



BIOMETRICS
DEPARTMENT OF DEFENSE

**WHAT DOD THINKS OF BIOMETRICS:
EXCERPTS FROM INTERVIEWS CONDUCTED FOR THE
DEPARTMENT OF DEFENSE
BIOMETRICS MANAGEMENT OFFICE
JANUARY – JUNE 2003**

**John D. Woodward, Jr.
Director
Department of Defense
Biometrics Management Office
June 2004**

**Department of Defense
Biometrics Management Office
Biometrics Fusion Center
www.biometrics.dod.mil
☎ (703) 602-5427**

INTRODUCTION

As part of its educational mission, DoD Biometrics is pleased to publish *What DoD Thinks of Biometrics*, which contains excerpts from interviews conducted with members of the Department of Defense community discussing biometric technologies and how they can be used by DoD components.

In reviewing the biometric literature, one is struck by the limited amount of information describing how potential implementers and users perceive the technology. This lack of information exists particularly with respect to the national security community. In light of this situation, DoD Biometrics hopes that this document will contribute to the DoD community's, and the general public's, understanding of biometrics.

By way of background, on November 27, 2002, the Deputy Secretary of Defense announced a biometrics survey to be conducted by the DoD Biometrics Management Office and the RAND Corporation Arroyo Center, the Army's only federally funded research & development center. The survey elicited information about current and future biometric usage and applicability to the various mission areas of DoD. Between January and June 2003, the survey team conducted more than 54 interviews with a broad range of participants across the United States and at U.S. military installations overseas. Interviewees included current and former political appointees, Senior Executive Service (SES) and General Officers, senior level (GS-15/O-6) and mid level (GS-14/O-5 and below) DoD employees, representatives from the Federal Bureau of Investigation (FBI) and the National Institute of Standards & Technology (NIST), as well as academic experts.

This publication includes selected excerpts from 13 interviews. While the chosen interviews are not statistically representative of the views of the DoD community, the selected excerpts provide interesting, informative, and insightful comments on biometrics.

Each excerpt has been redacted to protect the anonymity of the interviewee, as many interviewees provided their personal opinions regarding biometrics, and were not speaking officially for their offices or organizations. The source descriptions provide a general portrayal of each individual's responsibilities, background, and subject matter expertise. In the course of the biometrics survey, interviewees repeatedly raised several broad topics, and the comments have been divided along those lines into four main categories: Access Control, Tactical Applications for Biometrics, Identity Authentication, and General Comments.

ABOUT DOD BIOMETRICS

Department of Defense Biometrics consists of the Biometrics Management Office (BMO) and its subordinate unit, the Biometrics Fusion Center (BFC). The BMO is responsible for leading, consolidating, and coordinating the development, adoption, and use of biometric technologies for the Combatant Commands, Services, and Agencies. The mission focus is to support the warfighter and enhance Joint Service interoperability. The BMO reports to the Army Chief Information Officer who acts on behalf of the DoD Executive Agent for Biometrics, the Secretary of the Army. The BFC serves as a technical center to support DoD use of biometrics. The Assistant Secretary of Defense, Networks & Information Integration (ASD (NII)), is the DoD functional proponent for biometrics. The recently formed Identity Protection and Management Senior Coordinating Group provides senior-level, DoD-wide strategic guidance to the BMO, given its mission to oversee efforts in the areas of Biometrics, Public Key Infrastructure, and Smart Cards. For more information about DoD Biometrics, please visit www.biometrics.dod.mil.

TABLE OF CONTENTS

INTRODUCTION	i
ABOUT DOD BIOMETRICS	ii
TABLE OF CONTENTS	iii
ACCESS CONTROL	1
PHYSICAL ACCESS	1
Manpower Savings.....	1
Smart Gate	1
Throughput.....	2
Security Clearances.....	2
Contractors Accessing U.S. Installations.....	3
Foreign Visitors to DoD Research Facilities	3
LOGICAL ACCESS	5
Biometrics and Digital Signatures	5
Performance Issues	5
Computer Access	5
Biometrics as a “Core Technology” for Information Assurance	6
Defense in Depth: A New Paradigm.....	6
Biometrics & the Trusted Personnel Identification Service	7
Tracking and Auditing	8
Public Key Infrastructure v. Biometrics	8
Password Replacement?.....	8
TACTICAL APPLICATIONS FOR BIOMETRICS	9
Verification of Trusted Agents	9
Casualty Identification Assistance.....	10
Tactical Battlefield: Need for Continuous Verification.....	10
Continuous Verification System Requirements.....	11
High Assurance Application.....	12
Positive Identification as a Means of Control.....	12
Positive Identification for Force Protection.....	12

IDENTITY AUTHENTICATION	13
DEPARTMENT OF DEFENSE “CIVIL FILES”	13
Background	13
1:N Search Capability—Fixing Identity	14
Electronic Tracking.....	14
Leveraging the FBI’s IAFIS	14
Other Considerations	15
“Red Force” and Watchlists.....	15
Use by Law Enforcement.....	15
Casualty Identification	15
Counterintelligence and Counterterrorist Investigations	16
Discharged Service Members	16
Privacy Concerns	17
PRISON MANAGEMENT	18
Identification and Authentication of Prisoners	18
Identification and Tracking of Inmate Visitors.....	18
Identification and Tracking of Prison Staff	18
GENERAL COMMENTS ON BIOMETRIC USAGE	19
Technology Appropriateness	19
Necessary Levels of Surety.....	19
Enrollment.....	19
Defining the Mission for the Technology	19
Scaled Development	20
Number of Records	20
Mission Creep and Data Vulnerability	20

ACCESS CONTROL

Interviewees expressed greatest interest in using biometric technologies for physical and logical access control. Physical access control is the process of granting access, or entry, to a building or controlled space to authorized individuals only. Traditional physical access control methods involve human guards, manned checkpoints, and/or the use of personal identification numbers (PINs), passwords, cards, badges, keys, or tokens. These methods are susceptible to compromise, loss, theft, and forgetfulness.

Logical access control is the process of granting access to information, computers, and networks. Authorized users need to be able to properly access and share information, and unauthorized users need to be prevented from accessing the information. Computer and network access traditionally require usernames and passwords. Problems can arise when people forget their passwords, write down passwords where others can find them, or choose easy to remember passwords that are easy to guess.

PHYSICAL ACCESS

Source: A senior-level DoD official with responsibility for physical security who is familiar with biometric technologies.

The interviewee expects that biometrics will be integral to his mission in the future. He views biometrics as a *capability* to improve current access control methods. “We are going to have to have biometrics. Biometrics gives you that third level you need with *what you have, what you know, and what you are.*” He views physical access control as the most promising use for biometrics. He has a pressing need for a reliable technology to improve the current access control methods and enhance force protection measures throughout DoD.

Currently, “the man at the gate” who physically inspects photo identification largely fulfills this role. “Experience tells us that an individual looking at a card is not reliable... We need the technology to do the work for us.” Throughput is a significant priority with any technology application he elects to use because of the requirement to rapidly verify the identity of persons entering installations and facilities.

Manpower Savings

“Biometrics is being looked at as one of the enabling technologies.” Relying on the technology will allow DoD to reduce manpower by using biometrics with unmanned systems. Automating access control points frees up resources and allows that manpower to be employed elsewhere.

Smart Gate

The interviewee identified smart gates, which “let the good guys in,” as one of the best future applications for biometrics. He would like to facilitate access control through a combination of biometrics, smart gates, and proximity technologies. “If I tell you 100

feet before I get to the gate that I am coming in, you bring up my record [in the database].” This method should require a 1:1 match to ensure processing a fast pass through. The interviewee expressed a critical need for developing the technologies for smart gates.

Source: A former senior program director at a U.S. military research facility who is a biometric subject matter expert.

The interviewee believes that physical access should be a high priority for DoD because logical access aims to differentiate between people who have already gained physical access. From a security standpoint, physical access could benefit most from the improved security biometrics would provide.

Throughput

It can take a long time for an employee or visitor to get through a gate or entrance point at a military base or other secure facility. Biometrics, combined with other technologies like transponders, could be used to set up a special lane where a biometric (*e.g.*, face) and other information (*e.g.*, biographical data, vehicle information) would be automatically transmitted from the vehicle to the guard before the person arrived at the gate. The transmitted information would appear on the guard’s computer screen so that when the vehicle reached the checkpoint the system could verify the driver and all authorized occupants. Biometrics would not *replace* personnel, because security guards would still be needed to handle visitors and prevent unauthorized access, but biometrics could help speed throughput.

The interviewee believes that biometrics could also help alleviate the throughput issues that occur every morning in a front office loaded with employees and visitors. There are delays as each individual presents identification and guards locate the security clearances of visitors. In his experience, the guards are initially unable to locate the security forms a high percentage of the time, which leads to a large back-up as the guards search for the paperwork. If employees were able to gain access biometrically (with, for example, a biometrically enabled DoD Common Access Card (CAC)), it would free up guards to focus on visitors’ credentials, and the process would go faster for everyone.

Security Clearances

In a related issue, the interviewee thinks it might be possible to make the passing of security clearances more efficient by utilizing biometrics to identify the visitor and biometrically match that person to an electronically transmitted clearance. The interviewee traveled extensively when he worked for a military research facility, and had to build significant amounts of time into his travel plans to allow for the lengthy signing-in processes. Biometrics could remove an entire piece of the process without sacrificing security.

Source: A mid-level officer at a U.S. military installation with security and criminal investigation experience who is familiar with biometric technologies.

Contractors Accessing U.S. Installations

The interviewee observed that many contractors and other personnel (*e.g.*, garbage collectors, delivery drivers) routinely access U.S. installations with minimal background checks at best. He noted that contractors or other workers who are dismissed from such a job (*e.g.*, for being a security risk, for criminal behavior, for poor performance, etc.) can easily assume another identity supported by paper-based documentation fraudulently obtained from criminal sources. A dismissed worker can then go to another U.S. base in the area and get hired to work. U.S. authorities might conduct name-based checks, but these checks are not routinely done, and are not helpful when someone has created a new alias identity.

The interviewee would like to stop this behavior and pointed out that going after the criminal providers of false identification documents is not effective because there are too many of them. He advocated taking fingerprints (or similar biometric identification) of all contractors when they apply for a job on base. The contractor's fingerprints could then be searched against the Federal Bureau of Investigation's (FBI) criminal master file (the Integrated Automated Fingerprint Identification System (IAFIS), which consists of ten rolled fingerprints of 47+ million felony arrestees), the United States Citizenship and Immigration Services (USCIS) IDENT system (for illegal aliens), or related watchlist databases for possible matches. The fingerprints would then be stored in a DoD database where they could be searched in the future. In this way, if any workers are dismissed or determined to be security or terrorist threats, their fingerprints can identify them if they reapply under a different name at another U.S. base. The interviewee feels that the ability to identify previously dismissed workers is an immediate requirement.

Source: A former political appointee in the DoD who is very familiar with biometric technologies and policy issues.

Foreign Visitors to DoD Research Facilities

Each year approximately 40,000 foreign visitors access DoD research facilities. The current admittance process involves the guest signing in by name on a paper and ink guest log maintained by a security guard. Although it would be beneficial from a security standpoint to be able to track these visitors—to know how many facilities they accessed, where, and when—there is currently no way to accomplish this. The foreign visitors' database is name-based. Name-based searches can be rendered ineffective due to miskeys or transliteration errors when records are created. Also, there is no way to track individuals who intentionally circumvent the current system by altering identity documents or using alias identities.

The interviewee described a system proposed several years ago that, if implemented, could streamline the administrative process for the visitor, fix or freeze the individual's identity, provide biometric identifiers, and track each individual. The key part of the

system, from a biometric standpoint, is that foreign visitors would supply a biometric (*e.g.*, iris, fingerprint) and a facial photograph. A temporary pass would be issued with the visitor's photograph and biometric, and the U.S. Government would be able to correlate and build data linked to a known set of visitors.

ACCESS CONTROL

LOGICAL ACCESS

Source: An SES official at a Military Department who is responsible for information technology. He is familiar with biometric technologies.

The interviewee does not foresee biometrics fully replacing passwords. He would like to introduce biometrics to the logical access arena from a logistics and convenience standpoint by binding biometric data to smart cards like the CAC. The interviewee debated when or whether a biometric should ever fully replace a PIN, allowing that it would depend on how strongly people come to believe in biometrics and how well biometrics perform. He envisions a future time (as the cost of biometric technologies decrease) when devices such as computer keyboards will be routinely equipped with imbedded biometric scanners and swipe card readers.

Biometrics and Digital Signatures

Ultimately, the interviewee prefers the stronger authentication and revocation capabilities associated with Public Key Infrastructure (PKI), digital signatures, and cryptographic log-on. In this sense, he sees a person using a biometric, in lieu of a PIN, to help create his or her digital signature—*e.g.*, the sender's use of his or her biometric would bind the digital signature attached to the electronic transmission of the sender.

He summarized the advantages of such an approach:

- Using the biometric, in lieu of a PIN, is easier and more convenient,
- Using the biometric may create a higher degree of non-repudiation than a PIN,
- Using the biometric is an additional security feature that can be offered to the local commander:
 - The biometric can take the place of the PIN, or
 - The biometric can be used in addition to the PIN.

Performance Issues

The interviewee said that biometric performance issues are a major concern for him. What are the error rates (*e.g.*, false accept, false reject, failure to enroll, etc.) associated with the various biometric technologies? He thinks that DoD Biometrics, through its Biometrics Fusion Center (BFC), could help provide valuable data with respect to performance issues.

Source: A General Officer at a Combatant Command, experienced in special operations. He is familiar with biometric technologies.

Computer Access

“The computer should know it's me.” A password or an ID card (such as the CAC) does not achieve this level of identity authentication because they are not implicitly tied to the individual who is entitled to have access. Passwords are vulnerable because it is not

uncommon for them to be shared between senior personnel and their assistants and support staff, and ID cards can be stolen.

The interviewee said he has a requirement for auditing his personnel's use of DoD computer networks, explaining that if a user on a Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) computer goes to an unapproved site (*e.g.*, a site displaying pornography) he would like an auto-response e-mail: "you went to this site, don't do it again." If the user did not in fact visit that site, it would indicate a breach in security.

The interviewee agreed that biometrics can provide better non-repudiation, and could help monitor the insider threat or other unauthorized use of DoD computers by providing robust auditing trails. Biometrics could be used in office operations as part of a tiered security system.

The interviewee said his instinct is that an ID card used for logical access should be paired with a biometric, without greatly reducing convenience—he envisions swiping his card and putting his thumb on a reader, with the computer verifying "it's me." Along these lines, using a biometric in conjunction with the CAC is a good idea because the CAC is already an agreed upon DoD platform.

Source: An SES official at a Combatant Command who is responsible for information technology. He is very familiar with biometric technologies.

Biometrics as a "Core Technology" for Information Assurance

The interviewee said that he considers biometrics to be a core technology for information assurance in the DoD. He explained that biometrics uses a person's physical characteristics for a digital cyberspace signature; the biometric is connected to who you inherently are, as opposed to something you have in your possession (*e.g.*, a token like a card) or something you know (*e.g.*, a password or PIN). With a card, you are just authenticating the card—whoever physically possesses the card gets access. With a password, you are just authenticating the password—whoever knows the password gets access. With a biometric, you are authenticating the inherent physical characteristic of the person—it is extremely hard for someone else to possess or know the biometric. This inherency, in his view, accounts for greater security of the biometric.

The interviewee said that DoD components currently use user IDs and passwords for logical access. The problem is that user IDs offer minimal security protection and there is great risk of passwords being compromised, as they are inconvenient and difficult to remember, particularly when personnel have multiple passwords to remember.

Defense in Depth: A New Paradigm

Biometrics is a core technology because it will serve as a fundamental part of what the interviewee calls a "Trusted Personnel Identification Service" for what he envisions as the new DoD Defense in Depth paradigm. The current DoD Defense in Depth approach

protects operating systems (OS), local area networks (LANs), and wide area networks (WANs). The interviewee believes that DoD needs to move to a new Defense in Depth paradigm that protects:

1. Infrastructure—the OS, LANs, WANs, etc., that enable information to be processed, stored, and transmitted.
2. Community—only those who are trusted are in this community and you have a very high level of assurance that you are dealing with the trusted party—this is where biometrics and the Trusted Personnel Identification Service are used.
3. Information—the content; information is what DoD is really protecting (*e.g.*, information about the location and strength of U.S. forces). We do not want this information to be stolen, spoofed, or improperly changed.

By way of background, the interviewee explained that in the industrial age (*i.e.*, before the computer-intensive information age), information was attached to a particular physical medium (*e.g.*, a map showed the disposition of U.S. forces). By protecting the physical medium, the informational content was adequately protected (*e.g.*, the map was put in a safe).

According to the interviewee, the information age has caused that approach to “information assurance” to change radically. No one can easily “hold” information; no one can easily hold the medium because electrons hold the information and they are too easily copied, processed, stored, and transmitted. However, much of the Department of Defense’s thinking about information assurance is still mired in this pre-information age view—“protect the medium.”

Information has to be tagged so that it can be protected, for example, by encryption or other appropriate measures. The information should be tagged with indicators such as its releasability and accessibility.

With respect to community, teams in the industrial age were in close physical contact with one another and shared the same physical space. In the information age, you do not need to be in the same space to have a team. Teams can be distributed globally and they need ways to access, with a high level of assurance, trust, and permissions, information that they need to do their jobs. Teams use information and bring value to the information. For example, the team may use information on the location of enemy forces to target the enemy forces.

Biometrics & the Trusted Personnel Identification Service

The interviewee envisions a new paradigm for the Department of Defense, based on the Trusted Personnel Identification Service. He stressed that role-based access control is essential to this paradigm, and this is the function of the Trusted Personnel Identification Service. The Trusted Personnel Identification Service provides a high level of assurance that the person in the network is who he purports to be. It incorporates biometrics as a core technology because it is: (1) part of the way we vet the person (*e.g.*, the search of a person’s biometric against watchlists and databases, like the FBI’s IAFIS), (2) the principal way we can fix the person’s identity in the system (*e.g.*, one-to-many searching

of a person's biometric against the community database to assure that the person's biometric is unique to the community database—a match could indicate that the person is already enrolled under an alias identity), and (3) a principal method of access control, or the way a person will enter a computer system or network.

The Trusted Personnel Identification Service will also use the DoD CAC PKI certificate as well as user IDs and passwords.

Tracking and Auditing

The interviewee said that he regards the “insider threat” as the greatest danger to the security of DoD information. He said that DoD performs various monitoring of its computers and networks, and thought that biometrics would help make a better audit trail. Biometrics are much harder to repudiate, whereas something like a cipher lock, combination, or even a password does not necessarily tie access to a particular individual the way a biometric, like a fingerprint, does.

Source: An OSD SES official with extensive experience in program analysis and evaluation. He is not familiar with biometric technologies.

Public Key Infrastructure v. Biometrics

The interviewee pointed out that logical access will, in part, be secured using new federal PKI technology for authentication purposes, as well as existing policy in place to protect access to the computer networks, like SIPRNET (Secret Internet Protocol Router Network) and NIPRNET. The interviewee made the point that DoD has invested a great deal of money in PKI, which was developed simultaneously with the development and distribution of smart cards—the CAC. The interviewee wonders if there is also a need to add the additional layer of biometrics to this system. He also asked if biometrics was in direct competition with PKI and whether the costs associated with biometrics are worthwhile. “Is it all solving the same problem?”

Password Replacement?

The interviewee would like to see more studies that address the need to replace passwords and tokens with a biometric. For example, how much data do we have that shows negative results from forgotten or misplaced passwords in DoD? The interviewee would like to have data demonstrating how biometric technology could represent a cost savings to DoD in terms of costs incurred to maintain a user password. He would also like to see data on how well the various biometrics perform.

TACTICAL APPLICATIONS FOR BIOMETRICS

Source: A General Officer at a Combatant Command, experienced in special operations. He is familiar with biometric technologies.

The interviewee discussed several military requirements that biometrics could help fulfill. In terms of his priorities, he has an immediate requirement to improve identification authentication in certain functions in the tactical arena, to include classified activities. Biometrics may help fulfill this requirement by authenticating the identity of U.S. personnel transmitting sensitive information. This tactical requirement is a higher priority for him than using biometrics for physical access or logical access. His specific tactical requirements are explained below.

Verification of Trusted Agents

The interviewee expressed concern that as sensitive information is becoming more lethal, (e.g., information sent by special operations forces on the ground to direct air strikes) it is becoming more important to verify the identity of the person sending the information, and to ensure that he has not been compromised and the device transmitting the sensitive information has not fallen into the wrong hands. For example, if a trusted agent on the ground in a foreign country is logging in and reporting back sensitive information on a particular situation, we must know that he is who he says he is and he has not been captured nor the system compromised.

The reality is that there are small numbers of U.S. military personnel in harm's way with a mission to direct increasingly lethal fire on enemy positions and targets. The Department of Defense has a requirement for a very reliable way to ensure that the system of transmitting this information will work dependably and that the enemy cannot exploit it. For example, if you require a PIN for identity authentication on the transmitting device (e.g., a portable digital assistant) and the agent is killed, the PIN might still be in it (or the PIN could be compromised) and the device could be captured and used by the enemy to direct U.S. fire on U.S. positions or targets.

The interviewee believes a biometric could provide better identity authentication and security; however, it is essential that the fallen agent's teammates also be able to use the device (which means the device would have to accommodate several biometric users). Also, the interviewee is interested in having the trusted agent use a biometric as a duress signal to indicate that he has been compromised. He also has a short-term requirement for a reliable continuous verification capability in this tactical environment, and asked if biometrics perform well enough to help him with this requirement.

The interviewee explained that aircraft frequently receive target coordinates from trusted agents on the ground. Even as the time between identification of the target, confirmation of the enemy, and the air strike is decreased, the targets must be verified. They need to ensure that the information is coming from a trusted agent who has not been compromised, and not an enemy who has captured or intercepted the system.

Additionally, there is a throughput issue. In Afghanistan, U.S. aircraft were stacked up in the skies, waiting for target coordinates to be verified. If you expedite this process by letting the agents dial directly to the aircraft, you set yourself up to be deceived if, for example, the enemy captures the transmission device and uses it to send a false transmission to bomb U.S. positions. The interviewee emphasized that he has a short-term requirement for a highly reliable, high performance way to verify that the person sending the coordinates is who he says he is in the scenario he described. Again, he thinks biometrics might be able to help him with his requirement.

Casualty Identification Assistance

The interviewee believes that biometrics could provide a quick means to identify casualties, a long-standing requirement, if biometric records of service members are kept in a searchable database. This way a fingerprint of a casualty could be searched against the central database for possible matches. This use of biometrics would probably be faster than using DNA in many cases.

Source: A former senior political appointee with extensive military manpower and training, research analysis, and management experience. He is familiar with biometric technologies.

Tactical Battlefield: Need for Continuous Verification

The interviewee is very concerned about the security risk of computer networks in a tactical environment on the battlefield and believes that biometrics might be able to address this problem.

By way of background, the U.S. Army has decided that a common operating picture of the battlefield provides tactical advantages during combat, such as improving command and control, providing situational awareness, etc. However, the interviewee noted that system developers and implementers of these digital battlefield command and control, visualization, and management systems must also consider tactical risk. His specific concern is that U.S. opponents may try to capture battlefield computers and/or access the U.S. battlefield computer network clandestinely. Once these opponents have access to such systems, even for short time periods of minutes or half an hour, they could use it to undermine U.S. battlefield management and combat operations, which could pose a significant tactical risk.

The interviewee said that, currently, when a U.S. Army soldier logs onto a battlefield computer (such as those in a tactical operations center), access control involves standard civilian computer security systems. Such systems have user password verification only at the start of the session; there is no re-verification of the authorized user. If the computer were captured, an opponent could gain system access. Given this risk, the interviewee feels there is a need for continuous verification of the computer operator to ensure that the authorized user is still on the system.

In order to secure this tactical battlefield computer system, the interviewee discussed two general options:

1. The computer system is designed so that the machine constantly validates the person using the system with a biometric technology that can perform a check very frequently—every minute or so. This system would lock a person out immediately if the biometric verification check fails. He thinks there are probably technical challenges to performing such continuous verification, given the system requirements of a hostile battlefield environment, but if they could be addressed then this security problem could be solved.
2. The computer network is partitioned such that if a system node is compromised the information that can be accessed is limited and other users are notified that the network has been compromised. In this case, sufficient compartmentalization of the system is needed, so that only very localized information is visible. A secure firewall must also be implemented so that core information cannot be accessed. However, such a system does not seem that feasible to the interviewee because a skilled computer systems person can get around firewalls. In addition, it may not be feasible to design such a partitioned system. Therefore, he feels the first option is a more promising solution to this problem.

Continuous Verification System Requirements

The interviewee described how this continuous verification system should work. He stressed that it must be “active,” “frequent,” and “non-disruptive.” The authorized system operator would be registered in a local database for a local tank, platoon, or command. When the operator logs onto the computer, and every minute or so while on the system, there would be an “active” biometric scan (such as an iris scan) that scans the person automatically to verify that the individual is authorized to use the system. He does not think that a passive scan, which examines behavior patterns (such as typing patterns), would be sufficient. The system would have to be non-disruptive, so it would not interfere with the operator’s battlefield mission. In order to be non-intrusive the system would have to be miniaturized to fit within battlefield equipment.

A key system requirement that the interviewee thought poses significant technical challenges is that the biometric technology must be robust and stable enough to verify the person “100% of the time” in the hostile battlefield environment. The scan cannot have any false negatives. A battlefield environment means a person may be:

- Severely stressed,
- Deprived of sleep,
- Exposed to chemical weapons, including smoke, etc.,
- Exposed to other physical irritants, such as dust, dirt, and wind,
- Wearing gloves, goggles, or a gas mask,
- Operating in a dynamic environment with respect to light, noise, air quality, and temperature.

Source: A mid-level Army officer at the National Defense University with information operations, information assurance, and network security experience. He is very familiar with biometric technologies and has published papers on the topic.

High Assurance Application

Given the current state of biometrics, the interviewee would use biometrics only for very high assurance operations, “like nuclear release activity or very high variance message traffic.” He does not think the technology is ready for deployment to enable basic weapons systems. “For wide-spread, muddy boots use? I am erring on the side of caution. I would worry about robustness. It needs long-term testing first.”

However, the interviewee sees opportunities for garrison-level use in the field, utilizing biometrics as a means to offer an element of control, which he identifies as a tactical usage.

Positive Identification as a Means of Control

The interviewee identified a broader scale need for biometrics at the tactical level for controlling non-government people. The interviewee would like to employ biometric technologies to aid in identification and authentication of indigenous personnel where U.S. forces are deployed because the military has to secure and bring order and control into an area. “It is a place where you don’t know who is who and you’re in the middle of it.”

Positive Identification for Force Protection

The interviewee also recommends using biometric means to enhance force protection efforts. Collecting biometrics from prisoners or people determined to be a threat provides a database to eliminate future applicants for employment or other authorization needs. Moreover, the interviewee thought that cameras could be used “if you have some faces of the people you capture, or want to use a camera to look for certain individual movement patterns.” However, he noted that there is a lack of independent data for facial recognition studies; he believes there is a need for certification for this area of research.

The interviewee wondered if it was possible for the DoD to impose these types of measures, using biometrics to protect DoD personnel “where we are trying to take control of an area and bring stability to a situation.”

IDENTITY AUTHENTICATION

DEPARTMENT OF DEFENSE “CIVIL FILES”

Although some interviewees expressed concerns about the storage of such information, the idea of a Department of Defense “civil files”—similar to the FBI’s civil files—was largely supported.

Source: A mid-level Army officer with extensive experience in law enforcement, criminal investigations, and counter-intelligence. He is a biometric subject matter expert.

The interviewee said there is an immediate requirement to establish a searchable fingerprint database of DoD members to fix identity and aid in casualty identification, criminal investigation, counterintelligence, and counterterrorism matters.

Background

By way of background, the interviewee noted that the Federal Bureau of Investigation’s “civil files” database maintains approximately 87 million civil fingerprint cards representing approximately 40 million people. These individuals have been fingerprinted as a result of federal employment applications or military service, for alien registration and naturalization purposes, as well as for voluntary submission for personal identification purposes. Thus, the fingerprints of DoD civilians and military members are taken by law and copies reposed in the civil files.

The FBI’s civil files database is not yet automated, unlike the FBI’s Integrated Automated Fingerprint Identification System (IAFIS), holding the criminal fingerprint records (known as the “criminal master file”), which is fully automated. The vast bulk of the civil files’ fingerprint records are still the paper and ink variety. Since May 2000, the FBI has taken steps to automate the database from “Day One forward” as it receives electronic versions, *i.e.*, new fingerprint cards in electronic format. Thus, over time, as the FBI receives more and more electronic images, the civil files will become an increasingly useful database in which to search for national security, criminal investigation, or other purposes. The FBI also has the option of scanning into the database the pre-May 2000 paper and ink fingerprint records, *i.e.*, tenprint cards, to convert them into electronic format as it did with the criminal master file.

In the case of the DoD, the FBI, with the DoD’s blessing, is scanning in the 2.1 million fingerprint records of enlisted military personnel dating back to May 1990. The FBI is electronically organizing a special “latent searchable” database within the civil files database for these military members. By recording civil fingerprint records electronically into the civil files database, the civil files database, like the criminal master file database, would become more easily and readily searchable. According to the interviewee, the ink and paper civil files are massive, and difficult and time-consuming to search.

1:N Search Capability—Fixing Identity

The interviewee believes that the one-to-many (1:N) searching capability of a DoD civil files database—which could *fix* identity—is an essential short-term capability (requirement) for the Department of Defense.

The interviewee explained that when an individual joins the military, or applies for employment at DoD, a National Agency Check (NAC) includes a search of the person's ten rolled fingerprints in the FBI's IAFIS. When the NAC comes back clean (*i.e.*, no match found), that is the end of the current check. The fingerprints are not checked against DoD fingerprint records to see if the individual has ever previously been in the military or enrolled under a different name.

If this 1:N check could be done against a DoD civil files database of all current and former military members and DoD civilians to ensure the enlistee is not already enrolled in alias, then the individual's identity could be fixed or frozen and entered in the DoD civil files. From that point forward, a comparison could always be made to that record with a 1:1 search as part of identity authentication.

Electronic Tracking

The interviewee strongly recommends developing an electronic tracking capability in conjunction with the civil files, such that every fingerprint allegedly submitted as an individual is stored. Thus, DoD would have a record of the fingerprint that was submitted and rejected—and could monitor whether rejections were false rejects or fraud.

The technology currently exists to make the searchable DoD civil files a near-term reality. Civil files would help criminal investigation, counterterrorism, counterintelligence, and casualty identification. However, the biggest challenge to making the civil files a reality will be policy.

Leveraging the FBI's IAFIS

The Department of Defense should leverage the FBI's systems wherever possible, build to FBI standards to ensure interoperability, and have subsets of files (containing millions of individuals) that belong to DoD.

When asked who should be responsible for stewardship of the DoD searchable civil files—the DoD or the FBI—the interviewee said that DoD should control:

- Input—what goes into each file?
- Access—who can access the file and for what purpose?
- “Flash identity”—certain individuals' records are flagged and protected. For example, the Connecticut police arrested an individual and sent his card to the FBI to search in IAFIS. The individual was a protected witness whose information is stored in IAFIS as a flash identity (as are undercover agents, etc.), so the FBI reported “no record” to the Connecticut police, and reported the arrest to the U.S. Marshals (who run the witness protection program). Within DoD there are individuals who do not exist in open files—such as those on classified missions or covert operations—who must be protected.

Other Considerations

The FBI's IAFIS has an excellent reputation, and it is the most accurate large-scale system that exists in the world. Working with the FBI is the best way to proceed, but DoD shouldn't relinquish stewardship of its civil files. It will also be important to include other parties that will be involved in and be affected by the creation of the DoD civil files to ensure oversight, such as DoD's law enforcement, the relevant DoD legal representatives, the Biometrics Management Office, and many others. It is important to get the various parties on board early as an oversight group, and work with them to outline the details of input, access, limitations, and controls for the database.

"Red Force" and Watchlists

The interviewee believes the DoD civil files database should be able to link to U.S. maintained databases of "red force" records of all enemy prisoners of war (EPWs), detainees, and others (for example, the records that have been collected in Iraq and Afghanistan), and these should help populate a watchlist. The Department of Defense should create an interface system with the FBI watchlist so that, for example, when a person with a fake military ID shows up on base and his or her fingerprint does not produce a match within the civil files, it will automatically be checked against the watchlist.

Use by Law Enforcement

The existence of searchable DoD civil files will likely lead to requests for searches from non-military law enforcement. The interviewee believes that there should be authorization for this type of search in the policy, if the request is for a bona fide investigation. For example, if a murder occurs next to a military base and the evidence includes a latent fingerprint from the murder weapon, the police would search the FBI's IAFIS criminal master file. If the IAFIS search comes back negative, it is reasonable to request a search of the DoD civil files database. A soldier does not have the right to not be identified because he is in the military. The interviewee is not really worried about abuse of the system or DoD being inundated with requests for frivolous searches because many states do not even search IAFIS unless it is a murder investigation. DoD would only grant permissions for bona fide cases, and a DoD oversight board should be established to monitor such searches.

Casualty Identification

The interviewee said that if DoD succeeds in creating a searchable DoD civil files with ten print records from every military member and DoD civilian employee, casualty identification will become one of the new capabilities; casualty identification is a desirable short-term requirement. Fingerprints often are preferred over DNA for identification in scenarios where—for example—the body is contaminated. Fingers can be imaged without risk of chemical contamination and without collecting physical samples. If fingerprints are available, casualty identification is much faster.

Source: A former SES official at the Federal Bureau of Investigation who is a biometric subject matter expert.

The interviewee is very familiar with the FBI's IAFIS, and observes that it can compare fingerprint images it receives with its huge database of fingerprints and determine if there is a match in an average of one hour. He believes that DoD should create and maintain a DoD civil files database that can be searched as part of background investigations and against all arrest records. He contends that having such an electronic civil files database of fingerprint records would make for better public safety because it would enable DoD and the U.S. Government (USG) to update the process of ensuring that military members, USG employees, and those with national security clearances have not run afoul of the law.

Counterintelligence and Counterterrorist Investigations

Searching the civil files also could be an aid in counterintelligence and counterterrorist investigations. For example, if U.S. authorities learn that an intelligence officer of a foreign government used a particular hotel room to meet with an unknown person, that room could be checked for latent prints. Ideally, the authorities would want to learn the identity of the person with whom the foreign intelligence officer met, because that person might be committing acts of espionage by providing unauthorized information to the intelligence officer, or planning terrorist attacks. Any prints recovered from the hotel room could be searched against the civil files for a possible match. A match, while not conclusive evidence that the person is a spy, would help the authorities' investigative efforts. Similarly, if the authorities found prohibited terrorist literature in the possession of a military member, they could examine the literature for fingerprints. Any recovered latent prints could be searched against the civil files to help determine who else accessed the literature.

Discharged Service Members

The military regularly ejects Service members for reasons other than criminal conduct. After their discharge from the service, some of these ejectees try to re-enlist in the military under another name—and some are successful. Searching the civil files for all enlistees would soon put a stop to this behavior because when the person tried to re-enlist in alias, his fingerprints would be searched against the civil files database and be matched to the fingerprints he submitted when he first joined the military under a different name.

Creating a searchable DoD civil files database will require extensive policy and legal work and will probably meet with some opposition from certain quarters. Oversight mechanisms will be needed to protect privacy, respect DoD military and civilian members' rights, and ensure against any misuse of the data. Moreover, many DoD components will have to be involved in the policy making process.

Source: A former high-level political appointee in the DoD who is very familiar with biometric technologies and policy issues.

Privacy Concerns

The interviewee said that although the arguments for a searchable DoD civil files database are persuasive, he has concerns about privacy issues and the potential for governmental abuse. He believes that the U.S. needs to increase civil applications of biometrics, but there is the issue of protecting privacy. Many people do not trust that the government is skilled enough or motivated enough to protect their privacy. Also, although this may be a reliable system to catch “the innocent or the dumb,” it will not work against “the willful or the smart.” He worries about counting on a perimeter security screen, or relying on a hypothetical bad guy to provide a starting point (*e.g.*, leaving a latent print or trying to enroll twice) for security officers and law enforcement. It comes down to a question of privacy controls and how good the professionals are.

These concerns do not mean that DoD should not pursue this civil files approach; rather, DoD must work hard to develop better privacy controls and better procedures. The interviewee emphasized that he is not opposed to biometrics, but he is opposed to people who think it is an easy solution. Biometrics is the easy part—the challenge is developing the discipline to protect privacy and the ability to move against threats in a smart way.

IDENTITY AUTHENTICATION

PRISON MANAGEMENT

Source: A university researcher with extensive civilian and military corrections management and technology experience who is very familiar with biometric technologies.

According to the interviewee, “identification and authentication are fundamental requirements for security in corrections.” As of June 2002, there were over two million inmates in U.S. prisons and jails. Prisoners are fingerprinted when they enter the system; however, there are no standards across states, local jurisdictions, private prisons, etc., for the continued tracking of prisoners.

Identification and Authentication of Prisoners

Systems are needed to prevent inmates from switching identities and to track inmate movements within and between institutions. According to the interviewee, this is especially important when the time comes to release an inmate because “you don’t want to release the wrong person.” Currently, inmate movements are controlled and monitored by facility staff. Many facilities use paper passes that are logged at each location. Further checks are made by utilizing multiple inmate “counts.” This system is cumbersome, inefficient, and susceptible to error.

Identification and Tracking of Inmate Visitors

The need to identify and authenticate individuals in the prison system also applies to visitors at prison facilities. The interviewee indicated that prison policy is that visitors should appear on only one inmate’s visitor list. This is to prevent visitors from acting as messengers or couriers for the prisoners. With the current system of checks, it is very difficult to verify that visitors are only on one list. By enrolling visitors in a biometric system, officials could track visits and prevent individuals from visiting more than one prisoner. In addition, a biometric system could speed up throughput during visitor hours.

Identification and Tracking of Prison Staff

Biometric technologies can also be used to control prison staff movement. Staff could easily check in and out of the facility using biometrics. This would provide an efficient and quick way to determine who was in the facility during an emergency situation, such as a prisoner riot.

The interviewee stated that the military could take the lead in this area of biometric usage and in proving the technology. The population in military prisons has increased and the military is now taking the lead with terrorist detainees (*e.g.*, the detainees held at Guantanamo Bay). Thus, the need for reliable tracking is even more important. However, the interviewee notes that moving too quickly could cause the death of a biometric program in this environment, cautioning that “one wrong person released [because of an error in the biometric check] and the program would be sunk.”

GENERAL COMMENTS ON BIOMETRIC USAGE

Source: A senior DoD official who is responsible for critical infrastructure protection. He is familiar with biometric technologies.

Technology Appropriateness

Biometric technologies should be appropriate to the task. Biometrics should be used to supplant or support other identification measures based on the level of certainty required for a given situation. The interviewee did not express a preference for any particular biometric; however, he suggests a sliding scale depicting necessary levels of surety that subdivides activities with identity assurance needs. For example, gaining entrance to the National Military Command Center could require a photo ID at the exterior, a fingerprint scan once inside, and an eye scan for access to a computer.

Necessary Levels of Surety

Certainty Level	Example	Identity Assurance Procedures
High	Accessing an automated data system that can launch nuclear missiles.	Token AND Password AND Biometrics; a layered approach to ensure correct person is given correct access.
Low	Accessing the physical fitness center.	Token OR Password OR Biometrics; weigh convenience more heavily.

Enrollment

Enrollment represents a particular vulnerability in all identification systems, including biometric systems. The issue is more a function of processes and procedures than specific technology. The interviewee expressed a need for strong caution and rigor to ensure the security and fidelity of the enrollment process, noting especially that *no single person* should have control of the initial enrollment. He suggested specific steps to help ensure secure enrollment, including random checking of enrollees and close attention to revocation list protocols.

Source: An OSD SES official with extensive experience in program analysis and evaluation. He is not familiar with biometric technologies.

Defining the Mission for the Technology

The interviewee encouraged the Department of Defense to think through the purpose of using biometrics:

- What is the goal?
- What does it cost?
- What infrastructure is required?
- What else could be done at the same or lower cost?

He thinks that it is important to make determinations about the necessity for biometrics. The question shouldn't be, "Can we build this?;" it should be, "Is there a need?" He does not support developing a technology for which there is little demand. The interviewee is concerned that the DoD biometrics program is following a model of building the technology and then waiting for a need to develop. "You have to have a mission needs statement: here is the threat, or, here is the goal you are trying to meet."

The interviewee also expressed a number of concerns with regards to a centralized repository of biometric information.

Scaled Development

The interviewee expressed concern about attempting to develop a Department-wide central repository too quickly. He cautions against trying to build the entire database all at once. The interviewee said that this is, in part, a scalability issue. If it is established that a repository is necessary, he recommends building the repository incrementally; rolled out small, adding modules to the database as it is constructed.

Number of Records

The interviewee is curious about the size of such a database. He believes that there are scenarios where biometrics would prove useful. At the same time, "you don't need to have every cafeteria worker in the system." The interviewee believes that the database could become too large. "If I am a visitor to [a military installation], are you going to collect my biometric? Who will set the limits?" He would like to determine the needs of a central repository and the purpose served by having one.

Mission Creep and Data Vulnerability

The interviewee is also concerned about how a central repository of biometric data could be used. Who will have access to it? How long will biometric data remain on file? He asked about precautions to ensure against fraud. There is a privacy concern for protecting repository data and the future use of the data. There is also a cost (possibly large) to provide that protection.