Space must include interagency and international activities, industry and academic relationships, and Non Government Organizations.

2. Recommend best organizational fit within DoD to implement the biometric and identity management and identity dominance missions. The Task Force should examine the organizational roles which best achieve this in both a DoD wide framework and the interagency framework: Specifically:
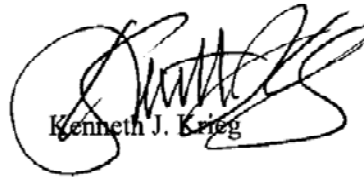
       a. Identify the proper role of OSD. Should a biometrics Principal Staff Assistant (PSA) role exist to champion advocacy, resource sponsorship and requirements validation?

       b. What is the proper role of the Joint Staff and Combatant Commanders in biometric activities?

       c. What role should the Military Departments exercise in biometric activities? Is Executive Agency the proper vehicle for DoD biometric program implementation?

       d. What is the best acquisition mechanism for developing and obtaining biometric capabilities?

       3. Identify the biometric mission space metrics across the major applications (e.g. physical and logical access, intelligence, data sharing, Homeland Defense, force protection/counter terrorism, privacy protection, administrative and business practices – pay, human resource, medical, digital signature etc)

       4. Develop a methodology to address needed taxonomy and policy development activities within the Department of Defense.

       5. Identify the activities required for effective operational support and organizations structure to support those activities.

       6. After its initial report the Task Force should consider the following topics:

       a. Parsing the defense in depth mission space for the biometric community of interest;

       b. Developing a science and technology approach to multimodal analysis of collected biometric data (e.g., matching the fingerprints of an individual collected in one geographic encounter with the iris scan data collected in another);

       c. Developing a technology approach to combining transliteration with biometrics to establish the identity of an individual.

       7. The Task Force will report interim results to USD(P) and VCJCS in May 2006. The final report will be due in Nov 2006.

    The Study will be co-sponsored by myself, as the Under Secretary of Defense (Acquisition Technology and Logistics), the Under Secretary of Defense (Policy) and the Vice Chairman, Joint Chiefs of Staff. Dr. Joe Markowitz will serve as Chairman and Mr. William Gravell will serve as co-Chairman of the Task Force. Ms. Christina

Filarowski Sheaks will serve as Executive Secretary and Maj Chad Lominac, USAF, will serve as the Defense Science Board Secretariat representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Kenneth J. Krieg

Appendix B — Task Force Members and Advisors

Dr. Joe Markowitz, *Private Consultant   -- Chair*

Mr. William Gravell, *Private Consultant   -- Co-Chair*

Task Force Members

Mr. Buddy Beck, *Private Consultant*

ADM Joseph Lopez, USN (Ret.) *Private Consultant*

Mr. Peter Marino, *Private Consultant*

Mr. Mark McGovern, *Lockheed Martin*

Ms. Kathy Pherson, *Pherson Associates, LLC*

ADM Donald Pilling, USN (Ret.), *LMI*

Executive Secretary

Ms. Christina Filarowski Sheaks, *OUSD(P)*

Government Advisors

Mr. Duane Blackburn, *Executive Office of the President, Office of Science and Technology Policy*

Ms. Jeanne Fites, *DUSD(PI)*

Mr Arthur Friedman, *OASD(NII)*

MAJ Michael Galope, USA, *Biometrics Task Force*

Mr. Michael Griffes, *Office of the Secretary of the Navy*

Mr. John Haberkern, *OUSD(I)*

Dr. Steven King, *OUSD(AT&L) S&T*

Dr. Maren Leed, *Office of the Vice Chairman, Joint Chiefs of Staff*

Mr. Robert Lentz, *OASD(NII)*

Mr. Russell McIntyre, *DIA/DT*

CAPT John McLawhorn, USN, *OASD*(*SO/LIC)*

Mr. Al Miller, *OUSD(P)*

Lt Col Harold Montague, USAF, *Joint Staff J-2*

COL Christopher Pritchett, USA, *Joint Staff J-34*

Mr. Ben Riley, *OUSD(AT&L)*

Mr. James Roberts, *OASD(SO/LIC)*

Mr. Monte Strait, *FBI Criminal Justice Information Systems Division*

Mr. Scott Swann, *FBI Criminal Justice Information Systems Division*

Dr. George Webber, *NRAC Task Force on Biometrics*

MAJ Veronica Wendt, USA, *Joint Staff J-6*

Mr. Brad Wing, *DHS*

DSB Secretariat

Maj Charles Lominac, USAF, *Defense Science Board*

Support

Ms. Michelle Ashley, *SAIC*

Ms. Amely Moore, *SAIC*

Appendix C — Briefings Received

12 April 2006

DSB Legal Considerations	Ms. Judy Kim	DoD General Council

2 May 2006

Data Sharing Issues	Mr. Jim Williams	DHS
Biometrics: Potential and Challenges	Mr. John Haberkern	USD(I)
Overview of the NSTC Subcommittee on Biometrics	Mr. Duane Blackburn	EOP/OSTP
Interagency Cooperation and Information Sharing	Mr. Monte Strait	FBI/CJIS
Warfighter Needs	Dr. Maren Leed	OVCJCS
DoD Biometrics Enterprise	Mr. Robert Brandewie	DMDC

11 May 2006

Army Biometrics Overview	MG Conrad Ponder and COL David Scarbalis	CIO/G6
OASD(NII) Perspective on Managing the DoD Biometrics Enterprise	Mr. Robert Lentz	OASD(NII)
OUSD(P&R) Perspective on Managing the DoD Biometrics Enterprise	Ms. Mary Dixon	OUSD(P&R)
Managing a New Enterprise, Lessons from Industry	Mr. Henry Dreifus	DAL

22 June 2006

Strategic Aspects of Biometrics and Structure and Policy implications	LtCol Michael Scheiern	Marine Corps Center for Lessons Learned
Overview of: HumanID at a Distance, Face Recognition Grand Challenge, and Iris Challenge Evaluation	Dr. Jonathan Phillips	NIST
Discussion with DSB Task Force on Biometrics	Mr. John Woodward	Intelligence Policy Center, RAND Corp

13 July 2006

Advanced Biometric Research Development Efforts at the Intelligence Technology Innovation Center	Dr. Michael King	CIA – ITIC
Intelligence and Biometrics	MG Robert Harding, USA (Ret.)	Harding Security
NSA's Biometrics Vulnerability Work	Mr. Adam Whisman	NAS

2 August 2006, Clarksburg, WV

Next Generation Identification	Mr. Gary Barron	FBI/CJIS
IDENT/IAFIS Interoperability	Ms. Cynthia Estep	FBI/CJIS
Multimodal Biometrics	Mr. B. Scott Swann	FBI/CJIS
Biometrics Fusion Center Overview	Mr. Sam Cava	BFC

28-29 September 2006

GIG IA Architecture	Mr. Dave Wennergren	DON-CIO
GIG IA Architecture	Mr. Chris Kubic	NSA
GIG IA Architecture	Mr. George Wauer	OASD/NII
GIG IA Architecture	Ms. Debra Filippe	OASD/NII
USG Interagency Biometrics Coordination	Mr. Duane Blackburn	EOP/OSTP
International Biometric Program Status and International Biometric Technical Standards	Mr. Brad Wing	DHS
DNI'S National Signatures Program	Mr. Ron Fleming	NSP
Social Issues in Biometrics	Mr. Peter Sand	DHS
DNA Biometrics in the DoD	CDR Craig Mallak	Office of DoD Medical Examiner
Biometrics Standards and Interoperability	Mr. Fernando Podio	NIST
Comparative Accuracy of Biometric	Mr. Patrick Grother	NIST

Modalities

Emergent Biometric Modalities	Dr. Larry Hornak	WVU
Carry-over from 2 August Visit to CJIS	Mr. David Cuthbertson	FBI/CJIS
National Biometrics Security Project	Mr. John Siedlarz	National Biometrics Security Project
An Industry Perspective on the Current State of Biometrics and General Trends in the Industry	Mr. Walter Hamilton	International Biometrics Industry Assoc.
New NSA Visitor Policy	Mr. Dave Manning	NSA

Appendix D — Appointing New OSD PSA for Biometrics

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT - 4 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
                    CHAIRMAN OF THE JOINT CHIEFS OF STAFF
                    UNDER SECRETARIES OF DEFENSE
                    ASSISTANT SECRETARIES OF DEFENSE
                    GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
                    DIRECTOR, OPERATIONAL TEST AND EVALUATION
                    INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
                    ASSISTANTS TO THE SECRETARY OF DEFENSE
                    DIRECTOR, ADMINISTRATION AND MANAGEMENT
                    DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
                    DIRECTOR, NET ASSESSMENT
                    DIRECTORS OF THE DEFENSE AGENCIES
                    DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Defense Biometrics

The Director Defense Research & Engineering (DDR&E) is designated the Principal Staff Assistant (PSA) for biometrics, with responsibility for the authority, direction, and control of DoD biometrics programs, initiatives, and technologies.

As PSA, the DDR&E will develop and coordinate DoD biometrics policy, ensuring that other DoD policies are consistent with and support the DoD biometrics enterprise and the interagency. Biometrics policy will be promulgated through the Under Secretary of Defense for Acquisition, Technology, and Logistics.

To fully coordinate and synchronize Defense biometrics requirements, doctrine, organization, training, materiel, logistics, architecture, standards, and funding, the DDR&E will establish the position of Director for Defense Biometrics. The Director for Defense Biometrics will utilize personnel detailed from the DoD Components, as required, to accomplish the central management mission. The Director of Defense Biometrics will be the representative of the Department on biometrics-related matters with agencies of US Government and international organizations, as appropriate.

The DDR&E will approve biometrics funding across the DoD in support of validated requirements and approved standards and architecture. For this purpose, the the Secretary of the Army, as Executive Agent, the Services, and Agencies will submit to the DDR&E funding plan proposals for the Military Departments' biometrics programs. The DoD Components will execute biometrics programs according to the DDR&E-approved plan.

To ensure timely and vigorous action on biometrics-related activities across the Department, the DDR&E, as the PSA, will also establish an Executive Committee. The

Committee will be co-chaired by the DDR&E and a General/Flag Officer named by the Chairman of the Joint Chiefs of Staff. Members of the Executive Committee will include senior representatives of the Department's policy, operations, intelligence, personnel, acquisition, and information communities, the Military Departments, and others as determined by the PSA. As directed by the PSA, the Executive Committee will be supported by the Identity Protection and Management Senior Coordinating Group.

As the Executive Agent, the Secretary of the Army is responsible for ensuring that biometrics data and associated information is fully and promptly accessible to required users. To ensure timely and vigorous action, the Secretary of the Army will support the implementation of joint biometrics capabilities, including joint standards, architecture, and research and development activities as directed by the PSA.

The Secretaries of the Military Departments, the Combatant Commanders, and the Heads of other DoD Components will coordinate with the PSA and the Executive Agent in the development and fielding of biometrics applications, and will submit spend plans for consolidation and approval by the PSA.

This memorandum supersedes conflicting portions of all other DoD issuances and other guidance. The DDR&E, in coordination with the Military Departments and the Director for Administration and Management, will develop a DoD Directive for Defense Biometrics to address this policy and the roles and responsibilities of the DoD Components.

ENGINEERING-PDH.COM
| ELE-142 |

Appendix E — Capstone Operational Scenarios

Taken from *Capstone Concept of Operations (CONOPS) For DoD Biometrics In Support of Identity Superiority* (DRAFT, version 2.0 dated 8 JUL 06)

Track a High-Value Target

While on patrol, a squad of Marines detects an Improvised Explosive Device (IED). Explosive Ordnance Disposal (EOD) technicians render safe the device and collect latent biometric samples (fingerprints and DNA).

The fingerprint samples are formatted into an electronic file, matched to samples on file, and stored locally. There is no match at the local-trusted source, and the data is enrolled into a biometric file. Both the electronic fingerprint file and DNA sample are transmitted to their respective authoritative source for further comparison. Acknowledgement of receipt is transmitted back to the local source. Matching at the authoritative source does not yield a DNA match and the sample is stored for further comparison. These biometric samples are shared with Coalition partners, revealing a fingerprint match to a suspected bomb-maker. Based on this identification, the Coalition partner provides a biometric thermal image of an individual's face and identifying photographic samples.

Analysis of the shared biometric samples and associated information indicates his last reported location was outside the joint area of operations in a country providing sanctuary. This analysis, as well as the samples provided by coalition partners, is sent to the DoD Authoritative Source to update the biometric file. An alert (flag) containing pointers to information located in non-biometric reference data is disseminated to tactical users to facilitate future data comparisons on their local Biometrics systems should they encounter the individual.

A series of raids on suspected insurgent locations provides more biometric samples that are matched to the individual. This match information, the biometric files and the associated information from the previous analysis that led to his being tied to the IED incidents are shared with interested parties for analysis. Analysis of associated information indicates that he is moving within the Area of Responsibility (AOR) and provides possible future locations of the individual. Sensors with Biometrics collection capability are positioned accordingly and succeed in identifying the individual from a distance. Once located, the individual is tracked to the vicinity of a farmhouse. A tactical unit conducts a raid to apprehend him.

The raid force encounters six men at the site, all with authentic-looking identification in their possession. Pictures of the bomb-maker provided to the raid force are outdated and do not closely resemble any individual at the raid site. But a field biometric test matches the suspected bomb-maker. Analysis of that biometric match result and associated information from the previous analysis that tied him to the IED incident enable the raid force leader to decide to detain that man. The other men are released. All collected samples and associated contextual information are updated in their respective biometric files and annotated to reflect that the raid force encountered them in the company of a known bomb-maker. Relevant associated

information found at the scene is also collected by the raid force and subsequently stored in a repository of associated information for use in later analysis.

- **Operational Tasks Achieved Using Biometrics**:
  - ✓ Identify an Unknown Individual During Tactical Operations
  - ✓ Locate a Person of Interest
  - ✓ Track a Person of Interest
  - ✓ Collect Forensic Evidence
  - ✓ Share Identity Information

Maritime Interdiction Operation

The US Navy, with a US Coast Guard Law Enforcement Detachment (LEDET) on board, is conducting a compliant maritime interdiction operation seeking terrorists. After obtaining flag state consent, the LEDET team boards a large container ship and collects biometric samples from each crewman. The data is transmitted to a DoD authoritative source, and is followed up with acknowledgment of receipt. The biometric data is compared against all stored files, and shared with mission partners. A subsequent match is made on three of the crewmen. Furthermore, the matched files show a link to the NCTC's terrorist watchlist. The authoritative source updates the applicable biometric files with newly collected biometric samples and contextual data. The LEDET team is informed of the match result and watchlist status.

Further analysis of the biometric files and additional associated information indicates the three crewmen have travel patterns consistent with those of previously apprehended terrorists. Based on this information, the on-scene commander detains the three crew members pending further disposition.

The on-scene commander further requests, and is granted, flag state authorization to conduct a detailed search of the vessel. In the course of the search, 40 undocumented individuals are discovered in a cargo hold. They are determined to be attempting illegal entry into the US. Also during the search, documents related to the design of an improvised nuclear device are discovered and collected. Biometric samples are collected on the ship's crew and undocumented individuals. The biometric data is again transmitted to the DoD authoritative source and compared to all stored files. No match is made. Each individual's biometric data is enrolled into a biometric file, linked to the WMD information, and stored for later use. The on-sight commander analyzes the results of the biometric match processes and other available information to determine a course of action. The biometric files and related associated information are shared with the mission partners and entered into interagency systems, including the Maritime Domain Awareness Systems, the FBI Criminal Justice Information Systems (CJIS), and DHS Immigration Systems. The on-scene commander informs the appropriate authority and, after receiving flag state and US Government authorization, takes the undocumented individuals into custody pending further disposition.

- **Operational Tasks Achieved Using Biometrics**:
  - ✓ Identify an Unknown Individual during Tactical Operations
  - ✓ Locate a Person of Interest
  - ✓ Track a Person of Interest

✓ Collect Forensic Evidence
✓ Share Identify Information

Interagency Operations in a Foreign Country

US and Allied forces are supporting a foreign state's rebuilding process, which is being undermined by smuggling into the state. The host government has only allowed US forces to use collected biometric data within the host nation. Therefore, all biometric operations are conducted using local un-trusted sources.

In accordance with standard operating procedures, a truck driver provides biometric samples to the border police at a remote international border crossing supported by US military personnel. The biometric samples and contextual information are transmitted to the local un-trusted source and subsequently compared to locally stored biometric files. The truck driver's biometric data does not match any file at the local un-trusted source and a negative response is provided back to the border police. The trucker driver also is checked against local and national criminal records. The border police review the match result, associated information and other available situational information and clear the truck driver to continue. The biometric file is enrolled and stored at the local un-trusted source, as well as shared with US forces, Coalition partners, and non-governmental organizations operating within the country.

Several months later, the host nation's national police, supported by a US Government agency, conduct a raid on a drug-smuggler's safe house and seize numerous documents and other evidence. Biometric samples are collected and compared to the local un-trusted source. A match is made between the latent samples collected during the raid and the truck driver's previous biometric file on file. An analysis of the raid, as well as additional associated information, is completed and the truck driver's non-biometric reference information is updated with these new samples, flagged for future matches, and shared with all local sources within the country.

Several days later, the truck driver attempts to cross at a different border checkpoint. He submits his individual identification and a biometric sample for verification. The sample is compared against the truck driver's biometric sample on file, which alerts the border police to the flag stored at the local un-trusted source. The truck driver is detained for questioning and his biometric file is updated with the newly collected biometric sample and contextual data.

- **Operational Tasks Achieved Using Biometrics**:
  ✓ Identify an Individual During Tactical Operations
  ✓ Locate a Person of Interest
  ✓ Track a Person of Interest
  ✓ Control Physical Access
  ✓ Collect Forensic Evidence
  ✓ Share Identity Information
  ✓ Manage Local Populations during Military Operations

Personnel Recovery

US Government, DoD, Allied, and Non-Governmental Organization (NGO) personnel are conducting stability operations in a country coping with insurgent activity. Several civilians have been abducted.

A US Special Operations Forces (SOF) team receives information from intelligence sources concerning the location of a British government civilian who has been held by insurgents for nearly 30 days.

Prior to conducting a rescue operation, the SOF team downloads digital biometric files and associated information on the captive from the British authoritative source in order to authenticate the individual's identity.

During the operation, the team detains seven individuals at the site and collects their biometric data. Using their tactical biometric device, the team immediately matches one sample to the individual the unit was sent to recover. The team also uses associated information obtained from the British government to verify the identity of the individual.

Other individuals are not immediately matched and their biometric files are transmitted, enrolled, and stored at the authoritative source. The authoritative source acknowledges receipt of biometric files.

The team initiates handling protocols for the rescued captive and detains the remaining individuals. At the repository, the files are processed and stored for future use.

- ▪ **Operational Tasks Achieved Using Biometrics**:
  - ✓ Identify an Individual During Tactical Operations
  - ✓ Locate a Person of Interest
  - ✓ Identify Friendly Forces

Controlling Access

An Air Force civilian is scheduled to visit a US military installation. Notification of approval for the visit has been sent to the installation's access control office roster. At the installation's main gate, the base's access control system scans the visitor's official individual biometric-enabled identification token, collects a biometric sample, and verifies the visitor's credentials and authorization based on a positive match with the appropriate access roster. The access control office grants installation access privileges based on the visitor's identification data, DoD affiliation, and the current threat level. The Air Force civilian's biometric file is updated.

Upon completion of in-processing, the visitor is granted access to specific parking lots and buildings on the installation. The validation process is repeated in a layered security procedure, using the individual's specific identification biometric-enabled token processed by networked security access control devices. The visitor's identification and access level is confirmed at each location. The visitor enters the main building for a scheduled meeting, where he must provide a biometric sample to gain access. The collected sample is compared to the local trusted source,

and following a positive match access is granted. Physical security personnel ensure that the visitor does not possess any prohibited items.

While waiting for the meeting to begin, the visitor decides to use the common computer workstation to review information relevant to his upcoming meeting. The workstation's network security repeats the security process, using the individual's biometric-enabled identification token data and real-time biometric samples provided by the individual. Information Assurance is provided through the use of identification and authentication. The workstation network client enables the user's configuration data in hardware and software for workstation operations, communications, a list of permitted installation and building network resources, and associated file data.

- ▪ **Operational Tasks Achieved Using Biometrics**:
  - ✓ Identify Friendly Force Individuals
  - ✓ Authorize Access to Privileges
  - ✓ Control Physical Access
  - ✓ Enable Information Assurance

Disaster Relief

The US Government is responding to a request from a country that has experienced a catastrophic disaster. The disaster has created the immediate need to locate, rescue, and manage the affected population.

The host government approves the Coalition response force to collect biometric samples from the civilian population to assist with disaster relief efforts with the stipulation that: (a) the biometric information only be used to identify individuals located and rescued and to manage the flow of casualties and the displaced population; and (b) the biometric information not be removed from the country.

Biometric data is collected as the affected individuals are rescued, treated or entered into the refugee management process. DoD personnel utilize the collected biometric files stored in the local un-trusted source as the reference set against which subsequent matches are made. As personnel are placed aboard transportation, provided medical care or basic services at a disaster relief site, the individuals' biometrics are the "tokens" that authorize their access. In each instance, once the biometric file is matched, the identity is referenced against repositories of non-biometric information such as camp rosters, medical records, records of service provided, transportation logs, etc. to enable better management of services provided and needs of the population. This data and the collected biometrics are shared with the host nation and our coalition partners to assist in integrating their relief efforts with those of US forces. The host nation also compares the collected information to compare with whatever repositories of non-biometric data may have survived the disaster (tax records, census data, etc) to assist in the speedy location and reuniting of families. At the request of relief organizations, the national government shares the biometric data and identification results with NGOs and neighboring countries affected by the refugee flow.

- **Operational Tasks Achieved Using Biometrics**:
  - ✓ Manage Local Populations during Military Operations
  - ✓ Manage Emergency Situations
  - ✓ Share Identify Information

Access to Services for Non-US Personnel

While operating in the host nation, the US contracts with local nationals to provide labor and services. As a condition of employment, the laborer must provide individual identity information and biometric samples for screening and background check purposes. Biometric samples are taken and matched against both host nation and US authoritative sources. Both positive and negative matches result in the update and enrollment of individual biometric files, respectively. Additionally, once stored, these biometric files are shared with host nation and US non-DoD parties for subsequent analysis and fusion of applicable biometric and associated information (e.g., criminal records). Based on this exhaustive research, the US military decides whether to offer employment and issue Biometrics-enabled identity cards to the job applicant. Successfully screened laborers receive identity cards that they must display to access the base and receive wages for work performed. Biometric matching of all laborers is conducted on payday to confirm identity prior to payment.

One individual has lost his ID card, but his biometric sample matches his file in the local trusted source. Analysis of associated information by finance personnel indicates that he worked every day. He is paid. The worker's biometric file is updated.

A second individual presents his ID card and a biometric sample. He is matched to the local trusted source, but his biometric file indicates his record is flagged for being fired two days ago. Finance personnel determine how much he is owed and he is required to surrender his ID card upon leaving the installation.

A third individual provides his ID card. His picture appears to match; however, his biometric sample does not match to any individual stored in the local trusted source. On-scene analysis reveals he is the brother of an actual worker. The individual is detained and escorted off base. A biometric file is created and stored at the local trusted source and later shared, along with other non-biometric information, with non-DoD partners. Additionally, a flag with this information is attached to his biometric file for possible disciplinary action the next time he attempts to enter the base. The brother's (actual worker) biometric file is also flagged to indicate his credentials have been compromised, and this information is provided to other relevant authorities.

- **Operational Tasks Achieved Utilizing Biometrics**:
  - ✓ Identify Unknown Individuals During Tactical Operations
  - ✓ Manage Local Populations during Military Operations
  - ✓ Authorize Access to Privileges
  - ✓ Control Physical Access

Foreign Humanitarian Assistance-Relief Mission

The US military is responding as part of an international disaster relief effort. Thousands of injured are being treated and awaiting further treatment as soon as field medical hospitals are assembled and operational. All individuals who receive medical attention within the disaster area are immediately enrolled in a DoD biometric local un-trusted source that has been established for management of the refugees. All treatment records are linked to their respective biometric files. Many of the injured, after being initially treated, voluntarily relocate within the disaster area. This movement is making it difficult for medical personnel to efficiently provide medical services or track patients for follow-up treatment.

Navy Corpsmen are performing triage for refugees arriving by buses at one of the newly established US field hospitals. The Corpsmen collect biometric samples from each refugee for identification purposes as part of the initial medical assessment process. The biometric files are then sent for matching against the local un-trusted source to assist with the identification of the individual and retrieve any available treatment history.

A refugee who cannot be matched against the local un-trusted source is enrolled as a new biometric file. All subsequent medical treatment will later be linked to that file. When a refugee is positively matched against the local un-trusted source, links to his medical history are accessed and his prior treatment records are retrieved. Subsequent treatment is updated in the refugee's medical record so that information can be accessed by others again in the future through utilizing the established net-centric links between the non-biometric repository (medical files) and his biometric file. The Corpsman uses these medical records to aid in triage.

- ▪ **Operational Tasks Achieved Utilizing Biometrics:**
  - ✓ Manage Local Populations During Military Operations
  - ✓ Manage Emergency Situations
  - ✓ Share Identity Information

Theater Security Cooperation and Exercises

The US military furthers security cooperation through Medical Civic Action Programs (MEDCAPs) to remote regions of allied nations in conjunction with port visits and combined military exercises.

During an annual combined exercise, an Army medical detachment executes MEDCAPs in a number of villages within the exercise Area of Operations (AOR). Army medics collect biometric information on those who receive vaccinations and medical treatment during the MEDCAPs. Biometric files are enrolled and stored for each individual receiving treatment and/or vaccinations. These biometric files are linked to subsequent treatment and vaccination records stored in other repositories of associated information.

The following year a different Army medical detachment deploys to the AOR to perform MEDCAPs. At the first village, Army medics encounter far more villagers awaiting vaccination than anticipated, creating concern that the amount of on-hand vaccine is insufficient. To assist the ongoing mission, a repository of associated information has been established during previous

MEDCAP exercises. Biometrics samples are collected on each person awaiting vaccination and matched to the local-trusted source.   Numerous positive matches occur. These match results are compared against the repository of associated information to identify which individuals received vaccinations in the past.   Analysis of the match results and the repository of associated information reveals that a large number of those awaiting vaccination have already received the vaccine during previous MEDCAPs.

Relying on the biometric data, the on-scene commander orders vaccination of only those with no biometric match and those with biometric matches whose linked medical treatment record does not indicate the vaccine was previously received. The villagers are briefed accordingly.

The Army medics successfully complete the MEDCAP with the vaccine on hand. The on-scene commander is confident that the total supply of vaccination is sufficient for future MEDCAPs based on the biometric matches experienced in this initial MEDCAP.

- **Operational Tasks Achieved Utilizing Biometrics:**
  - ✓ Manage Local Populations During Military Operations
  - ✓ Authorize Access to privileges
  - ✓ Share Identity Information

Foreign Humanitarian Assistance—Security Mission

The US and Coalition partners operate from several dozen military bases in an allied nation and contract locally for a wide range of services, such as: vehicle rental and maintenance, civil construction, provisioning of food and water, and waste removal. Biometrics is collected to support a wide range of activities, from base access to monitoring all contracting activities. All biometric data are matched against the local-trusted source and repositories of associated information for the purposes of vetting. All samples reveal a negative match and are enrolled in the local-trusted source and transmitted to the authoritative source.

Several base contracting officers encounter a dishonest local contractor who is awarded contracts and receives partial payment but never performs the work, essentially disappearing with the money. This associated information is analyzed with relevant biometric data. This analysis is transmitted to the authoritative source, the individual's biometric file is flagged, and repositories of associated information are modified for future analysis to indicate he is barred from further contracts. This information is then shared with local-trusted sources and other interested parties.

The dishonest local contractor relocates to another region and applies for new US and coalition contracts using a different company name and false personal data. The contracting official collects his biometric sample and requests a match from the local-trusted source. A subsequent positive match reveals a flag directing the user to relevant associated information indicating his previous activities and status. His bids are eliminated. The dishonest contractor's biometric file is updated with the newly collected biometric sample and contextual data, and the attempt is shared with all appropriate authorities.

A newly-arrived disbursing officer is ordered into the local community to pay a contractor for recently completed work. This officer has never met the local national to whom he is to pay a

large sum of cash. Following the directions provided by a local interpreter, the disbursing officer arrives at what he believes is the office of the intended contractor. Unbeknownst to the disbursing officer, he has arrived at a fake contractor's office. As a condition of payment the supposed contractor provides his biometric information. A field match test reveals the presented biometric samples do not match the biometric file of the individual identified in the contract. The disbursing officer refuses to pay despite the local interpreter's and contractor's insistence.

Upon returning to base the disbursing officer provides the collected biometric information and his incident report to the Provost Marshal for investigation with the local police. The local interpreter is immediately detained on-base for questioning. The fraudulent contractor's biometric file is enrolled and stored within the local-trusted source, transmitted to the authoritative source, and shared with interested parties. Upon conclusion of the investigation, the Provost Marshal concludes that the contractor is a fraud. US military contracting offices operating within the region as well as the host nation update their respective repositories with this information.

- **Operational Tasks Achieved Utilizing Biometrics:**
  - ✓ Manage Local Populations During Military Operations
  - ✓ Control Physical Access
  - ✓ Share Identity Information
  - ✓ Track a Person of Interest
  - ✓ Authorize Access to Privileges

United States Law Enforcement Support

A squad on a patrol is attacked by armed plainclothes fighters. After the initial skirmish, the fighters surrender their arms and are detained by US military forces. A search of the subjects' possessions reveals falsified identification documents from Iraq, Afghanistan, and Pakistan.

Biometric samples are collected from each of the detainees and are transmitted to a DoD authoritative source. The data is compared against all files within the authoritative source and a positive match is made on two of the individuals. Match results indicate these two subject's biometrics had been found at a location containing bomb-making materials in Yemen around the time of the USS Cole attack.

After updating and storing the subjects' new biometric files, the DoD shares all of the biometric samples and associated information with the Federal Bureau of Investigation's (FBI) biometric database, which in turn also automatically shares the files and associated information with the Department of Homeland Security (DHS). After analysis of available biometric and associated information, the subjects are nominated and promoted by the National Counter-terrorism Center (NCTC) as Known or Suspected Terrorists. The subjects' biometric files are flagged and linked to the NCTC's terrorist watch list at the DoD Authoritative Source, as well as entered into the FBI's Known or Suspected Terrorist (KST) database.

Several months later, the detainees are released to a foreign government for adjudication and repatriation.

Several years later, a US police department responds to a trespassing complaint at a local water treatment plant, which services a large metropolitan area. Two subjects are apprehended and fingerprints are taken at the police department's primary booking station. The fingerprints are transmitted to the FBI's fingerprint database and matches are made against the previously shared biometrics files collected from the military detainees. Because the fingerprints have been entered into the FBI's KST file, the FBI CJIS Division Intelligence Group immediately alerts the Terrorist Screening Center (TSC) of the encounter. Upon notification, the TSC advises the local Joint Terrorism Task Force to investigate whether the trespassing act was an indication of a terrorist threat to the nation.

Operational Tasks Achieved Using Biometrics
- ✓ Identify An Unknown Individual During Tactical Operations
- ✓ Share Identity Information
- ✓ Locate a Person of Interest
- ✓ Track a Person of Interest
- ✓ Collect Forensic Evidence

United States Border Protection Support

Allied forces are supporting a foreign country's operation to neutralize a suspected WMD bomb-making facility within the country's borders. During a successful raid of the facility, US military forces locate stockpiles of improvised explosive devices and detain several subjects in connection with the operation.

The subjects are turned over to the foreign country's government after biometric samples and contextual data are collected and transmitted to a DoD Authoritative Source. The data is compared against all files within the authoritative source and no matches are made on any of the individuals. The DoD Authoritative Source enrolls the new biometric files. The DoD shares the biometric files and associated information with the FBI. There are no matches at the FBI's database

Several months later, the subjects escape from the foreign government's prison system.

Several years later, the Department of Homeland Security's (DHS) Bureau of Customs and Border Protection (CBP) collects a visitor's fingerprints during a primary border-entry check. The CBP Bureau transmits the biometric information to the DHS authoritative source. Through system interoperability with the FBI's biometric database, DHS identifies one of the subjects as having been previously detained at the WMD bomb-making facility.

Upon notification of the match, the primary border check escalates to a secondary CBP inspection and an investigation into the encounter is initiated. After a more detailed inspection, an improvised explosive device is found concealed in the subject's vehicle and is later determined to be a WMD. The subjects are immediately detained and handed over to the FBI for further questioning.

Operational Tasks Achieved Using Biometrics
- ✓ Identify An Unknown Individual During Tactical Operations

- ✓ Share Identity Information
- ✓ Track a Person of Interest
- ✓ Control Physical Access

Appendix F—Information Assurance: CAC Authentication[50]

The fundamental goal of using the Common Access Card (CAC) is to authenticate the identity of the cardholder (Uniformed Military and Civilian DoD personnel and Contractors) to a system or person that is controlling access to a protected resource or facility. This end goal may be reached by various combinations of one or more of the validation steps described below.

Card Validation

This is the process of verifying that a CAC Card is authentic (i.e., not a counterfeit card) and has not been subjected to tampering or alteration. Card validation mechanisms include:

- Visual inspection of the tamper-proofing and tamper-resistant features of the CAC.

- Use of cryptographic challenge-response schemes with symmetric keys,

- Use of asymmetric authentication schemes to validate private keys embedded within the CAC Card.

Credential Validation

This is the process of verifying the various types of credentials (such as visual credentials, CHUID[51], biometrics, CAC keys and certificates) held by the CAC. Credential validation mechanisms include:

- Visual inspection of CAC Card visual elements (such as the photo, the printed name, and rank, if present),

- Verification of certificates on the CAC,

- Verification of signatures on the CAC biometrics and the CHUID,

- Checking the expiration date,

- Checking the revocation status of the credentials on the CAC.

Cardholder Validation

This is the process of establishing that the CAC Card is in the possession of the individual who is the legitimate owner of the card. Classically, identity authentication is achieved using one or more of these factors: a) something you have, b) something you know, and c) something you are.

---

[50] Sources: FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors (March 2006)
NIST SP 800-73-1, Interfaces for Personal Identity Verification (March 2006)
NIST SP 800-76, Biometric Data Specification for Personal Identity Verification (February 2006)
NIST SP 800-78-1 Draft, Cryptographic Algorithms and Key Sizes for Personal Identity Verification (June 2006)

[51] CHUID -Card Holder Unique IDentifier

The assurance of the authentication process increases with the number of factors used. In the case of the CAC Card, these three factors translate as follows: a) something you have – possession of a CAC Card, b) something you know – knowledge of the PIN, and c) something you are – the visual characteristics of the cardholder, and the live fingerprint samples provided by the cardholder. Thus, mechanisms for CAC cardholder validation include:

- Presentation of a CAC Card by the cardholder,

- Matching the visual characteristics of the cardholder with the photo on the CAC Card,

- Matching the PIN provided with the PIN on the CAC Card,

- Matching the live fingerprint samples provided by the cardholder, with the biometric information embedded within the CAC.

Operational Tasks Achieved Utilizing Biometrics:
- ✓ Authorize Access to Privileges and Resources
- ✓ Control Physical Access
- ✓ Enable Information Assurance

Appendix G — Security Clearance Use Case

Individual contemplating service in the United States Armed Services submits to the collection of electronic fingerprints at the Military Entrance Processing Command (MEPCOM) facility. The electronic fingerprint files are then electronically sent to the Office of Management and Budget and the FBI for comparison matching with the criminal fingerprint database as a component of a National Agency Check (NAC).

During the course of the NAC, the prints are compared to the DoD ABIS database which contains latent prints collected by DoD.

Once the NAC is completed the fingerprint files is stored in the FBI Integrated Automated Fingerprint Identification System (IAFIS) Civil Files database. The file remains on file for 100 years, however, currently cannot be accessed for additional match purposes.

Should a Department of Defense employee or service member require access to a higher levels of secure information, a background investigation or special background investigation is conducted. During these investigations a digital fingerprint file is collected from the individual and a match against the master criminal database is again performed as well as a match against the previously submitted prints maintained in the civil files. (Currently that second set of prints is also retained in the IAFIS Civil Files, but cannot be matched against the prior set of prints in the files).

Note: Prints are not requested from individuals undergoing periodic security clearance reinvestigations.

Connectivity to the authoritative database uses a highly security encrypted web centric network.

Operational Tasks Achieved Using Biometrics:
- ✓ Establish the Military Identify an Individual
- ✓ Validation that Individual's prints do not have a latent match
- ✓ Periodic revalidation of an individual's identity

Appendix H — Pay and Benefits Use Case

After discussing options for enlisting in the Navy, a seaman apprentice begins his/her paperwork to enlist. Prior to departing the U.S. Military Entrance Processing Command (MEPCOM) facility, 10 fingerprints are collected and linked to identification credentials and citizenship documentation to establish the individual's military identity. The fingerprints are electronically stored at the Defense Manpower Data Center, Monterey, California. And paper fingerprint cards are sent to the FBI for a background check. Weeks later, the individual enters a classroom to take a battery of tests to determine the best fit for his/her skills for assignment in the Navy. To ensure the same person who enlisted at the MEPCOM facility is the same individual taking the tests, a live scan verification of an index finger is compared with the fingerprint template collected during enlistment at the MEPCOM facility.

After completion of enlistment in-processing, the seaman apprentice enters basic training at the Naval Training Center at Great Lakes, Illinois. Once again during check-in, the individual's index finger is live scanned to verify identity prior to beginning basic training.

After completion of basic training, the individual's military identity is verified using a live scan collection of a index finger, he is then enrolled into the Defense Enrollment Eligibility Reporting System (DEERS) using the Real-time Personnel Identification System (RAPIDS). During this enrollment process two index fingers are live scanned into the DEERS database. Once enrolled in the DEERS database, any changes to pay or benefits during the duration of military service requires identity verification using a live scan collection of an index finger print. This live scan is compared using a one on one match to the fingerprint template on file at the Defense Manpower Data Center, Monterey, California. Identity, once verified, enables the individual to modify/confirm pay and benefit entitlements. These entitlements may be modified to reflect changes in marital status, birth of a child or movement to a new duty station and other factors affecting pay and benefits.

The fingerprint samples are formatted into an electronic file, matched to samples on file, and stored in a central database at DMDC. There is no matching to local-trusted biometric databases. Both template and image electronic fingerprint files are maintained by DMDC. Matching with the DMDC authoritative database only uses templates to reduce the time required for identity validation from over 30 seconds for images to approximately two seconds. This same authoritative database is used to validate identity during the issuance process for the Department of Defense Common Access Card (CAC).

Connectivity to the authoritative database uses a highly security encrypted web centric network. To access the network, a combination of Public Key Infrastructure (PKI) (private and public keys) are linked to the authorization permissions granted to a CAC holder using the same fingerprint matching algorithm previously delineated to verify military identity.

Operational Tasks Achieved Using Biometrics:
     ✓ Establish the military identity of a previously unknown individual
     ✓ Verify the military identity of a person requesting military pay and benefits

✓ Verify the military identity of a person being issued a military credential to enable pay and benefits access

Appendix I — Humanitarian Assistance Use Case

During hurricane evacuation operations the Department of Defense was requested by the Federal Emergency Management Agency (FEMA) to assist with evacuee accountability and evacuation activities. Over 100 enrollment stations are established in a greater metropolitan area using man-portable enrollment stations manned by Federalized National Guard personnel. Each evacuee prior to accessing a public transportation conveyance (bus, plane, boat) is enrolled in the Evacuee Tracking and Accountability System (ETAS). Enrollment requires the entry of a name, fingerprints and a digital picture into a centralized database. Each evacuee is issued a wristband embedded with a barcode before leaving the evacuation area. After the individual arrives to a "safe harbor" location, identity is verified using fingerprints before food, money and shelter are provided to measure the amount of relief aid provided and prevent fraud.

After the evacuees are safely situated in safe harbor a temporary identification card can be issued using the fingerprints and digital photo collected at the point of evacuation to validate evacuee identity. This identity can be later used to provide a means to reunify families and provide rapid dispensing of relief aid.

The fingerprints and digital photos are formatted into an electronic file and stored in a central database. There local-trusted biometric databases will be created in the absence of connectivity with the internet. These local databases will later be added to a centralized authoritative database which will be used to validate identity during the remainder of the hurricane disaster.

Connectivity to the authoritative database uses a highly security encrypted web centric network.

Operational Tasks Achieved Using Biometrics:
- ✓ Establish the disaster identity of a previously known or unknown individual
- ✓ Verify the disaster identity of a person requesting disaster relief benefits
- ✓ Verify the disaster identity of a person being issued a temporary credential to enable benefits access

Appendix J — Medical and Mortuary Scenarios

Biometric, but not Identity Management

A US Special Operations Forces (SOF) team engaged a fortified position of insurgents resulting in the wounding of several SOF personnel.

A SOF medical team responds and reads the recorded biometric information from medical transponders on the wounded personnel to determine the priority of treatment for each individual. Key biometric information includes heartbeat signatures and vital organ electrical outputs.

Identity Management

After searching the battlefield area, the remains of a soldier are found in close proximity to the crater of an impacted mortar round. The body parts are unidentifiable and no fingers are found to collect fingerprints. The field medical unit collects DNA samples and available teeth for identification purposes. The remains of the soldier are transported to the United States. At Dover Air Force Base, Delaware Mortuary Affairs in cooperation with the Armed Forces Institute of Pathology use the biometric identifiers in DNA and dental fragments to identify the deceased unknown soldier.

Operational Tasks Achieved Using Biometrics:
- ✓ Identify an Individual During Tactical Operations
- ✓ Identify a deceased individual

Appendix K — IED-Forensic Scenario

Scenario Prepared[52] for the Defense Science Board: Road Side Improvised Explosive Device Attack describing the recovery and biometric exploitation of captured or found IED components and affiliated components.

Methodology:

The scenario is fact-based using a composite of actual events. Not all IED incidents provide the amount of recoverable items as the one described hence its illustrative nature. The scenario has been reviewed by the JIEDDO and TEDAC. Elements of the actions taken by the responders at the incident site have been omitted if they did not directly relate to the scenario's purpose. To keep the scenario at the FOUO level specific technical details of the exploitation process have been omitted. If desired a classified version can be prepared.

The Setting:

A combined patrol was traveling along a major road outside of Kirkuk when an IED detonated underneath a HUMVEE flipping it over and killing all the soldiers inside. It happened at 1415 hours and it was 100 degrees. The remainder of the patrol executed their IED incident battle drill; established a perimeter, halted traffic both ways, called for a MEDAVAC, a quick reaction force and EOD team to the battle Captain in the battalion tactical operations center. In addition the battle captain dispatched the Weapons Intelligence Team assigned to the BCT with the EOD team to assist in the exploitation of the site. While the on–site tactical commander was informing higher headquarters of the incident and requesting support, one of the patrol's soldiers spotted a military-aged male fleeing on motorcycle from a palm grove that overlooked the ambush site. One team from the patrol initiated a pursuit of the suspect but he evaded capture. The Iraqi was surprised by the quick unit response and he dropped a portable Motorola radio in his haste to escape.

The Tactical Response:

The quick reaction force with the explosive ordinance team and weapons intelligence team arrived. The EOD team commander quickly debriefed the on – site command on what occurred, determined the entry control point to begin his teams render safe procedure to ensure that that are had no more IEDs. The quick reaction force fanned out and expanded the perimeter. The WIT members began interview patrol unit members, began taking photographs of the area. As the EOD team expanded their search area they found the dropped PMR and recovered it. The EOD team member who recovered it checked for it being booby trapped not being aware that the insurgent had dropped it while fleeing the site. The EOD operator was forensically aware knowing that it may have latent finger prints on it. He left for the WIT to handle. No further IEDs were found and the EOD team cleared the WIT on to the site pointing out the PMR

---

[52] Russell L. McIntyre, SIO, DIA/DT, (703) 907-0265

 location and the IEDs firing pack that was covered with dirt and trash partially blown off by the IED's explosive force. The firing pack was checked by an EOD operator to ensure that it was not booby trapped. A WIT member photographs the firing pack *in–situ* then removes it using forensic gloves for recovery back to the forward operating base.

OBSERVATIONS: Actions taken to render safe by EOD and exploit an IED incident site need to be executed efficiently and quickly. Holding the outer perimeter secure and not providing insurgents a static target are two drivers that can result in on average a time on target of approximately 30 minutes. The EOD operators and the WIT members are forensically aware and trained in the proper handling of found or captured devices. What can happen is Soldiers or Marines in the impacted unit or as part of the quick reaction force find something, pick it up and then it gets passed up the entire on – site chain of command. This of course impacts negatively on the found items forensic – biometric value. Biometric awareness training is now a common skill needed for service members.

First Phase Exploitation (Tactical)

The recovered PMR and firing pack, note figure 2, have been cleared by the EOD team. Both items are photographed with any identifying serial numbers included in the reports prepared by the WIT and EOD team members. The battalion and brigade intelligence officers are briefed on the incident, how relates to the pattern of previous enemy activity and if anything outside was has been previously seen was noted. The PMR and firing pack are prepared for evacuation to the Explosive Ordinance Battalion (EOD) located at Camp Victory, Baghdad.

OBSERVATIONS: Tactical commanders desire the ability to biometrically exploit captured devices. Remove the latent prints, place them into a digital format having access to a data base to store the result and compare it against previously recovered prints. This goal presents several challenges. Detecting and removing latent prints from electronic components can damage the device to the extent that further media exploitation is impaired. Follow – on exploitation includes the devices electronic components or the discovery of latent DNA. The optimum location to begin the biometric recovery is where the devices value relative to the bigger IED picture is held, at the Combined Explosive Exploitation Cell (CEXC). The CEXC has the capability to meet both needs – electronic exploitation and biometric recovery can occur with minimum risk for compromising the value of each as well as retaining utility for third phase or forensic recovery at the Terrorism Explosive Device Analysis Center or TEDAC.

Second Phase Exploitation (Operational):

The CEXC has received both devices from the EOD Battalion for second phase exploitation. The second phase exploitation will consist of checking for latent prints on the exterior of the devices. If found they will be recovered and entered into the Biometric Automated Tracking System or BATs. Matches are reported to the appropriate entities to support follow – on operations. The wrapping of the firing pack is removed and retained for forwarding to TEDAC

for third phase exploitation. The interior of the device is examined and exploited by the members of the CEXC. Results of the exploitation are reported by the CEXC in a Quick Look Report and follow – on analysis fitting the recovered devices within an overall regional pattern determining if it is a new device requiring it to receive priority for technical exploitation with biometric recovery secondary.

OBSERVATIONS: The entire exploitation chain is under continual command pressure for more expeditious results that will match specific persons to specific locations and or events. The reality is that the introduction of greater collection capability for found or captured devices with the deployment of the WITs and soon Sensitive Site Exploitation Teams is not matched with an investment to process the volume at the operational and national levels.

Third Phase Exploitation (National):

The CEXC is central to the 2nd phase of the exploitation chain for IEDs and their affiliated and associated components routinely forwarding those items to the TEDAC which is co – located at the Federal Bureau of Investigation Crime Laboratory at Quantico, Virginia. The TEDAC represents the third phase of forensic and biometric exploitation. Although the focus of the paper is on biometrics, specifically latent prints, TEDAC is capable of and does the full range of forensic exploitation. The TEDAC examines and removes all latent prints from all of the forwarded components and their affiliated wrapping materials to include the interior of the devices. The TEDAC has representatives from the Bureau of Alcohol, Tobacco and Firearms (ATF) and the US Army's National Ground Intelligence Center (NGIC) who assist in the exploitation. The recovered prints are forwarded to the IAFIS and ABIS data bases. As with the rest of the biometric exploitation process the volume of device recovery compared to the number of skilled personnel available to recover and automate the results for later matching and analysis to support tactical executions results in time lags for exploitation. The point of this comprehensive and resource intensive exercise outlined in the scenario is to help find and positively identify specific members of insurgent and terrorist networks so that they can be targeted, captured and prosecuted.

Use of biometrics as a forensic element in the exploitation chain for captured IED components is a new activity for DoD, tactical commanders and their Soldiers and Marines. Practical education has not yet caught up with expectation for result. In the scenario presented only those forensically trained handled recovered devices. However another scenario often occurs in which several soldiers handle devices without forensic awareness training or proper gloves, evidence bags. The DVD titled "Biometrics: New Techniques to Fight the War on Terrorism presented the strategic need well however success with this forensic application begins at the tactical level with proper training and education for the first tactical responders.

As with any other application that has evidentiary value in a court of law its value, acceptance and standard of application have to be known before it enters said court. In a counterinsurgency operation sovereignty is ultimately shared with the supported country with the host's courts law where those involved in insurgent activities are tried. This is the case in Iraq. The identity system of Iraq, how it functioned, where it resided, who was in it and the standards by which that occurred was not known nor regarded as significant. Biometric data recovered from device, weapon, document or other circumstance needs to be handled and presented in such a way as to support to the identification and prosecution of suspected insurgents.

Appendix L — DHS: US-VISIT Passport Control, Border Management

US-VISIT is a system designed to keep persons out of the U.S. who are potential or known threats to our society, while facilitating the legitimate flow of people across our borders. US-VISIT maintains a database of fingerprints called IDENT. It contains fingerprints, photographs and biographical information on foreign persons entering the US through ports of entry, those apprehended by the Customs and Border Protection (including the Border Patrol) or Immigration and Customs Enforcement, persons deported from the US, persons who have applied for Border Crossing Cards in Mexico, persons who have applied for asylum, and lookout data. US-VISIT closely coordinates with other Government agencies, such as the Department of Justice to incorporate information on foreign-born individuals that are wanted for crimes or are suspected of terrorism. Information is also received from other reliable sources such as INTERPOL.

US-VISIT

At the time of visa application or application for a Border Crossing Card with the Department of State (DOS), the individual must provide a photograph and have a finger-scan taken. The finger data is sent to the US-VISIT database where it is checked to determine if there is any adverse information associated with that person or if that data is associated with another name. DOS runs photographic data against its database for persons exempt from the fingerprint requirement (such as diplomats) and has detected several cases of suspected fraud in that manner. The consular official can then make a decision about granting a visa to the applicant based on US-VISIT and DOS supplied information.

Upon arrival at a port of entry, the individual has finger scans and a photograph taken. The purpose is to verify that the person granted the visa is the person attempting to enter with that visa. For persons coming from visa-waiver nations, a record is created at the time of entry with the biographic and biometric information. A watch list check is performed for all of these people.

A record of exit is made using information received from transportation companies or from the individual directly. This is cross-checked against arrival information to verify that the person has not violated the terms of entry by overstaying.

Another aspect of US-VISIT is facilitation of travel for legitimate visitors. The International Registered Traveler Program is one example. In a test with the Netherlands, biometrics are used to allow pre-screened travelers to bypass normal inspection at a port of entry and use an automated kiosk. Biometric checks are performed (including watch list checks) prior to admitting the person.

Transportation Security Administration Biometrics Programs

The Transportation Security Administration (TSA) has several programs involving biometrics, such as the domestic Registered Traveler program. It is designed to allow low-risk individuals to bypass the long security inspection lines in airports and proceed through a biometrically-enabled

checkpoint. Another program is focused on verifying the identity of hazardous material truck drivers. Verifying that a person has the authority to enter a restricted area of an airport gave rise to a program designed to establish a biometrics qualified products list that airport authorities can rely upon to select devices that will meet TSA requirements. The Transportation Worker Identity Card (TWIC) is a major initiative that will allow workers to access different facilities with one identity document that may contain multiple biometrics and authorization levels for various locations. It is being designed to be conformant with the specifications of the PIV for Government workers and contractors accessing government facilities.

First Responders

The Federal Emergency Management Agency (FEMA) has started work on smart card identification for First Responders. The initial test area is the National Capital Region. In an emergency, there is a requirement to rapidly and correctly verify that a person has the authority to enter a restricted zone and the authority to perform certain functions (such as medical support). Biometrics is expected to play a major role in this program. The cards will be issued by local units (such as Fire Departments) conformant to FEMA requirements.

Other Border and Homeland Security Biometric Programs

Citizenship and Immigration Service's Business Transformation project that is designed to ensure that a person applying for a benefit (such as a change of immigration status) has only one identity in the system -- that is, hasn't applied under different names in different locations. Facial biometrics has, for instance, detected several cases of persons committing Marriage Fraud. Fingerprints have detected imposters appearing for interviews in asylum cases who have been trained on how to answer the questions.

The Coast Guard has initiated a project to examine the feasibility of Biometric Identification at Sea, with the initial focus on applying biometrics to alien migrant interdiction operations between the Dominican Republic and US territory.

Customs and Border Patrol (CBP) administers AirNexus, a joint program with Canada that relies upon iris recognition in kiosks at selected airport pre-inspection locations in Canada. The purpose is to allow pre-screened and low-risk travelers to bypass the long immigration inspection lines. Other facilitation programs involving biometrics checking at the time of enrollment include SENTRI and FAST. Fingerprint checks are performed on all applicants to determine eligibility for enrollment in the program.

International Access

The Department of Homeland Security (DHS) and INTERPOL exchange fingerprint data on internationally wanted criminals. DHS also shares lookout records on terrorists and major criminals, gang-related records (such as MS13) and deportee records with other countries. This information may be shared on a case-by-case basis with other countries *and agencies*, depending on agreements with the data provider. An example is working with the Government of El Salvador to exchange biometric information on persons involved in gang related activities.

CBP manages the Regional Movement Alert List (RMAL) RMAL enables remote checks of lost/stolen/invalid passport numbers and "positive validation" of passports/passport holders through international data-sharing. It is currently in the prototype stage with the US and Australia.

As part of the Visa Waiver Program, DHS validates the e-Passports of participating nations for compliance with the requirements of the program, including the storage of biometric data in accordance with the specifications of the International Civil Aviation Organization (ICAO). This program includes 27 nations. All of the VWP nations must have their e-Passports validated by DHS prior to October 26, 2006 in order to remain in the program. In addition, DHS has offered this capability to non-VWP nations as they develop e-Passports. Thailand and Russia have taken advantage of this to date, with other nations indicating that they will do so once their e-Passports are ready.

International Relationships

DHS is an active participant in the international standards arena in the areas of biometrics and travel documents, and participates in international standards development activities through ISO/IEC SC37 and ICAO.

DHS and international partners OECD and ICAO are working on the Enhanced International Travel Security (EITS) program. EITS seeks to develop mechanisms for real-time communications between distributed international data systems to validate travel documents and verify traveler identity. EITS could enable a border management agency of one government to send an automated request, which would include the traveler's photograph, biographic, and other information, to the issuing authority of another government regarding a particular travel document, and to receive an automated reply within several seconds. Current participants are the U.S., UK, and Australia.

DHS has established working relationships with the Governments of Australia and the United Kingdom to coordinate research activities in biometrics. US-VISIT has provided a staff member for on-site work with the UK government as they develop their e-borders program. DHS also works closely with the EU in the planning for their Visa Information System (VIS). This will involve the capture of biometric data from visa applicants to the EU. Each nation will maintain their own database, but they will be linked in a hub-and-spoke system so that when an application is received, the nation can verify with other EU and other Schengen-area nations (including Switzerland, Iceland, Norway and Liechtenstein) whether the person has previously applied for a visa with another nation and had the application denied. Similar efforts are in the planning stages with Japan.

DHS also works with nations to review their biometrics and identity management programs. A recent example is the seminar held with the Government of Indonesia on e-Passports and national ID.

Appendix M — Current Integrated Automated Fingerprint Identification System (IAFIS) Use Cases

Federal Agencies / Risk Assessment

A visa subject requests entry

A visa subject requests entry to the United States at a Port of Entry. All documentation appears to be in order. A fingerprint background check of IAFIS reveals that the subject has previously been ordered for deportation using another name. The subject is not granted entry to the United States.

An immigrant is applying for naturalization benefits

An immigrant is applying for naturalization benefits through the Department of Homeland Security's Citizenship and Immigration Services. A fingerprint check of IAFIS reveals the subject has a previous arrest using various other names and is currently wanted in California for homicide. The subject is not granted naturalization benefits. The local and the wanting law enforcement agencies coordinate apprehension, detention, and extradition of the subject.

A subject is applying for a position in a nuclear power facility

A subject is applying for a position in a nuclear power facility. The subject is fingerprinted as part of the pre-employment screening process. The fingerprint check of IAFIS reveals a previous arrest and that the subject is on a terrorist watch list under a different name. The subject is immediately detained.

Non-federal Agencies / Risk Assessment

A nursing applicant in an elder-care facility

A subject is applying for a nursing assistant position in a residential care facility for the elderly or disabled. The subject is fingerprinted as part of the pre-employment background check. A fingerprint check of IAFIS reveals the subject is wanted for a sex offense in another state and is a registered sex offender using a different name. The subject is disqualified for employment and the local law enforcement agency is notified regarding the location of the subject. The local and the wanting law enforcement agencies coordinate apprehension, detention, and extradition of the subject.

A would-be banker, required by law to undergo background check

Legislation requires all potential bankers to undergo a criminal history background check. The subject is fingerprinted as part of the pre-employment screening for a criminal history background check. The fingerprint check of IAFIS reveals that the subject had previously been arrested and convicted of larceny and embezzlement. The subject is disqualified for employment.

Federal Criminal Justice Agencies / Establish Identity

Otherwise unidentified victims of a natural disaster

A natural disaster occurs and many people in the United States are killed. Some of these individuals cannot be identified. The deceased individuals are fingerprinted. A fingerprint check of IAFIS reveals the identities of the individuals who have a previous criminal history or who have held a Federal position of trust (e.g. Federal government employee, military applicant, naturalized immigrant).

State or Local Criminal Justice Agencies / Establish Identity

A routine traffic stop

A state or local police officer makes a routine traffic stop. The officer suspects the driver's license information is fraudulent. The subject is detained. A fingerprint search of IAFIS reveals the subject is wanted under a different name for murder and was previously deported. The implication is that the subject may be in the country illegally and further investigation is warranted. The local and the wanting law enforcement agencies coordinate apprehension, detention, and extradition of the subject.

State, Local, or Federal Criminal Justice Agencies / Investigation

A latent fingerprint on a weapon

A crime laboratory submits latent fingerprint images, acquired from a weapon, to the IAFIS in order to assist in the investigation of an elderly woman's murder. A search of the system reveals several image candidates. Based on these candidates, the fingerprints are identified by a latent examiner as belonging to a subject with a previous criminal record in another state. Further investigation by detectives leads to the location and apprehension of the subject.

Captured irregular fighters

Armed plainclothes fighters attack a U.S. military squad while on patrol. After the initial skirmish, the fighters surrender their arms and are detained by U.S. military forces. A search of the subjects' possessions reveals falsified identification documents from Iraq, Afghanistan, and Pakistan.

Biometric samples are collected from each of the detainees and transmitted to the DoD Automated Biometric Identification System (ABIS). ABIS Automatically shares all of the biometric samples with the IAFIS. After analysis of available biometric and non-biometric information, the subjects are nominated and promoted by the National Counterterrorism Center (NCTC) as known or suspected terrorists (KST). The subjects' biometric files are flagged and linked to the NCTC terrorist watch list and entered into the FBI's KST File.

Several months later, the detainees are released to a foreign government for adjudication and repatriation.

Several years later, a U.S. police department responds to a trespassing complaint at a local water treatment plant. Two subjects are apprehended and fingerprints are taken at the police department's primary booking station. The fingerprints are transmitted to the FBI's fingerprint database and matches are made against the previously shared biometric samples from the military detainees. Since the fingerprints have been entered into the KST File, the FBI's CJIS Division Intelligence Group notifies the Terrorist Screening Center (TSC) of the encounter. As a result, the TSC notifies a Joint Terrorism Task Force to investigate whether the trespassing act was an indication of a terrorist threat to the nation.

Appendix N —Battlefield Capture of Sensitive Devices

As military high-tech devices work their way down through the echelons, the risk of an enemy capturing such a device on the battlefield increases. If the device were operable by the enemy, the effects might be consequential.

Biometrics might be one key to enhancing both mission/data security *and* functionality by incorporating a sort of "dead man's switch" into tactical/mobile command, communications and information-display systems. If the authorized operator was disabled, or the equipment was accessed when that person was not present, a security feature unique to the intended operator (e.g. PIN/password) might prevent sensitive information from being improperly accessed. If the security feature had a purely physical form (a key or access card), that object might be stolen or taken from the operator, leading to defeat of the security lockout. Use of a biometric adjunct to PIN, password and/or token would strengthen the assurance that the device could not be suborned…although some would note that this could put an authorized operator at greater physical risk, if captured.

It has been suggested that within the context of a broad privilege management regime, built on HSPD-12, it could be possible to dynamically control access to key data, equipment and even facilities, selectively enabling new operators, while "locking out" systems or operators which had been compromised.

Appendix O - Biometric Modalities Matrix[53]

COMPLETE MODALITIES MATRIX LOCATED AT

http://www.acq.osd.mil/dsb/reports/2007-03-Defense_Biometrics_Program.xls

---

[53] This chart represents the biometric modalities deemed to be of greatest relevance and incidence today; as such, it is not an all-inclusive list. Values assigned for the various qualities are subjective judgments, based on expert opinion and review of (several) current published sources.

Appendix P — Glossary of Terms

[Where appropriate, the usage and definition of terms corresponds to those developed by the NSTC Subcommittee on Biometrics and their glossary can be found at www.biometrics.gov/]

A

ANSI - American National Standards Institute

A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

Application Programming Interface (API)

Formatting instructions or tools used by an application developer to link and build hardware or software applications.

Accuracy

A catch-all phrase for describing how well a biometric system performs. The actual statistic for performance will vary by task (verification, open-set identification, watchlist, and closed-set identification). *See also d prime, detection error trade-off (DET), detect and identification rate, equal error rate, false acceptance rate (FAR), false alarm rate (FAR), false match rate, false non-match rate, false reject rate, identification rate, performance, verification rate.*

Algorithm

A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc.

Assertion (of an identity)

The process of claiming an identity in order to claim a privilege previously established for that identity.

Attempt

The submission of a biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual. *See also biometric sample, identification, verification.*

Authentication

1. The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: "This individual's name is 'Joseph K.' " or "This child is more than 5 feet tall."
2. A security service provided by an information processing system, which can provide for: initial one-way authentication, *i.e.,* identifying a principal at the beginning of a session; two-way authentication, *i.e.,* identifying the entity at each end, *e.g.*, client v. server; continuous authentication, *i.e.*, maintaining the binding between session traffic and the identities authenticated during session initiation.
3. In biometrics, "authentication" is sometimes used as a generic synonym for verification. *See also <u>verification.</u>*

Automated Biometric Identification System (ABIS)

1. Department of Defense (DoD) system implemented to improve the U.S. government's ability to track and identify national security threats. The system includes mandatory collection of ten rolled fingerprints, a minimum of five mug shots from varying angles, and an oral swab to collect DNA.
2. Generic term sometimes used in the biometrics community to discuss a biometric system. *See also AFIS.*

Automated Fingerprint Identification System (AFIS)

A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc). *See also IAFIS.*

<u>B</u>

Behavioral Biometric Characteristic

A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics. *See also <u>biological biometric characteristic.</u>*

Benchmarking

The process of comparing measured performance against a standard, openly available, reference.

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges. *See also friction ridge, minutia(e) point , ridge ending.*

Binning

Process of parsing (examining) or classifying data in order to accelerate and/or improve biometric matching.

BioAPI – Biometrics Application Programming Interface

Defines the application programming interface and service provider interface for a standard biometric technology interface. The BioAPI enables biometric devices to be easily installed, integrated or swapped within the overall system architecture.

Biological Biometric Characteristic

A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than an acquired behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry. *See also behavioral biometric characteristic.*

Biometrics

A general term used alternatively to describe a characteristic or a process.

As a characteristic:

A measurable biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition.

As a process:

Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric Consortium (BC)

An open forum to share information throughout government, industry, and academia. For more information visit www.biometrics.org.

Biometric Data

A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to collateral identity information such as user name, demographic information and authorizations.

Biometric Sample

Information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.

Biometric System

Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of:

1. Capturing a biometric sample from an end user
2. Extracting and processing the biometric data from that sample
3. Storing the extracted information in a database
4. Comparing the biometric data with data contained in one or more reference references
5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved.

A biometric system may be a component of a larger system.

Breeder Documents

Documents (*e.g.,* driver's licenses) that can be used to gain access to an individual's personal or financial information; *de facto*, reasonably universal tokens. *See also <u>foundational documents.</u>*

<u>C</u>

Capture

The process of collecting a biometric sample from an individual via a sensor. *See also <u>submission.</u>*

CBEFF - Common Biometric Exchange File Format

A standard that provides the ability for a system to identify, and interface with, multiple biometric systems, and to exchange data between system components.

Challenge Response

A method used to confirm the presence of a person by eliciting direct responses from the individual. Responses can be either voluntary or involuntary. In a voluntary response, the end user will consciously react to something that the system presents. In an involuntary response, the end user's body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks. *See also liveness detection.*

CHUID

Card Holder Unique IDentifier

CJIS

The FBI's Criminal Justice Information Services Division, which operates IAFIS, the Integrated Automated Fingerprint Identification System (IAFIS).

Claim of identity

A statement that a person is or is not the source of a reference in a database. Claims can be positive (I am in the database), negative (I am not in the database) or specific (I am end user 123 in the database).

Closed-set Identification

A biometric task where an unidentified individual is known to be in the database and the system attempts to determine his/her identity. Performance is measured by the frequency with which the individual appears in the system's top rank (or top 5, 10, etc.). *See also identification, open-set identification.*

Collateral Identity Information

The information other than biometrics that is associated with the identity fixed by the biometric—*e.g.*, name, rank and serial number, date and place of birth …

Comparison

Process of comparing a biometric sample with a previously stored reference or references in order to make an identification or verification decision. *See also match.*

Cooperative User

An individual that willingly provides his/her biometric to the biometric system for capture. An individual who wishes to assert an identity. Example: A worker submits his/her biometric to clock in and out of work. *See also indifferent user, non-cooperative user, and uncooperative user.*

Core Point

The "center(s)" of a fingerprint. In a whorl pattern, the core point is found in the middle of the spiral/circles. In a loop pattern, the core point is found in the top region of the innermost loop. More technically, a core point is defined as the topmost point on the innermost upwardly curving friction ridgeline. A fingerprint may have multiple cores or no cores. *See also arch, delta point, friction ridge, loop, whorl.*

Covert (biometric collection)

Collection of a biometric without the knowledge of an individual. An instance in which biometric samples are being collected at a place and/or time that is not known to bystanders. An example of a covert environment might involve an airport checkpoint where facial images of passengers are captured and compared to a watchlist without their knowledge. *See also non-cooperative user, overt.*

Crossover Error Rate (CER)

See equal error rate (EER).

Cumulative Match Characteristic (CMC)

A method of showing measured accuracy performance of a biometric system operating in the closed-set identification task. Templates are compared and ranked based on their similarity.

The CMC shows how often the individual's template appears in the ranks (1, 5, 10, 100, etc.), based on the match rate. A CMC compares the rank (1, 5, 10, 100, etc.) versus identification rate.

D

D-Prime (D′)

A statistical measure of how well a system can discriminate between a signal and a non-signal. [The distance measured in standard deviation units between two probability density functions usually representing two hypotheses, *e.g.*, signal or noise.]

Database

Organized information - a collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, and/or collateral identity information (aka: related end user information). *See also gallery.*

Decision

The resultant action taken (either automated or manual) based on a comparison of a similarity score (or similar measure) and the system's threshold. *See also underline comparison, similarity score, threshold.*

Degrees of Freedom

A statistical measure of how unique biometric data is.

Technically, it is the number of statistically independent features (parameters) contained in biometric data.

Delta Point

Part of a fingerprint pattern that looks similar to the Greek letter delta (),. Technically, it is the point on a friction ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence. *See also core point, friction ridge.*

Detection and Identification Rate

The rate at which individuals, who are in a database, are properly identified in an open-set identification (watchlist) application. *See also open-set identification, watchlist.*

Detection Error Trade-off (DET) Curve

A graphical plot of measured error rates. DET curves typically plot matching error rates (false non-match rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate). *See also Receiver Operating Characteristic.*

Difference Score

A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference. *See also hamming distance, similarity score.*

Digital Identity

An expression of one's identity suitable for computer-mediated transactions, on-line transactions, or transmission/certification of identity over modern communications networks.

E

Eavesdropping

Surreptitiously obtaining data from an unknowing end user who is performing a legitimate function. An example involves having a hidden sensor co-located with the legitimate sensor. *See also* *skimming.*

EFCON - Electronic Fingerprint Conversion

Electronic Fingerprint Converter; IAFIS "front-end" that checks submissions to ensure compliance with the IAFIS specifications outlined in the FBI Electronic Biometric Transmission Specification.

EFTS - Electronic Fingerprint Transmission Specification

A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS). This specification facilitates information sharing and eliminates the delays associated with fingerprint cards. *See also* *Integrated Automated Fingerprint Identification System (IAFIS).*

Encryption

The act of transforming data into an unintelligible form so that it cannot be read by unauthorized individuals. A key or a password is used to decrypt (decode) the encrypted data.

End User

The individual who will interact with the system to enroll, to verify, or to identify. *See also* *cooperative user, indifferent user, non-cooperative user, uncooperative user, user.*

Enrollment (Enrolment)

The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Equal Error Rate (EER)

A statistic used to show biometric performance, typically when operating in the verification task. The EER is the location on a ROC or DET curve where the false accept rate and false reject rate (or one minus the verification rate {1 -VR}) are equal.. In general, the lower the equal error rate value, the higher the accuracy of the biometric system. Note, however, that most operational systems are not set to operate at the "equal error rate" so the measure's true usefulness is limited to comparing biometric system performance. The EER is sometimes referred to as the "Crossover Error Rate." *See also Detection Error Trade-off (DET) curve, false accept rate, false reject rate, Receiver Operating Characteristics (ROC).*

Executive Agent

The DoD Executive Agent, per DoD Directive 5101.1, shall:
1. Execute DoD Executive Agent responsibilities, consistent with applicable law, DoD Directive 5100.3 (reference (d)), DoD Directive 5100.73 (reference (e)), and this Directive.
2. Ensure proper coordination with the DoD Components for the responsibilities and activities assigned to provide continuous, sustainable, and global support as required by end users. Ensure effective planning throughout operations by developing a coordinated process and support plans for transition from peacetime to wartime and/or contingency operations.
3. Identify requirements and resources, including force structure to the extent permitted by law, necessary to execute assigned responsibilities and functions. Submit these requirements to the cognizant Head of the DoD Component to be included in their respective budget documentation.
4. Monitor resources used in performing assigned responsibilities and functions.
5. Develop, maintain, and report results of performance of DoD Executive Agent responsibilities and functions, as may be required by law, Secretary of Defense decision, or other Congressional requirements.
6. Obtain reports and information, consistent with DoD Directive 8910.1 (reference (f)), as necessary, to carry out assigned DoD Executive Agent responsibilities, functions, and authorities.
7. Establish, maintain, and preserve information as records, consistent with DoD Directive 5015.2 (reference (g)), that document the transaction of business and mission of the DoD Executive Agent.
8. Designate a focal point to coordinate matters regarding assigned DoD Executive Agent responsibilities, functions, and authorities.

Extraction

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference. *See also biometric sample, feature, template.*

<u>F</u>

Face Recognition

A biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

Failure to Acquire (FTA)

Failure of a biometric system to capture and/or extract usable information from a biometric sample.

Failure to Enroll (FTE)

Failure of a biometric system to form a proper enrollment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

False Acceptance Rate (FAR)

A statistic used to measure biometric performance when operating in the verification task: the probability that a system will fail to identify a registered user; the percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim. *See also <u>false match rate,</u> <u>type II error.</u>*

False Alarm Rate

A statistic used to measure biometric performance when operating in the open-set identification (sometimes referred to as watchlist) task. This is the percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank isn't in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

False Non-Match Rate

A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not.

False Rejection Rate (FRR)

A statistic used to measure biometric performance when operating in the verification task: the probability that a system will incorrectly identify an individual or fail to reject an impostor; the percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim. *See also false non-match rate, type I error.*

Feature(s)

Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference. *See also extraction, template.*

Feature Extraction

See extraction.

FERET - FacE REcognition Technology program

A face recognition development and evaluation program sponsored by the U.S. Government from 1993 through 1997. For more information visit http: / /www.frvt.org/ FERET/default.htm. *See also FRGC, FRVT.*

Fingerprint Recognition

A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings. *See also bifurcation, core point, delta point, minutia(e) point.*

Foundational Documents

Foundational documents allow the government and other organizations to issue other identity documents—*e.g.*, birth or baptismal certificate. *See also breeder documents.*

FpVTE - Fingerprint Vendor Technology Evaluation (2003)

An independently administered technology evaluation of commercial fingerprint matching algorithms. For more information visit http://fpvte.nist.gov/.

FRGC - Face Recognition Grand Challenge

A face recognition development program sponsored by the U.S. Government from 2003-2005. For more information visit http://www.frvt.org/FRGC/. *See also FERET, FRVT.*

Friction Ridge

The ridges present on the skin of the fingers and toes, and on the palms and soles of the feet, which make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints. *See also <u>minutia(e) point.</u>*

FRVT - Face Recognition Vendor Test

A series of large-scale independent technology evaluations of face recognition systems. The evaluations have occurred in 2000, 2002, and 2005. For more information visit <u>http: / /www.frvt.org/</u> FRVT2005 /default.aspx. *See also <u>FRGC,</u> <u>FERET.</u>*

<u>G</u>

Gallery

The biometric system's database, or set of known individuals, for a specific implementation or evaluation experiment. *See also <u>database, probe.</u>*

Gait

An individual's manner of walking. This behavioral characteristic is in the research and development stage of automation.

<u>H</u>

Hamming Distance

The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms. *See also <u>difference</u> score, <u>similarity score.</u>*

Hand Geometry Recognition

A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

<u>I</u>

ICE - Iris Challenge Evaluation

A large-scale development and independent technology evaluation activity for iris recognition systems sponsored by the U.S. Government in 2005.. For more information visit <u>http: //iris.nist.gov/ICE/.</u>

Identification/One-to-many

A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity. *See also <u>closed-set identification,</u> <u>open-set identification,</u> <u>verification,</u> <u>watchlist.</u>*

Identification Rate

The rate at which an individual in a database is correctly identified.

Identity Management

The combination of systems, rules and procedures that defines an agreement between an individual and organization(s) regarding ownership, utilization and safeguard of personal identity information, and all the collateral information, explicit and inferable associated with that identity. (The TF notes that the true and full scope of IM, and thus its crisp definition, remain a matter of discussion within the community of practitioners. Our central insight is that the DoD has much at stake in the outcome of such debate, and must engage in it, thoughtfully and broadly).

Identity Theft

An individual's fraudulent claim that he or she is the person to whom the information in the system refers, allowing him or her to derive some benefit from another party who is relying on that claim.

Identity theft encompasses a myriad of criminal activities including "true name" fraud, account takeover, and fraudulent applications fraud. "True name" identity theft involves acquiring a person's identity to establish new financial accounts or loans, obtain employment, create fraudulent identification, or to commit other crimes. Account takeover identity theft refers to the acquisition of a person's existing credit card or bank account or an existing non-credit card account. Fraudulent application fraud occurs when a criminal uses an identity other then his/her own to apply for credit or services.

Identity Theft Assumption and Deterrence Act, as amended, defines identity theft as the knowing transfer or use, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[54]

---

[54] 18 U.S.C. 1029(e)(1)

Impostor

A person who submits a biometric sample in either an intentional or inadvertent attempt to claim the identity of another person to a biometric system. *See also <u>attempt.</u>*

INCITS - International Committee for Information Technology Standards

Organization that promotes the effective use of information and communication technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations. For more information visit <u>http://www.INCITS.org/.</u> *See also ANSI, ISO, NIST.*

Indifferent User

An individual who knows his/her biometric sample is being collected and does not attempt to help or hinder the collection of the sample. For example, an individual, aware that a camera is being used for face recognition, looks in the general direction of the sensor, neither avoiding nor directly looking at it. *See also <u>cooperative user,</u> <u>non-cooperative user,</u> <u>uncooperative user.</u>*

Infrared

Light that lies outside the human visible spectrum at its red (low frequency) end.

Integrated Automated Fingerprint Identification System (IAFIS)

The Criminal Justice Information Services (CJIS) Division System of Services (SoS), located in Clarksburg, West Virginia, includes the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Instant Criminal Background Check System (NICS). IAFIS provides an up-to-date, integrated system to respond to the needs of the FBI and the law enforcement community. It houses the largest collection of digital representations of fingerprint images, features from the digital fingerprint images, and criminal history information in the world. Collectively, these data comprise the biometrics, content, format, and units of measurement for the electronic exchange of information that may be used in the fingerprint identification of a subject. The current IAFIS, implemented in July 1999, allows the standard electronic submission of fingerprint identification data to the FBI. *See also AFIS.*

Integration, Tasking and Networking (ITN)

Integration, Tasking and Networking; one of five IAFIS segments that provides workflow management of ten-print, document, and latent print processing, as well as storage and retrieval of fingerprint images; maintains FIMF and provides connectivity among all IAFIS segments, as well as the front-end communications between the IAFIS and LE community who make electronic submissions and requests.

Interstate Identification Index (III)

A national network for the exchange of criminal history records. It includes elements of participating state systems, the NCIC System, the Nlets, and other systems.

Iris Recognition

A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes. The iris muscle is the colored portion of the eye surrounding the pupil.

IrisCode©

A biometric feature format used in the Daugman iris recognition system.

ISO - International Organization for Standardization

A non-governmental network of the national standards institutes from 151 countries. The ISO acts as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users. For more information visit http://www.iso.org. *See also ANSI, INCITS, NIST.*

J

K

Keystroke Dynamics

A biometric modality that uses the cadence of an individual's typing pattern for recognition.

L

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger. *See also friction ridge.*

Live Capture

Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface). *See also sensor.*

Liveness Detection

Ensures only characteristics from a living person can be stored, read or used; a technique used to ensure that the biometric sample submitted is from a living end user. A liveness detection method can help protect the system against some types of spoofing attacks. *See also challenge response, mimic, spoofing.*

Loop

A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered. This pattern will contain one core and one delta. *See also arch, core point, delta point, friction ridge, whorl.*

M

Match

A decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (difference or hamming distance). *See also false match rate, false non-match rate.*

Matching

The process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold. *See also comparison, difference score, threshold.*

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter. *See also challenge response, liveness detection, spoofing.*

Minutia(e) Point

Friction ridge characteristics that are used to individualize a fingerprint image, see illustration below. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes. *See also friction ridge, ridge ending.*

Modality

A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

Model

A representation used to characterize an individual. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates. *See also "template".*

Multimodal Biometric System

A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple; a system that uses two or more biometric characteristics or sensor types. Some systems identify subjects by comparing multiple files Fingers can be scanned individually or together as 'slaps'.

Multi-Factor Authentication

Use of two or more authentication techniques - passwords or PINs, smart-cards or other tokens, and biometrics - to perform user authentication.

N

Neural Net/Neural Network

A type of algorithm that learns from past experience to make decisions. *See also algorithm.*

NIST - National Institute of Standards and Technology

A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's measurement and standards work promotes the well-being of the nation and helps improve, among many others things, the nation's homeland security. For more information visit http://www.nist.gov/. *See also ANSI, INCITS, ISO.*

Noise

Unwanted components in a signal that degrade the quality of data or interfere with the desired signals processed by a system.

Non-cooperative User

An individual who is not aware that his/her biometric sample is being collected. Example: A traveler passing through a security line at an airport is unaware that a camera is capturing his/her face image. *See also cooperative user, indifferent user, uncooperative user.*

NSTC

The National Science and Technology Council (NSTC), established by [Executive Order](#) on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

O

One-to-many

A phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. Sample is compared to all biometric data saved in a system. It seeks to find an identity, rather than verify a claimed one. The phrase typically refers to the identification or watchlist tasks.

One-to-one

A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one) and the identification task can be accomplished by a series of one-to-one comparisons.

Open-set Identification

Biometric task that more closely follows operational biometric system conditions to 1) determine if someone is in a database and 2) find the record of the individual in the database. This is sometimes referred to as the "watchlist" task to differentiate it from the more commonly referenced closed-set identification. *See also closed-set identification, identification.*

Operational Evaluation

One of the three types of performance evaluations. The primary goal of an operational evaluation is to determine the workflow impact seen by the addition of a biometric system. *See also technology evaluation, scenario evaluation.*

Overt

Biometric sample collection where end users know they are being collected and at what location. An example of an overt environment is the US-VISIT program where non-U.S. citizens entering the United States submit their fingerprint data. *See also covert.*

P

Palm Print Recognition

A biometric modality that uses the physical structure of an individual's palm print for recognition purposes.

Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system. *See also accuracy, crossover error rate, cumulative match characteristics, d-prime, detection error trade-off, equal error rate, false accept rate, false alarm rate, false match rate, false reject rate, identification rate, operational evaluation, receiver operating characteristics, scenario evaluation, technology evaluation, true accept rate, true reject rate, verification rate.*

PIN - Personal Identification Number

A security method used to show "what you know." Depending on the system, a PIN could be used to either claim or verify a claimed identity.

Pixel

A picture element. This is the smallest element of a display that can be assigned a color value. *See also pixels per inch (PPI), resolution.*

Pixels Per Inch (PPI)

A measure of the resolution of a digital image. The higher the PPI, the more information is included in the image, and the larger the file size. *See also pixel, resolution.*

Population

The set of potential end users for an application.

Private Management

All management processes related to the application of an established identity in a specific context, for the purpose of achieving some access, benefit or other purpose. These processes include, inter alia, privilege granting, alteration and revocation; transaction auditing; and cross-organizational mapping of identities and associated roles with an identity universe (e.g. the US federal government), and/or across universes (e.g. government-civil relationships).

Probe

The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery. *See also gallery.*

PSA

OSD Principal Staff Assistant (PSA) reports directly to the Secretary of Defense, to promulgate DoD policy in DoD Instructions within the responsibilities, functions, and authorities assigned. The OSD Principal Staff Assistant, per DoD Directive 5101.1, shall:

1. Oversee the activities of DoD Executive Agents in their functional areas of responsibility.
2. Assess periodically, but not less than every three years, DoD Executive Agent assignments and arrangements associated with such assignments, under their cognizance for continued need, currency, and effectiveness and efficiency in satisfying end user requirements. Recommend establishment, continuation, modification, or cancellation of those DoD Executive Agent assignments and arrangements associated with such assignments, under their cognizance, as appropriate.
3. Designate a focal point to implement the guidance contained in this Directive and to coordinate matters regarding identification, control, and evaluation of the DoD Executive Agent assignments and arrangements associated with such assignments within their area of cognizance.

Q

R

Radio Frequency Identification (RFID)

Technology that uses low-powered radio transmitters to read data stored in a transponder (tag). RFID tags can be used to track assets, manage inventory, authorize payments, and serve as electronic keys. RFID is not a biometric.

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC compares false accept rate vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

Recognition

A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply the verification, closed-set identification or open-set identification (watchlist).

Record

The template and other information about the end user (e.g. name, access permissions).

Reference

The biometric data stored for an individual for use in future recognition. A reference can be one or more templates, models or raw images. *See also <u>template.</u>*

Resolution

The number of pixels per unit distance in the image. Describes the sharpness and clarity of an image. *See also <u>pixel , pixels per inch (PPI).</u>*

Ridge Ending

A minutiae point at the ending of a friction ridge. *See also <u>bifurcation, friction ridge.</u>*

Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor.

Root Identity

The "authoritative" identity established and maintained with high integrity by the system—the identity which points to, and is pointed to from, all related information in the system—generally thought to be established adequately only by the use of biometrics.

<u>S</u>

Scenario Evaluation

One of the three types of performance evaluations. The primary goal of a scenario evaluation is to measure performance of a biometric system operating in a specific application. *See also <u>technology evaluation, operational evaluation.</u>*

<u>Sclera</u>

The opaque (usually white), fibrous, protective layer of the eye containing collagen and elastic fibers. In biometrics terms, the pattern of blood vessels traversing this space is currently being explored as a potential biometric modality.

Security Services

In an information processing system, the system-provided functionality that assures confidentiality, access control, integrity, non-repudiation, and authentication.

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression.

Sensor

Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.

Sensor Aging

The gradual degradation in performance of a sensor over time.

Signature Dynamics

A behavioral biometric modality that analyzes dynamic characteristics of an individual's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Similarity Score

A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference. *See also difference score, hamming distance.*

Skimming

The act of obtaining data from an unknowing end user who is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus. *See also eavesdropping.*

Slaps/Slap Fingerprint

Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card. Slaps are known as "four finger simultaneous plain impressions."

Speaker Recognition

A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said, and is not a biometric technology. *See also speech recognition, voice recognition.*

Speaker Recognition Evaluations

An ongoing series of evaluations of speaker recognition systems. For more information, visit http://www.nist.gov/speech/tests/spk/index.htm

Speech Recognition

A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology. *See also speaker recognition, voice recognition.*

Spoofing

The ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database. *See also liveness detection, mimic.*

Submission

The process whereby an end user provides a biometric sample to a biometric system. *See also capture.*

T

Technology Evaluation

One of the three types of performance evaluations. The primary goal of a technology evaluation is to measure performance of biometric systems, typically only the recognition algorithm component, in general tasks. *See also operational evaluation, scenario evaluation.*

Template

A digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model.*

Threat

An intentional or unintentional potential event that could compromise the security and integrity of the system. *See also <u>vulnerability.</u>*

Threshold

A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application. *See also <u>comparison,</u> <u>match,</u> <u>matching.</u>*

Throughput Rate

The number of biometric transactions that a biometric system processes within a stated time interval.

Token

A physical object that indicates the identity of its owner. For example, a smart card.

True Accept Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

True Reject Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

Type I Error

An error that occurs in a statistical test when a true claim is (incorrectly) rejected. For example, John claims to be John, but the system incorrectly denies the claim. *See also <u>false reject</u> <u>rate</u> <u>(FRR).</u>*

Type II Error

An error that occurs in a statistical test when a false claim is (incorrectly) not rejected. For example: Frank claims to be John and the system verifies the claim. *See also <u>false accept rate</u> <u>(FAR).</u>*

U

Uncooperative User

An individual who actively tries to deny the capture of his/her biometric data. Example: A detainee mutilates his/her finger upon capture to prevent the recognition of his/her identity via fingerprint. *See also cooperative user, indifferent user, non-cooperative user.*

User

A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. *See also cooperative user, end user, indifferent user, non-cooperative user, uncooperative user.*

US-VISIT - U.S. Visitor and Immigrant Status Indicator Technology

A continuum of security measures that begins overseas, at the Department of State's visa issuing posts, and continues through arrival and departure from the United States of America. Using biometric, such as digital, inkless fingerscans and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the U.S. border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the U.S. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a know security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry and exit procedures address the U.S. critical need for tighter security and ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

V

Verification

A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. *See also identification, watchlist.*

Verification Rate

A statistic used to measure biometric performance when operating in the verification task. The rate at which legitimate end-users are correctly verified.

Voice Recognition

See speaker recognition.

Vulnerability

The potential for the function of a biometric system to be compromised by intent (fraudulent activity); design flaw (including usage error); accident; hardware failure; or external environmental condition. *See also threat.*

W

Watchlist

A term sometimes referred to as open-set identification that describes one of the three tasks that biometric systems perform. Answers the questions: Is this person in the database? If so, who are they? The biometric system determines if the individual's biometric template matches a biometric template of someone on the watchlist. The individual does not make an identity claim, and in some cases does not personally interact with the system whatsoever. *See also closed-set identification, identification, open-set identification, verification.*

Wavelet Scalar Quantization (WSQ)

An FBI-specified compression standard algorithm that is used for the exchange of fingerprints within the criminal justice community. It is used to reduce the data size of images.

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas. *See also arch, delta point, loop, minutia(e) point.*

X Y Z