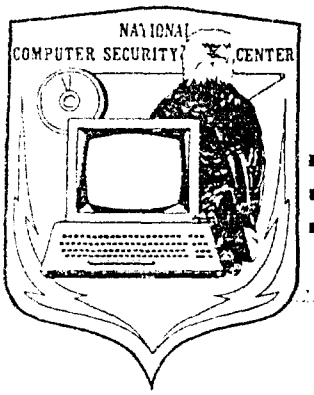


NATIONAL COMPUTER SECURITY CENTER



# FINAL EVALUATION REPORT OF IDENTIX, INC. IDX-50

## VERSION 7



1 February 1988

Approved For Public Release:
Distribution Unlimited

# SUB-SYSTEM EVALUATION REPORT

# IDENTIX, INC.

# IDX-50 VERSION 7

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

February 1, 1988

CSC-EPL-88/001
Library No. S230,456

This page intentionally left blank.

# FOREWORD

This publication, the Sub-system Evaluation Report, IDENTIX, Inc., IDX-50 Version 7, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the evaluation of IDENTIX's IDX-50. The requirements stated in this report are taken from Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985.





Approved:

February 1, 1988

Eliot Sohmer
Chief, Computer Security Evaluations, Publications, and Support
National Computer Security Center

## ACKNOWLEDGEMENTS

### Evaluation Team Members

Stephen F. Carlton
Myron M. Coplin
John L. Wyszynski

### Further Acknowledgements

James L. Arnold
Ronald J. Bottomly

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

## CONTENTS

This page intentionally left blank.

## EXECUTIVE SUMMARY

IDX-50(1) Version 7, has been evaluated by the National Computer Security Center (NCSC). IDX-50 is considered to be a security sub-system rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. Specifically, the features included in this evaluation were Identification and Authentication (I&A) and Audit of the I&A.

The NCSC evaluation team has determined that the IDX-50 can apply these features to any host system which provides the ability to accept I&A information from the IDX terminal. The host must be able to make access decisions based on the information received and create an audit trail from the information. The host software which provides these features must be protected from modification by users. The IDX-50 system does not include any host software.

IDX-50 supplies the I&A information based on a comparison made between a user's fingerprint and a record, stored on a smart card, which represents the user's fingerprint. The result of this comparison (either confirmed or denied) is sent to the host system.

---

(1) IDX-50 is a registered trademark of the IDENTIX Corporation.

This page intentionally left blank.

# INTRODUCTION

## Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems: systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

## The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the TCSEC. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

## PRODUCT EVALUATION

### Product Overview

IDX-50 is a security product which uses biometrics to provide user Identification and Authentication (I&A) information to a host computer and the capability for the host to audit the I&A. It is comprised of a stand-alone terminal, a smart card for every user of the system, and a key to turn on the terminal. For IDX-50 to be used as an effective I&A mechanism, the host computer must provide software which is capable of reading the I&A information sent from the IDX-50 terminal (via an RS-232 connection) and granting or denying access based on that information. The host must have the ability to protect this software from modification. The evaluation of the IDX-50 did not examine any host software.

The front of an IDX-50 terminal has a liquid crystal display, card slot, keypad, and scanning lens. The display is used for prompts, queries, and status information. A user inserts his smart card into the card slot during authentication and enrollment. The keypad is used for user responses to terminal queries. It contains the numbers zero through nine and two additional keys "YES/FN" and "NO/CLR". The scanning lens is used to examine a person's fingerprint during enrollment and verification.

The rear of the IDX-50 terminal has a key switch, two serial ports (labeled AUX and MAIN), and a door relay output port. The key switch is used to turn the terminal on. The serial ports are used to send, to the attached host system, information concerning every transaction that takes place on the terminal. The two ports are functionally equivalent, with the exception that the port labeled MAIN sends internal diagnostic messages along with the I&A information. The AUX port should be used to send the information to the host computer while the MAIN port could be used to send the information to a printer for an audit of all transactions that take place on the terminal. The door relay output port can be used to control the access through an electronically controlled door. This feature of the IDX-50 was not evaluated.

Every user of the system must have the smart card with which he was enrolled in order to be authenticated. A smart card is about the size and shape of an ordinary credit card and contains memory on an embedded chip. It is used during the verification process and contains authentication data pertaining to the user to whichhe card was assigned. This data includes the fingerprint record and the

Personal Identification Number (PIN) of the user. A smart card can not be reprogrammed after a fingerprint record has been enrolled on it. If it is desired to change a user's PIN, a new card would have to be enrolled.

All users of the IDX-50 are given an authorization level when they are enrolled. The three authorization levels defined by IDX-50 are USER, ENROLLER, and MANAGER. A person with USER authorization can only use the IDX-50 to go through the normal verification process. A person with ENROLLER authorization has the additional privilege to enroll other users or enrollers on the IDX-50. He can not enroll managers. A person with MANAGER authorization has ENROLLER privilege plus the additional privilege to delete users, modify system parameters, and enroll additional managers.

Enrollment is the process by which information about a particular user is written to a smart card. That card becomes the user's key to being authenticated by the IDX-50. The user's authorization level, authorized access locations, expiration date, PIN, and fingerprint record are stored on the smart card. The system will assign for that user a unique serial number which will be a part of the data that is sent to the host during authentication. The serial number is comprised of the number of the terminal on which the user was enrolled, the enrollment date, and the enrollment time.

Only a user that has MANAGER authorization can invalidate users of the IDX-50 system. Deletion of users falls into one of three categories:

1. Automatic deletion.

2. Deletion with card present.

3. Deletion without card present.

The automatic deletion function is invoked if the card expiration date, specified at enrollment time, is exceeded. The user will no longer be able to pass the verification process after 12:00:01 A.M. on the morning of the specified expiration date. To deactivate a card in his possession, the manager enters the "delete card" function of the terminal and inserts the card to be invalidated when requested. The terminal will mark the card invalid and it cannot be used again. To deactivate a card that is not in his possession, the manager must use the "delete list" function of the terminal. The serial number of the user whose card is to be deactivated is entered into a list of cards that are to be deac-

tivated. The list may contain up to forty serial numbers. The next time the card is presented to that terminal for verification, the card will be invalidated and the user will not be verified.

A user with MANAGER authorization can modify any of the following IDX-50 system parameters:

1. DATE AND TIME: The date and time for this terminal.

2. SYSTEM NUMBER: A number between 00000 and 50000. All terminals at an installation have the same system number. This number prevents a user at one installation from accessing a machine at another installation.

3. NODE NUMBER: A two-digit number that identifies the terminal. Every terminal at an installation must have a unique node number.

4. ENROLLMENT TERMINAL: Status which indicates whether the terminal may perform enrollments.

5. NUMBER OF PRINTS FOR ENROLLMENT: A number from three to five which indicates the number of finger scans that will be used to create the fingerprint record when a user enrolls. The default value is five.

6. PIN REQUIRED: Status which indicates whether a PIN will be required when a user attempts to be verified to the machine.

7. PIN LENGTH: A number from one to nine which indicates the number of digits in a PIN. If the PIN length is decreased, existing users can be verified by using the first n digits of their PIN (where n equals the new PIN length). However, If the PIN length is increased, users enrolled with a shorter PIN must be re-enrolled with new cards. The default value is four.

8. RELAY DURATION: A time period between 0 and 25 seconds that the door relay signal is in effect after identity confirmation. (Not relevant for this evaluation)

9. RELAY DELAY: A time period between 0 and 25 seconds that the terminal will wait before activating the door relay signal. (Not relevant for this evaluation)

10. NUMBER OF TRIES TO VERIFY: The number of times the terminal will attempt to verify a finger before requiring the user to re-enter his PIN. This number is between one and three. The default value is three..

11. THRESHOLD: A number between 0 and 200 that indicates how well a user's fingerprint must match the template that is on the card before being accepted as identical. The higher the threshold, the closer the match must be for a positive authentication.

## Evaluation of Functionality

The team has determined that the IDX-50 can be used to provide information to a host system for I&A and audit of the I&A.

## Identification and Authentication

The IDENTIX IDX-50 is designed to connect with either a host computer or other device and provide I&A and audit information. This information is based on each transaction that takes place at the IDX terminal. When the IDX-50 is connected to a host computer, the host is responsible for making access decisions based upon the information received from the IDX terminal.

To be authenticated by the IDX-50 the user must be enrolled and must follow the IDX terminal's verification process shown below:

1. The user must insert his smart card into the terminal's card reader.

2. The correct PIN must be entered into the IDX-50 (if the manager has configured the terminal to require a PIN).

3. The terminal will prompt the user to place his finger on the scanning lens and scan the finger.

4. Identity is either confirmed or denied.

5. The terminal prompts the user to remove his or her card.

Identification is not confirmed if a user enters an invalid smart card, PIN number, or finger print.

In order to use the IDX-50 all users are required to enroll their fingerprint record on a valid smart card using the terminal. There are three possible authorization levels that give some users more privilege than others. The possible authorization levels are USER, ENROLLER, or MANAGER

.In order to start to enroll users onto the IDX-50, a manager or enroller must set the system to system mode. To accomplish this a manager or enroller would press the "YES/FN" button before verifying himself to the terminal. After the IDX-50 verifies the person as a manager or an enroller, the terminal will go to system mode. Once the IDX-50 is in this mode, a manager can enroll users, change system parameters, and delete users. An enroller can only enroll users.

The first time that the IDX terminal is used, the same procedure to get to system mode would be followed (as described above), except a non-enrolled (blank) smart card is used instead of an enrolled card; there is no verification process used; and the first enrollee is given manager privileges. This exception occurs only on the first enrollment. Since the first person to be enrolled is given MANAGER privilege, it is imperative that a manager is the first enrollee.

Once in system mode the terminal would display the following menu:

SYSTEM MODE

1-ENROLL 2-DELETE
3-MANAGER NO-QUIT

The enroller would select enrollment and proceed through the following steps:

1. Enter the new user's PIN

2. Select whether the enrollee is to be a manager, enroller, or user.
   NOTE: (Enrollers can only enroll other enrollers or users.
   Managers may enrol managers, enrollers, or users).

3. Select the terminals which can be accessed by the user.

4. Designate the smart card as either permanent or temporary. If temporary is selected, the enroller will be prompted for an expiration date.

5. The enrollee's finger is requested for scanning to be utilized in creating the fingerprint template.

6. The terminal will prompt the user for 3 to 5 more scans, depending upon whatever the manager has set that system parameter to.

7. When all of the necessary scans have been taken, the terminal will give a quality rating of the template.

8. The system will display all of the enrollment information and the serial number of the card (this number should be noted because it is used to deactivate the card).

9. All of the information entered is then written onto the card.

In order for a host computer to use the IDX-50, the host must be capable of making access decisions based upon the information received from the IDX terminal. The format of that information is as follows:

```
01/01/87 13:38:35 01 VERIFICATION CONFIRMED 21-122893-21821
```

Where:

1. 01/01/87 = transation date

2. 13:38:35 = transaction time

3. 01 = terminal node identification

4. VERIFIC... = transaction result

5. 21-1228... = user serial number

The IDX-50 will send this type of information for each transaction that takes place at the terminal.

Audit

The IDX-50 does not maintain actual audit logs. However, the host can maintain an audit log of each transaction that takes place on the IDX-50 by using the information it receives from the IDX terminal. The host can use and maintain the audit log, if it is connected to the terminal's RS-232 port with the following protocol:

| BYTE # | FIELD DESCRIPTION |
|---|---|
| 01-08 | Transaction Date |
| 10-17 | Transaction Time |
| 18 | Blank |
| 19-20 | Terminal Node Number |
| 21 | Blank |
| 22-62 | Transaction Result |
| 63 | Blank |
| 64-79 | User Serial Number |
| 80-81 | Carriage Return, Line Feed |

The terminal will provide audit information for every type of transaction that occurs. The possible types of transactions are identity and enrollment. The format of each of these types of transactions is the same as the Verification transaction shown in the I&A section. When the system is verifying identity, the team found five possible audit transactions (shown below):

1. verification denied: The user's identity was not confirmed
2. verification accepted: The user's identity was confirmed
3. verification incomplete: The user did not complete the verification process

4. invalid card: The user was using a card that was not formatted correctly

5. verification authority denied: A user with USER authorization was attempting to go into system mode

As shown below the audit transaction for enrollment is about the same as the verification transaction.

```
01/01/87 13:23:23 00 ENROLLMENT SUCCESSFUL QUALITY A 00-3473...
```

Where:

1. 01/01/87 = Date enrolled

2. 13:23:23 = Time of enrollment

3. 00 = Node

4. ENROLL... = Enrollment transaction result

5. QUALITY A = The quality of the enrollee's finger print template

6. 00-3473... = User ID

During enrollment the enrollment transaction result and quality can vary depending on the outcome of the enrollment. The possible entries for enrollment result are:

1. ENROLLMENT SUCCESSFUL

2. ENROLLMENT FAILS

3. ENROLLMENT INCOMPLETE

The possible entries for the quality rating are:

1. Quality A: An excellent enrollment
2. Quality B: An average enrollment
3. Quality C: A fair enrollment.

## Evaluation of Documentation

The IDX-50 documentation consists of one guide, the Operations Guide for the IDX-50 Personal Verification Terminal, 1987, IDX-50 Firmware Version V-C-03 and later, Release 1.2. This document describes in great detail the operations and security features provided by the IDX-50. The team found the document to be lacking a complete list of possible transactions that a host could expect. Otherwise, the document contained the necessary information to install and use the IDX-50.

## Operations Guide for the IDX-50 Personal Verification Terminal

This document is intended for managers, installers, and operators of the system. The following sections are included:

Section 1 - Setting up - This section is a basic introduction to the IDX-50 system. It includes a description of the hardware, installation instructions, and verification of correct operations.

Section 2 - Getting Acquainted - This section describes the basics of biometrics identity and identix smart cards. A description of general IDX-50 use and management are also covered in this section.

Section 3 - Enrollment - The third section provides information about enrolling users on the IDX-50. It also covers authority levels, access lists, and Personal Identification Numbers (PINs) Instructions on correct finger placement are also included in this part.

Section 4 - User Verification - The IDX-50's normal operations for user verification are covered in this section. In addition, possible error conditions, user problems, and transaction logging are discussed.

Section 5 - Deleting Users - Methods of invalidating users are discussed.

Section 6 - Problem Determination and Repair - This Section is a trouble shooting guide to the IDX-50. It also provides information on how to send a unit back to the factory for repair.

Section 7 - System References - Information about system specifications and protocols is provided in this section.

Section 8 - IDX-50 Wall-Mount Units - This section shows how to mount and set up the IDX-50W (Wall Mount Version of the IDX-50).

## THE PRODUCT IN A TRUSTED ENVIRONMENT

A growing concern in computer security has been in the level of assurance found in Identification and Authentication methods.

The traditional password mechanisms have changed very little since they were first introduced in the early days of computer systems. Passwords suffer from vulnerabilities because they can be easy to determine, and their compromise is not easily detected. The solution has normally been to improve the management of these passwords to reduce the possibility of duplication. The scope of these techniques is covered by the Department of Defense Password Management Guideline (CSC-STD-002-85).

Recent years have seen the introduction of a devices which are familiar to most people as automatic bank teller cards. Installing such a card system onto a computer system can offer a higher level assurance in that such cards are not easily duplicated. While cards could be duplicated, physical compromise of the card is usually necessary for this. Good management of the cards makes physical compromise easy to detect. If the data on the card is just guessed, the fabrication of cards would prove too costly as a hacking technique. Still a determined intruder with resources and knowledge of the system being attacked might overcome these obstacles.

Prior approaches to this problem suffer from a flaw which, until very recently, was not economically feasible to solve on most systems. The identification of the person was not tied to a unique characteristic of the individual in question; the identity could easily be passed to another individual. The class of devices which hold the promise of correcting this are called biometrics. Biometric devices measure some characteristic of an individual, which is checked for by matching against the known version of the characteristic. Common characteristics used are fingerprints, eye retina patterns, and signatures because they are easy to obtain and are unique by nature.

The IDX-50 can provide additional assurance to I&A mechanisms of a system when incorporated into the system in a secure manner. Several areas must be covered in bringing this about. The most important thing to consider is proper enhancements to the I&A mechanism already on a system to incorporate the identification data issued by the IDX-50. The system's I&A mechanism must be able to handle any of the possible messages received. To prevent the possibility of forging the smart cards, the serial numbers which are associated with IDX-50 users are to be considered passwords.

passwords and treated as such (i.e. they are to be protected in a manner which complies with the TCSEC for passwords). To provide the greatest confidence in the authentication process, the NCSC team recommends against removal of passwords in favor of the IDX-50. Rather it should be used as a supplement to the existing password mechanism.

Configuration of the IDX-50 operational parameters is flexible. However, two directly affect the amount of assurance one can place in the system. The team believes the threshold should be set at or above 120 and PINs should be enabled.

The installation of the IDX-50 requires that physical measures are taken to insure the integrity of the data the host receives. It is important that the connection between the IDX-50 and the host system is secured and tamper-proof. The information which is passed to the host computer can be simulated if the cable can be tapped into.

Also, to prevent someone from forging a card, good card management must be considered. All cards should be accounted for at all times. Any card which is missing should be reported and removed from the system immediately.

After a unit is properly set up, there should be little need for the manager to intervene in any manner except in the maintenance of card enrollments.

# PRODUCT TESTING

## Test Procedure

Testing represents a significant portion of a sub-system evaluation. The testing performed was primarily functional in nature; the security relevant characteristics of the product were compared against the claims of the vendor. The functional test suite of this product focused primarily on identifying Type I and Type II errors. A Type I error is one in which a user is not authenticated when he should have been and a Type II error is when a user should not be authenticated and is. In addition, the product was tested to assure that it worked as claimed in the vendor documentation (e.g., add and delete users, a person with enroller privilege could not enroll a manager, etc.). Also, some attempts were made to spoof an authorized fingerprint.

For this evaluation the IDX-50 was configured with the relevant system parameters set as follows:

1. ENROLLMENT TERMINAL = Yes
2. NUMBER OF PRINTS FOR ENROLLMENT = 5
3. PIN REQUIRED = Yes
4. PIN LENGTH = 4
5. NUMBER OF TRIES TO VERIFY = 1
6. THRESHOLD = 120

The IDX-50 should be configured to require a PIN (the length should be at least four) and have a threshold of no less than 120 to give increased assurance that a Type II error will not occur. The threshold represents how well a fingerprint must match the template in order for the user to be verified.

Test Results

The test results described below are basically oriented towards providing the evaluation team's findings concerning the strengths and weaknesses of each security relevant feature provided by IDX-50.

First, individuals were tested for Type I errors. We found the acceptance rate for individuals varied from 77.5% to 100%, with the average at 92.1%.(1)

We then tested for Type II errors using incorrect fingers. We used both the fingers of other test members and other fingers of the same test member. We were able to produce no such errors at the team's recommended threshold. Type II error testing continued by using wrong PINs, chosen at random. No errors were produced doing this.

The team attempted to produce a counterfeit finger in an attempt to spoof the IDX-50 into recognizing it. Commonly available materials were used to produce some close approximations to an actual finger, retaining the same surface characteristics. The team was unable to produce a finger which the machine would confirm.

The team also tested the administrative functions of the IDX-50 and found that they worked in the manner described in the documentation.

---

(1) It should be noted that the user would not have to go through the entire verification cycle for each Type I error if the NUMBER OF TRIES TO VERIFY parameter is increased to three.

# REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>UNCLASSIFIED | 1b. RESTRICTIVE MARKINGS<br>NONE |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>DISTRIBUTION UNLIMITED |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S)<br>CSC-EPL-88/001 | 5. MONITORING ORGANIZATION REPORT NUMBER(S)<br>S230,456 |
| 6a. NAME OF PERFORMING ORGANIZATION<br>National Computer Security Center<br>6b. OFFICE SYMBOL (If applicable)<br>C12 | 7a. NAME OF MONITORING ORGANIZATION |
| 6c. ADDRESS (City, State, and ZIP Code)<br>9800 Savage Road<br>Ft. George G. Meade, MD 20755-6000 | 7b. ADDRESS (City, State, and ZIP Code) |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>8b. OFFICE SYMBOL (If applicable) | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER |
| 8c. ADDRESS (City, State, and ZIP Code) | 10. SOURCE OF FUNDING NUMBERS<br>PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO. |

11. TITLE (Include Security Classification)

(U) Sub-system Evaluation Report on IDENTIX, Inc. IDX-50, Version 7

12. PERSONAL AUTHOR(S)

Stephen Carlton, Myron Coplin, John Wyzynski

| 13a. TYPE OF REPORT | 13b. TIME COVERED | 14. DATE OF REPORT (Year, Month, Day) | 15. PAGE COUNT |
|---|---|---|---|
| Final | FROM _____ TO _____ | 1 February 1988 | 24 |

16. SUPPLEMENTARY NOTATION

| 17. COSATI CODES | | | 18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | NCSC TCSEC I&A IDENTIX, Inc. IDX-50 identificaiton authentication biometrics |
| | | | |
| | | | |

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

IDX-50 is a security product which uses biometricsto provide user authentication to a host computer. IDX-50 supplies the informa.ion based on a comparison made between a user's fingerprint and a record, stored on a smart card, which represents the user's fingerprint. The result of this comparison (either confirmed or denied) is sent directly to the host system. The IDX-50 is comprised of a stand-alone terminal and a smart card for every user of the system.

This report documents the findings of the evaluation.

| | |
|---|---|
| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT<br>☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS | 21. ABSTRACT SECURITY CLASSIFICATION<br>UNCLASSIFIED |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>LTC Lloyd D. Gary, USA | 22b. TELEPHONE (Include Area Code)<br>(301)859-4458<br>22c. OFFICE SYMBOL<br>C/C12 |

DD Form 1473, JUN 86 *Previous editions are obsolete.*