BIOMETRICS
SECURITY TECHNICAL IMPLEMENTATION GUIDE
Version 1, Release 3

11 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

- The previous release was Version 1, Release 2, dated 11 August 2004.
- Updated Manual procedure section reference numbers in throughout the table in Section
- Added check for PDI 1001 in Section 3.
- Changed PDI numbers of all checks in Sections 2.4.5 and 2.4.6.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

Historically, biometrics has been relegated to a single method (fingerprinting). However, in the last two to three years, new biometric methods and technologies have been developed that lower cost and increase usability. Companies developing new methods number in the hundreds and their methods continue to evolve as the technology advances. The availability, effectiveness, and affordability of biometric technology continues to progress as the demand for authentication has increased. This increased interest is driven by an exploding problem with identity theft and computer fraud coupled with the increased use of remote connectivity methods, such as, Internet access.

With regard to technology, biometrics is the term given to the use of biological traits or behavioral characteristics to identify an individual. The trait used may be fingerprints, hand geometry, facial geometry, retina patterns, iris patterns, voice recognition, handwriting recognition, or any of the increasingly available traits. A biometric system is essentially a pattern recognition system. The system includes all the hardware, software, and the interconnecting infrastructure, which enables the matching of a live sample to a stored pattern in a database.

Biometric systems are used to provide access control for computer networks, banking services, and airport/seaport services. Biometric data is now being captured on passports and as part of the military service record. Central biometric repositories are planned for the DOD space, which will facilitate the rapid adaptation of biometric technology for both battlefield applications and support services.

Although biometrics can be used to enhance security, there are security risks associated with the use of any technology, which must be mitigated. The intent of this Biometrics STIG is to provide guidelines for the implementation of technological systems, which include biometrics.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

This document is a requirement for all DOD administered systems and all systems connected to DOD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "[*N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@ritchie.disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. INTRODUCTION TO BIOMETRIC TERMINOLOGY AND CONCEPTS

Biometrics is a very broad and fast moving segment of the information technology (IT) industry. Different vendors and support personnel can use different terminology to describe similar biometric concepts. To avoid ambiguity, this section defines terms and concepts that are necessary to interpret the guidance in later sections. It is not meant to be a general primer on biometrics.

2.1 Identification versus Verification

Biometrics can support either *identification* or *verification*. When biometrics is used in the identification process, users do not state who they are. For example, a fingerprint reader might be used to identify criminals who otherwise might refuse to identify themselves or present false identities. In the future, iris-scanning devices might be able to identify known terrorists in a crowd. When biometric technology is used in identification, the process is *one-to-many*. In other words, one reading must be compared against many potential profiles to find a possible match.

When biometrics is used in the verification process, users first declare who they are by entering their logon name (in the case of most computer logons) or presenting an identification card (most common in physical access control). Then biometric technology is used to *verify* that identity. The technology does this by comparing a biometric reading against a profile stored *for that user*. In this case, the process is considered to be *one-to-one*. That is, one reading is compared to one profile – they either match or they do not.

Identification processes are significantly more complex and error prone than verification processes. This STIG primarily addresses the use of biometrics in verification.

2.2 Authentication Factors

When a user authenticates to an access control system, the user presents an identity along with evidence of this identity. This evidence is either something the user; knows (e.g., a password); has (e.g., a token or smart card); and is (a biometric).

Each of these is considered an authentication *factor*. If only one of these factors is used to verify an identity, it is called single factor authentication. If two factors are employed, it is two-factor authentication. Similarly, if all three factors are required, this is three-factor authentication.

Some view biometrics as a potential *replacement* for authentication based on one or both of the other two factors, perhaps providing a level of convenience that could not be obtained with the other factors. Others view biometrics as a *supplement* to authentication based on one or both of the other factors, thereby strengthening an existing authentication scheme.

Depending upon the biometric technology and the risk environment, using biometrics as a replacement technology may either improve or degrade security. Using biometrics to supplement the other authentication factors will very likely enhance security. Accordingly, from a security perspective, biometric verification is best deployed as a component of two-or three-factor authentication.

2.3 Biometric Processes

Biometrics supports two basic core processes that together provide organizations the ability to verify claims of identity:

Enrollment – the initial association of an identity with a biometric characteristic.

Verification – the comparison of biometric data collected at the time of an authentication request with the biometric data collected during enrollment.

There are *administrative* and *cryptographic* functions that support both enrollment and verification. There must also be a *fallback* process that is implemented whenever the verification process cannot be utilized (e.g., the system is down or the user cannot present the biometric characteristic due to injury or physical challenge).

This STIG lists threats to each of these processes and describes how technical configuration or procedures can mitigate the risks associated with those threats. The remainder of this section provides additional detail on the core enrollment and verification processes.

2.3.1 Enrollment

The stages of the process are as follows:

Initial Verification of Identity happens when the user presents some evidence that he or she is in fact that individual without using the biometric technology for this verification. This might involve the presentation of photo ID or authentication to trusted computer. All subsequent verification of identity is dependent upon the strength of this initial verification. In other words, if an imposter can present a false identity at this stage in the process, he will be able to authenticate the impersonated identity in perpetuity unless there is some alternative means of detecting the false identity. The stages are as follows, Capture, Extraction, Package Creation and Assurance, and Package Storage.

In the Capture stage, biometric technology is used to record a user's physical characteristic or behavior. The hardware performing the reading is called the *capture device*. Capture devices typically are designed to capture one biometric characteristic such as a finger print, retina pattern or keyboard dynamic.

In the Extraction *stage*, the captured information from the capture device is translated into a digital representation of the biometric characteristic. This digital representation is known as the *biometric template*.

In the Package Creation and Assurance stage, the biometric template is associated or bound with the user's identity information (e.g., name, ID, etc.). The package is then encrypted and digitally signed to protect its integrity and confidentiality.

In the Package Storage stage, the biometric package is encrypted and signed package the written to a non-volatile storage medium for future use in the verification process. This storage medium may or may not be integrated into the biometric system. For example, packages might be transferred to a smart card or external database.

2.3.2 Verification

The stages of the process are as follows:

Identification – the user presents some form of identity, perhaps typing in a user name or ID number. Alternatively, the user could present a swipe card or smart card.

Capture – this is the identical process as the one performed during enrollment.

Extraction – this is also the identical process as the one performed during enrollment, but this time the result is called the *live sample* rather than the biometric template.

Package Retrieval and Validation – the biometric package is retrieved from storage and decrypted. Its digital signature is validated to ensure that it was created during the enrollment process and not modified since then.

Comparison – The live sample and biometric template are provided as inputs to a software module known as the comparator, which generates a score describing how close a match the two are to one another. Based on predetermined thresholds, the two are either declared a match given the resulting score (*acceptance*) or they are not (*rejection*). The determination is forwarded to whatever access control system the biometric technology is supporting.

2.4 Physical versus Logical Access Control

Biometric verification can be either a component of physical or logical access controls. Physical access refers to entry to a secure area such as a building or server room. Logical access refers to use of a computing resource such as desktop computer.

The biometric hardware and software to support physical and logical access control can be and often are identical. In both cases, the biometric system captures a biometric sample from the user, compares it against a template, and either verifies that the two are the same (acceptance) or that they are not (rejection). Therefore, the configuration of biometric authentication systems can be considered independently from the type of access control they support.

This page is intentionally left blank.

3. ADMINISTRATIVE THREATS AND CONTROLS

With biometric access control technology, administrators are the only users that interact with the system beyond the biometric capture device. This distinguishes it from most other technologies (operating systems, web servers, databases, desktop applications, etc.) in which users enter, manipulate and retrieve data on a regular basis. Any user action represents a potential point of vulnerability. Thus, in the case of biometrics, improper administrative user access poses one of the greatest security risks to the system.

First and foremost, only those designated with the authority to administer the biometric system should have access to its administrative controls. Thus, biometric system administrators should be required to authenticate to the biometric software before the software allows any access to its controls. Importantly, the authentication should be something other than biometric authentication (e.g., a password, perhaps combined with a token or smart card) in case the biometric system has been compromised or is not functioning.

3.1 Separation of Duties

Ideally, there should be a separation of duties within the administrative function. As is specified in the *Biometric Verification Mode Protection Profile for Medium Assurance Environments*, there should be, at a minimum, the following three administrative roles:

Enrollment Administrator – the individual who verifies the identity of new users and guides them through the creation of their associated biometric reference templates using the biometric capture device.

Security Administrator – the individual who establishes and modifies the values of configuration parameters in the biometric software.

Audit Administrator – the individual who reviews audit logs for security violations and related suspicious behavior.

- *(BIO1001: CAT II) The IAO will ensure that individuals are assigned to the following administrative roles: Enrollment Administrator, Security Administrator, and Audit Administrator.*

The integrity of the system may be impacted if these roles are combined. For example, if there is no independent audit administrator, then other administrators can tamper with the system without detection. If the security administrator is also the enrollment administrator, then he or she can manipulate configuration settings to allow for weak templates and then enroll users in a manner that will make it easier to breach the system at a later date. If there is separation of duties, then this is not possible unless the enrollment and security administrators conspire to jointly circumvent the system controls.

If the biometric software supports separation of duties as described above, the security administrator should activate this feature. If not, the Information Assurance Officer (IAO) should still implement compensating controls that make an administrator breach less likely to occur. For example, the IAO can regularly check that each user enrolled in the system has an approved System Authorization Access Request (SAAR) DD Form 2875 or similar access authorization forms used to request that access. In addition, audit logs can be regularly copied to a location inaccessible to biometric systems administrators so they can be reviewed independently.

- *(BIO1010: CAT III) The IAO will maintain lists of individuals authorized to perform each of the following functions: enroll or re-enroll users; modify the security configuration; and review and manage audit logs.*

3.2 Technical Restrictions on Administrative Access

Preferably, the biometric software will have its own administrative authentication module. If not, the systems administrator should limit permissions to all executable files to a user group whose membership consists of authorized administrators only.

- *(BIO1020: CAT I I) The IAO will ensure that the following functions are restricted to authorized Administrators:*

  - *Creation or modification of authentication rules*
  - *Creation, installation, modification or revocation of cryptographic keys*
  - *Startup and shutdown of the biometric service*

- *(BIO1030: CAT II) The IAO will ensure that only authorized Enrollment Administrators are permitted to create user biometric templates.*

- *(BIO1040: CAT III) The IAO will ensure that only authorized Audit Administrators can clear the audit log or modify any of its entries.*

- *(BIO1050: CAT II) The IAO will ensure that all Administrators must authenticate to the biometric system to perform administrative functions and that this authentication must include a factor outside of the biometric verification the system supports for ordinary users.*

4. CRYPTOGRAPHIC THREATS AND CONTROLS

Proper use of cryptography greatly reduces the risks of several key potential vulnerabilities in biometric systems. For example, through the use of digital signatures, the comparator can have greater assurance that biometric data has not been maliciously modified when it is transferred from storage to the comparator. This risk is substantial because biometric packages may be stored in a location outside the control of the biometric system such as on a smart card or in an on-line user directory.

In this case, encryption might work as follows. During the enrollment process, the biometric system would encrypt and digitally sign any package sent to storage. During the verification process, the comparator would decrypt the package and verify the associated signature to ensure that package was the one created during the enrollment process.

Suppose an adversary were able to breach the storage security and replace the biometric data with his own template. If there were no cryptographic protection, then the adversary would be able to pose as an imposter once the template had been replaced. With the application of digital signatures, replacement alone does not suffice for a successful attack because the adversary must also obtain the private key to sign the replaced profile. The security surrounding the key should be greater than that surrounding the biometric package, thereby making this impersonation attack much more difficult to achieve. For instance, the key could be on a hardened server in a secure data center while the biometric template might be on a smart card that could be lost or stolen in any environment.

4.1 Selection of Cryptographic Algorithm

The specifics of the possible cryptographic algorithms and their potential configurations are beyond the scope of this STIG. Nonetheless, the security administrator will activate cryptography when it is available and select appropriate algorithms and key lengths whenever cryptography is employed.

- *(BIO2009: CAT I) The Security Administrator will ensure that the system is encrypted.*

- *(BIO2010: CAT III) The Security Administrator will configure the biometric system to use Federal Information Processing Standard (FIPS) 140-1/2 validated encryption algorithms.*

4.2 Protection of Keys

As with any modern cryptographic system, the security of the system depends upon the keys. The compromise of shared secret or private keys undermines the assurance of anything based on those keys, including – in the case of biometrics – the confidentiality and integrity of biometric templates and live samples, and the non-repudiation of stored biometric packages. In other words, if someone were able to compromise a critical key, that person would probably have the means to bypass the authentication protection that biometrics provides.

There is no standard implementation of cryptography across the spectrum of biometric technologies. Nonetheless, to protect against such an occurrence, the following is required in the DOD-supported computing environment:

- *(BIO2020: CAT II) The Security Administrator will ensure that only the process running biometric software is able to read relevant private or shared secret keys (with the exception of key supersession events during which the Security Administrator may temporarily have the ability to replace the key [e.g., to modify the key file]).*

5. ENROLLMENT THREATS AND CONTROLS

Rapid advances in biometrics will inevitably lead to increasingly accurate and secure biometric technology over time. In this environment, it will become increasingly more difficult for adversaries to breach the verification process and the administrative and cryptographic systems that support it. This means that adversaries are more likely to exploit vulnerabilities in the enrollment process, as this may become the weak link in many biometric implementations.

At its core, the enrollment process establishes a relationship between a user identity and an associated biometric. Consequently, there are two general ways to compromise the enrollment process:

- Start with a false identity
- Associate the identity with a poor biometric template

5.1 Identification During Enrollment

To guard against the false identity threats, an organization must have a high level of assurance in its identification process. Whenever possible, the enrollment process should be conducted in-person by a trained enrollment administrator who would check for valid photo identification and a request form authorized with a verified signature.

Some biometric systems rely on self-enrollment of biometric data. In this case, there must be strong authentication to the self-enrollment system to ensure that the right person is creating the biometric template. The strength of the enrollment authentication required depends upon the risk profile of the environment being protected with biometrics. In no case, however, should the strength of the authentication required in the enrollment process be less than the strength of authentication required during the verification process because this begs for an attack on the enrollment process. For example, suppose an organization protects access to critical Windows servers with a domain logon and a fingerprint (two-factor authentication). The self-enrollment process, however, is controlled by Windows domain authentication only. In this case, an attacker would try to crack the Windows enrollment authentication in order to enter biometric credentials that subsequently could be used for logon to the critical servers because this would be easier than an attempt to beat the two-factor verification process on the critical servers.

- *(BIO3010: CAT II) The IAO will ensure that the enrollment process is conducted by an authorized Enrollment Administrator who will at a minimum check that:*

  - *The enrollee has submitted a completed SAAR DD Form 2875 or similar access authorization form used to authorize access to the system for which the biometric system supports authentication.*
  - *The enrollee is in possession of valid DOD photo identification.*
  - *The photo on this identification matches the physical characteristics of the enrollee.*

- *(BIO3020: CAT I) The IAO will ensure that users cannot self-enroll biometric information (i.e., enroll outside of the presence of an authorized Enrollment Administrator).*

5.2 Creation of Reference Templates

Even in cases in which the enrollment process provides high assurance that the person submitting biometric credentials is indeed the person whose identity will be associated with the template, there is still a significant risk that the generated template would not represent that user. The template submitted may either be too "quiet" or too "noisy", both of which would allow an adversary to pose as an "evil twin" of the individual with the poor template.

An example of a "quiet" template would be if someone spoke very softly when enrolling in a voice recognition system – so softly that the resulting template was effectively a recording of silence. If the system were to allow this, then anyone who remained silent during the verification process might be able to pose as the soft-spoken user. Similar scenarios apply to other biometrics – e.g., poor lighting during enrollment in a facial recognition system might allow null samples during the verification process.

"Quiet" templates are also an issue when the enrollee cannot supply an adequate sample due to an injury or disability. Nearly all biometrics are based on the assumption that all enrollees have the associated human characteristic and that it can be captured or measured. Yet many people do not have fingers or hands or eyes and, therefore, cannot provide anything but a null or "quiet" sample. In the DOD environment, many potential enrollees may have lost these physical characteristics as a result of combat in service of their country, which underscores the need to be sensitive to these cases. The appropriate way to handle them is to offer an authentication alternative that does not pose an undue burden on the enrollee, but not enroll a biometric package if it is likely that someone could exploit any inherent weaknesses and thereby easily impersonate the enrollee.

The problem of "noisy" templates is similar to that of the "quiet" template. Significant movement of the subject during enrollment could allow someone to pose as an "evil twin" by moving suddenly during verification. In these cases, the comparator might accept two blurred samples as a match, when it would have clearly rejected an imposter had the enrollee submitted a more accurate representation of the relevant biometric. Excessive background noise, light or heat during the enrollment process may all introduce a random element into the template that adversaries could exploit at a later time.

If a user has a disability or injury (e.g., a damaged finger or eye) that prevents the generation of a "normal" biometric, then it may be considerably easier to pose as an imposter because there might be a much wider variety of inputs that the biometric system will take as a match for the unusual template. This problem can also occur if the enrollment process is technically flawed. In this case, a "normal" user still may generate a bad template because the capture equipment was not utilized correctly.

To protect against the threat of a poor biometric template, there must be some form of quality control during the initial capture process. Good biometric software will test for the conditions described above and prohibit the creation of clearly inadequately specified templates. Even if this is the case, there is a possibility of a marginal template entering the system (i.e., just good enough to pass quality criteria, but still noisy enough to be susceptible to a sophisticated attack). Whether the biometric software has built-in quality controls or not, the enrollment administrator must be prepared to identify problems with the capture process and re-enroll users who have experienced these problems.

Another related threat is that two people in the system might have a very similar biometric characteristic, which would allow each to pose as the other. In this situation, both individuals may have been enrolled with high quality templates. Therefore, the solution is not to improve the quality of the process. Instead, the enrollment process should include a search through existing templates to determine if there are any matches. This is also a method for discovering whether someone is attempting to enroll twice under two different identities. Fortunately, with most leading biometrics, the probability of two different individuals having the same biometric characteristic is very low, although non-zero. For instance, identical twins still have different retina patterns and fingerprints.

- *(BIO3030: CAT III) The IAO will ensure that Enrollment Administrators receive appropriate training that covers, at a minimum:*

  - *The user identification and authorization requirements*
  - *How to use the biometric software and capture device to obtain an acceptable user template*
  - *How to identify when a template is unacceptable and needs to be recreated*

- *(BIO3040: CAT II) Enrollment Administrators will re-create templates when there is an indication that a template has not been properly captured.*

- *(BIO3050: CAT III) The Security Administrator will configure the system to search for matches between the enrolled template and previously existing templates and reject enrollment when a match is discovered. If this process cannot be automated, the Enrollment Administrator will enforce this requirement manually.*

5.3 Protection of Reference Templates

If an adversary is able to obtain the digital representation of a user's biometric, the adversary can use it to breach that system or even another one that uses similar technology. If an adversary is able to modify a user's biometric template, then the adversary can grant access to "imposters" by swapping the user's template with that of the imposter.

As mentioned, the storage of biometric templates is often outside the control of the biometric software (e.g., templates on a smart card). For this reason, the *Biometric Verification Mode Protection Profile for Medium Assurance Environments*, *see web link in Appendix A*, explicitly excludes template storage from its target of evaluation. Consequently, it is possible for a biometric technology implementation to be based on a Common Criteria validated biometric security product that is appropriately configured, but still have vulnerabilities in its storage component.

- *(BIO4010: CAT II) The Security Administrator will configure the biometric system to encrypt all biometric data resident on non-volatile memory or storage media.*

- *(BIO4015: CAT II) The Security Administrator will ensure biometric templates are protected by operating system permissions.*

- *(BIO4020: CAT II) The Security Administrator will ensure that no user ID has access to the files other than those required for running the biometric application software.*

6. VERIFICATION THREATS AND CONTROLS

Verification is the process that supports routine user authentication. A user seeking physical or logical entry presents a live biometric sample to a capture device, which extracts a digital representation of the sample and transfers it to a comparator. The key threats to this process are as follows:

- Flaws in the comparator that cause it to incorrectly accept false samples as a match.

- Adversaries that present artifacts (e.g., photographs, voice recordings, fake hands, etc.) to the capture device in an attempt to mimic the biometric characteristics of a legitimate user.

- The ability of someone to use a residual image on the capture device or in the biometric software to gain entry under the identity of someone who recently authenticated to the biometric system.

- Adversaries that repeatedly enter live samples in the anticipation that eventually the system will accept one as a match (a threat most commonly associated with behavioral biometrics such as written signatures and keyboard dynamics).

The remainder of this section will address these threats and describe controls that mitigate the risk associated with each of them.

6.1 Verification Process Assurance

6.1.1 False Acceptance Rate (FAR) Configuration

The central risk of the verification process is that the technology will mistakenly verify a user's identity when that person is actually someone else – a phenomena known as *false acceptance*. A key goal of many biometric scientists and software developers is to find algorithms that reduce the rate of false acceptances, but a perfect algorithm is essentially unobtainable because human beings are constantly changing – they age, gain and lose weight, sustain injuries, modify their behavior, etc. All of these phenomena mean that the biometric system must have some tolerance for error. If it did not, then common everyday changes in individuals would lead to *false rejection.*

The trick is balancing the tradeoff between the *false acceptance rate* (FAR) and *false rejection rate* (FRR). A high FAR means that security may be unacceptably weak. A high FRR means that the technology is likely to be a significant nuisance to falsely rejected users, whose subsequent complaints may undermine the long-term acceptance and therefore viability of the technology.

- *(BIO5010: CAT II) The Biometric Security Administrator will set the FAR to be no greater than 1 in 100,000.*

6.1.2 "Liveness" Check

As mentioned, one potential risk is that an adversary will present something other than his own biometric to trick the system into verifying someone else's identity. For example, with a poorly designed facial recognition system, an imposter may simply show the capture device life size photograph of a valid user or, in the case of voice recognition, a tape recording of the valid user's voice. For any biometric, one can devise a potential substitute to mimic the real user, though certainly some biometric characteristics are more susceptible to this than others.

To mitigate this risk, most leading biometric solutions have "liveness" checks that take some action to validate that the sample is coming from a live human being and not a facsimile. For example, the capture device might also test for body temperature or a pulse when reading input. "Liveness" checks should be implemented whenever feasible.

Alternatively, the organization using the biometric system for access control might implement human monitoring of the verification process (e.g., a security guard who can easily notice if someone were to present false credentials such as someone else's photograph or a false hand). This is known as supervision of the verification process. Supervision is not a valid substitute for embedded "liveness" checks because of the potential that the human supervisor could be distracted, corrupted or forcibly removed. Nevertheless, supervision is desirable as a supplement to "liveness" checking. If organizations cannot arrange for human supervision, then they should still perform random spot checks to learn how the biometric technology is used in practice. The mere possibility that human supervision of the verification process might occur on occasion could deter adversaries from attempting to breach the biometric system with a high-quality artifact.

- *(BIO5020: CAT II) The Security Administrator will activate at least one of the available "liveness" checks.*

6.1.3 Residual Image Check

Another potential attack involves using residual data on the reader or in memory to impersonate someone who authenticated to the system earlier. For example, if a valid user leaves his handprint or thumbprint on the capture device, then the next user could possibly submit a blank sample in an attempt to get the capture device to read the residual print that is already on the device.

Similarly, if the attacker gains control of the system, the attacker might be able to use live samples or templates in memory to breach the system. As noted previously, cryptographic methods such as digital signatures can prevent attackers from inserting or swapping biometric data without detection. If, however, the residual biometric data in memory has already been cryptographically validated, then an attacker may be able to use it to gain entry. Although this would be a sophisticated attack, it is an important one to protect against because of its potential to circumvent cryptographic controls.

Most leading biometric technologies have a means of preventing such an occurrence. The best mechanism is to clear all biometric data from memory before initiating another transaction. Another method is to reject consecutive identical samples. This can be effective because the likelihood that a user would submit the exact same biometric reading is very low and indicative of this type of attack.

- *(*BIO5030*: CAT II) The Security Administrator will configure the biometric system to prohibit the identical biometric sample from being used in consecutive authentication attempts.*

6.1.4 Limitation on Unsuccessful Authentication Attempts

As with any technical approach to authentication, the likelihood of a security breach is a function of the number of times an attacker can attempt to bypass technical controls. Therefore, one objective of the biometric system configuration is to limit the number of attempts any user can unsuccessfully attempt to authenticate. As with password-based systems, the system should lock the user out and log a security event whenever a user exceeds a certain number of failed logon attempts within a specified timeframe.

When an adversary tries repeated logon attempts, each attempt provides information (i.e., the credentials supplied either allow entry or they do not). In some cases, the system may provide more information than a simple yes/no answer. It might also reveal how close a match the credentials supplied is to the ones that would permit access. There is inherent variability in biometric samples and an exact match is often a cause for suspicion. Accordingly, all biometric systems rely on some form of scoring. The issue is who should know the score that results from a sample. While there may be a rationale for the audit administrator to have access to this information, under no circumstances should it be revealed to a user. To do so, would give an attacker clues how to modify inputs to increase the probability of a match.

- *(BIO5040: CAT II) The Security Administrator will configure the biometric system to lock out for 15 minutes any user upon the third unsuccessful authentication attempt within a 15-minute period.*

- *(BIO5050: CAT II) The Security Administrator will configure the biometric system to not reveal to a user any information related to how close the live sample he or she supplies is to the corresponding biometric template.*

6.2 Protection Against Bypass and Replay

Bypass is when someone circumvents one or more components of the biometric system, most probably the capture device because it is outside the perimeter of the protected system or area. The attacker might compromise the capture hardware or wiring to send electronic or digital representations of biometric data directly to the comparator without first presenting a sample to the capture device.

Replay is when someone is able to capture a valid user's biometric data and then use it at a later time for authorized access. The attacker may obtain the biometric data from the stored biometric template or as it is being transmitted from one element of the biometric system to another (e.g., the capture device to the comparator).

With the exception of voice recognition systems, replay attacks typically are the follow-on to a successful bypass attack. For example, rather than present a false hand in a hand geometry system, the attacker would learn how someone's hand is translated into an electronic or digital representation of the hand. Then the attacker would bypass the capture device to present the representation to the comparator.

- *(N/A: CAT II) To mitigate the risk of bypass and replay, the IAO will ensure that there is; Adequate physical security, encryption of transmitted data, monitoring and perhaps rejection of "exact matches"*

6.2.1 Physical Security

Physical security is particularly important to biometric systems because the capture device will almost always be outside the boundaries of the area or system to be protected by biometric authentication. Therefore, the trust level of the individuals who can touch and manipulate the capture device is necessarily lower than the trust level of those that the system authenticates. This creates a situation in which less-trusted individuals might be able to tamper with and perhaps bypass the capture device.

One possible strategy to mitigate this risk is to have some form of physical access control *prior* to reaching the capture device. For example, one might have to present a swipe card to enter an anteroom that contains a biometric capture device. Combining two-factor authentication with this form of layered physical security offers a high level of assurance. Another approach is to have human guards monitor the biometric capture device, either directly or through video cameras.

- *(N/A: CAT II) The IAO will ensure that the physical connections between the following biometric system components are adequately secured.*

  - *The connection between the capture device and the comparator*
  - *The connection between the comparator and the portal*

Adequate security depends upon what is being protected and the risk environment, but it, at a minimum, involves ensuring that no wiring is exposed to unauthenticated users and there is no means of opening the capture device with the use of common tools such as a screwdriver.

6.2.2 Cryptography

As discussed in *Section 4*, cryptography can greatly reduce the risk of replay attacks because attackers must be able to obtain the system's private key in addition to breaching the security of the capture device or biometric storage. This makes these attacks considerably more difficult to achieve.

In many cases, the appropriate use of cryptography will greatly reduce this threat. If in the fingerprint example above, the electronic representation of the fingerprint would need to be digitally signed for the comparator to accept it, then the attacker would also need to be able to manipulate the signature mechanism.

- *(2009: CAT II) The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric data before it is transmitted from one physical device to another.*

- *(4010: CAT II) The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric data resident on non-volatile memory or storage media.*

6.2.3 Exact Matches

An “exact match” occurs when the digital representation of the live sample extracted from the capture device is identical to the stored biometric template to which it is compared. In most applications, an exact match is a good thing, but in biometrics, it is cause for suspicion. There is inherent variability in the sample capture process that makes exact matches unlikely for many biometric technologies. When one occurs, it may be indicative that someone has improperly obtained the biometric template and is staging a replay attack.

A potential solution is to reject exact matches, thereby requiring the user to provide another sample. If the user is a valid one, then the variability in the sample capture process should lead to something other than an exact match on the second authentication attempt. On the other hand, if the user is an imposter who is in possession of the signed reference template only, then it may be difficult for the imposter to produce a different sample on the second attempt.

Despite the problem associated with exact matches, rejecting them may not be an appropriate strategy. Depending upon the specific capture and extraction technology in place, some biometric solutions may experience considerably more exact matches than others. Rejecting exact matches in these circumstances would be a nuisance. In addition, depending upon the technology, it may be relatively easy for an adversary to enter a small amount of noise in the sample to avoid an exact match but still be close enough for acceptance. In this environment, determining the difference between a true live sample and a replay attack is extremely difficult.

6.3 Risk Management of the Verification Process

The appropriate level of assurance that should accompany biometric systems depends largely upon the risk environment in which the technology is implemented. When determining how strong the biometric security controls should be, the IAO should consider the following three concerns:

- The value of the assets being protected
- The relative accessibility of biometric system components to adversaries
- The strength of other elements of the authentication process

The first one is common to all information assurance efforts. Biometrics that protect highly sensitive information about current military operations require higher levels of assurance than biometrics that protect phone numbers stored on a Personal Digital Assistant (PDA).

The second is more targeted to authentication systems. If the biometric system supports physical access to a military installation in a foreign country with known terrorist activity, then it must operate at a higher level of assurance than the biometric system that supports access to a device located in a secure server room that is itself in a secure facility. This is the case regardless of the assets being protected. Issues to consider in this regard are how many people can reach the capture device, how trusted are these individuals, and to what extent are the capture device and other components subject to tampering. In general, the assurance requirements for the biometric system increase as the level of trustworthiness in those with accessibility to the biometric system declines.

The final concern addresses the criticality of biometrics relative to other factors in the authentication process. Biometric systems that are integrated into a three-factor authentication solution can operate at a lower level of assurance than those that stand alone as the only means of authentication. In the first case, there is already a high degree of confidence that the user is valid if that user can present two of the three factors. In this case, biometrics serves as “icing on the cake” – false acceptances would not likely jeopardize security. In the second case, false acceptance means unauthorized access and, thus there is a greater need to make sure the biometric system is functioning properly.

Based on an assessment of these risk components, the IAO may be able to adjust the FAR/FRR and the strength of “liveness” checks to the extent these parameters are configurable.

7. FALLBACK THREATS AND CONTROLS

Fallback is the condition that occurs when the biometric system is not in use. There are three general fallback scenarios:

- Service disruptions
- Special users (i.e., those unable to present the biometric due to temporary injury or permanent disability)
- Override of the biometric technology (e.g., when someone provides access control to a user that is believed to be have been falsely rejected)

7.1 Fallback During Service Disruptions

Although biometric systems are expected to be available at all times, a proper implementation of biometrics must consider the case in which the biometric system fails to function. In this case, the system must *fallback* to an authentication alternative. Determined adversaries are likely to study the relative gap between the biometric system and its fallback alternative to determine whether it is easier to breach the biometric system or conduct a denial of service attack on the biometric system and then breach the fallback mechanism.

Consider a case in which a server room is protected by a turnstile that requires a swipe card, Personal Identification Number (PIN) and retina scan for entry (i.e., three-factor). Under one scenario, fallback might still require the swipe card and associated PIN (two-factor). Under another scenario, fallback might involve a manual badge check (single factor with no on-line check for badge revocation). Certainly, the first scenario offers much better protection than the second.

If, however, the biometric system was a replacement for the swipe card and PIN technology, then there may be no choice for the organization but to implement the second fallback scenario – the manual badge check. Consideration of the fallback contingency is one reason why biometrics should be part of a two-or three-factor solution.

- *(BIO6020: CAT II) The IAO will establish adequate identification and authentication procedures that must be followed whenever the biometric system is unavailable.*

- *(BIO6010: CAT II) The IAO will ensure that biometric technology is not the sole means of access control (i.e., it will be one component of a two or three-factor authentication solution or it will be accompanied by a automated fallback verification system).*

7.2 Fallback for Special Users

For any given biometric technology, there will be users unable to present the required live biometric sample – people unfortunately lose hands, eyes, the ability to speak, etc. In some cases, the loss of functionality may be temporary – a severe cut on a finger, an eye disease that requires the application of a patch for a period of time, a hand injury that prevents the user from writing or typing as he or she would normally, etc. Unfortunately, any fallback scheme provides a means for an imposter to circumvent the biometric technology. For example, someone with a close resemblance to the user may steal a user's badge and show up with an eye patch or cast to avoid use of the biometric technology that would likely detect the impersonation.

In these situations, the organization must provide some alternative to the biometric system for authentication, but – as with service disruptions – the key is to provide a fallback authentication scheme that still maintains an adequate level of assurance. One method is to introduce a second factor in the authentication process not present in the usual process. For example, if biometrics is coupled with a user name and password, then special users might be allowed to present a token or smart card in lieu of the biometric. Similarly, if biometrics is coupled with a smart card or token, then the special user might be allowed to enter a password or PIN in lieu of the biometric. If feasible, the authentication should be supervised to guard against improper manipulation.

In some cases, the biometric technology provides partial fallback mechanisms within the system itself. For example, users might enroll both thumbprints and use the right thumbprint for day-to-day verification. If the right thumb is unavailable for any reason, then the user may fallback to the left thumb. These approaches should be employed whenever feasible.

- *(*BIO6030*: CAT II) The IAO will establish adequate written identification and authentication procedures for users that are unable to present the required live biometric sample.*

7.3 Override

Many biometric implementations suffer from a high FRR. When false rejections occur too often, authenticated users are likely to treat any rejection as a false one and override the system to permit access to the rejected individual. This might be something as simple as opening a door for someone who shows a badge and claims that the system is not working. Unfortunately, if an adversary learns of this informal practice, the primary attack strategy is likely to involve a claim of false rejection rather than a more sophisticated approach. When assertions of false rejections become a credible excuse for circumventing the authentication system, biometrics becomes a security threat rather than an enhancement. For this reason, biometric systems must be accurate to be useful.

Inevitably, there will be some false rejections that require intervention to allow proper access (e.g., the recently injured user). Yet the determination of what constitutes a false rejection should not be left to ordinary users.

- *(BIO6040: CAT III) The IAO will designate personnel who have the authority to override false rejections and ensure that they receive proper training in how to implement the fallback protocol and verify a user's identity.*

- *(BIO6050: CAT II) The IAO will ensure that any override of the biometric system is accompanied by a photo ID check of the user and documentation of the following:*

  - *The name of the user who was granted entry with the override*
  - *The time the override occurred*
  - *The reason for the false rejection*

- *(BIO6060: CAT II) The Biometric Security Administrator will set the FRR to be no greater than 5 in 100.*

This page is intentionally left blank.

8. MONITORING AND AUDITING THE BIOMETRIC SYSTEM

Auditing for biometrics is as critical as it is for any other information system. Audit logs assist with intrusion detection as well as general troubleshooting. Investigations of information security incidents would be nearly impossible without them.

Ideally, audit systems should be accompanied by an appropriate separation of duties. The security administrator may be able to read the audit log, but should not be able to modify or delete log entries, a role that should be left to an audit administrator. This prevents a malicious security administrator from concealing unauthorized changes to the security configuration or access attempts. If separation of duties is not possible due to resource shortages or organizational structure, then the IAO should ensure that logs are regularly copied to a backup storage medium to which the security administrator does not have write or delete permissions.

In some biometric systems, there may be an option to log a "closeness score" – i.e., a metric that measures the level of similarity between the biometric template and the captured biometric sample. In a proper separation of duties, the security administrator should not be able to view this information because it would provide information on how adjustments to the security parameters might impact the authentication mechanism. For example, if a malicious security administrator could detect that a co-conspirator's biometric had a very close match to another user of the system, then he could adjust the FAR slightly upward to permit the co-conspirator access.

This problem does not arise if the system is configured to log exact matches, but not the quantitative closeness metric. As mentioned, exact matches are evidence of a potential replay attack. In this circumstance, someone may have circumvented the capture device and be transmitting a digital representation of the biometric template. The audit system should record these events in order that this type of behavior may be identified.

It is not feasible to provide specific security guidance for audit log security given the wide variety of potential technologies involved in a biometric deployment. Nevertheless, one can establish a relative standard that requires that biometric audit logs be at least as secure as other logs in that environment.

- *(BIO7010: CAT II) The IAO will ensure that the file permissions and storage scheme for biometric audit logs is no less secure than the scheme for the system audit logs of the operating system on which the biometric software resides.*

- *(BIO7020: CAT II) The Security Administrator will configure the biometric system to audit the following transactions:*

  - *All "exact match" verification transactions*
  - *All failed identification or authentication attempts*
  - *All start and stop events for the biometric service*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

DOD Biometrics Management Office (BMO), *Biometric Verification Mode Protection Profile for Medium Robustness Environments*, Version 0.7, March 2003.

DOD Directive 8500.1, Information Assurance, 24 October 2002.

Computer Security Act of 1987, Public Law 100-235, 8 January 1988.

This page is intentionally left blank.

APPENDIX B. INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

This appendix will list all IAVM bulletins that are uniquely applicable to Biometric systems or applications. There are no applicable IAVM Bulletins at this time. It is strongly recommended that each IAO regularly browse the DOD-CERT web page (http://www.cert.mil) for possible newly published bulletins.

This page is intentionally left blank.

APPENDIX C. LIST OF ACRONYMS

BMO	Biometrics Management Office
C&A	Certification and Accreditation
CDE	Common Desktop Environment
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSN	Defense Switched Network
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
FIPS	Federal Information Processing Standard
FSO	Field Security Operations
IAO	Information Assurance Officer
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IT	Information Technology
OS	Operating System
PDA	Personal Digital Assistant
PIN	Personal Identification Number
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
STIG	Security Technical Implementation Guide
VCTS	Vulnerability Compliance Tracking System
VMS	Vulnerability Management System