



Technical Report 08-04
March 2008

Results of a Pilot Test of the FBI Civil Fingerprint File

Kelly R. Buck
Howard M. Timm
Defense Personnel Security Research Center

Donald Linder
Deanna Sanner
Chad Rhoades
Teresa Kipp
Federal Bureau of Investigation/Criminal Justice Identification Services Division

Results of a Pilot Test of the FBI Civil Fingerprint File

Kelly R. Buck, Howard M. Timm
Defense Personnel Security Research Center

Donald Linder, Deanna Sanner, Chad Rhoades, Teresa Kipp
Federal Bureau of Investigation/ Criminal Justice Identification Services Division

Released By – James A. Riedel

BACKGROUND

The events of September 11, 2001, emphasized the importance of having secure means of vetting the identities of individuals who apply for government-issued credentials or access to sensitive government facilities, information systems, or classified information. The Federal Bureau of Investigation (FBI) and the Defense Personnel Security Research Center (PERSEREC) formed a joint team to explore the feasibility and effectiveness of using the FBI's civil fingerprint repository for identity vetting. Findings from this effort establish the value of further development of this valuable resource.

HIGHLIGHTS

Civil fingerprint file searches can identify individuals whose fingerprints have been submitted to the FBI for multiple purposes. For example, fingerprints could be submitted for immigration purposes and then later for civilian employment or security clearance. Therefore, individuals who misrepresent their citizenship and/or immigration history would be detected. Additionally, individuals who submit applications using different names, places of birth, dates of birth, and physical characteristics from what are already in the FBI civil file from prior applications can be detected.

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>					
1. REPORT DATE: (12-03-2008)		2. REPORT TYPE Technical Report 08-04		3. DATES COVERED (From – To) June 2005 - March 2008	
4. Results of a Pilot Test of the FBI Civil Fingerprint File		5a. CONTRACT NUMBER:			
		5b. GRANT NUMBER:			
		5c. PROGRAM ELEMENT NUMBER:			
6. AUTHOR(S) Kelly R. Buck, Howard M. Timm, Donald Linder, Deanna Sanner, Chad Rhoades, Teresa Kipp		5d. PROJECT NUMBER:			
		5e. TASK NUMBER:			
		5f. WORK UNIT NUMBER:			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497		8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: Technical Report 08-04			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497		10. SPONSORING/MONITOR'S ACRONYM(S): PERSEREC			
		11. SPONSORING/MONITOR'S REPORT NUMBER(S): 08-04			
12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited					
13. SUPPLEMENTARY NOTES:					
14. ABSTRACT: This study examined the feasibility of using the Federal Bureau of Investigation civil file for purposes of detecting identity fraud. A pilot test was conducted using fingerprints and other identifying information for 1,143 military applicants who processed through the Los Angeles Military Entrant Processing Station between December 2004 and May 2005. The FBI search attempted to match fingerprints from these applicants against their Civil File. Results demonstrated that FBI civil fingerprint file searches can identify individuals whose fingerprints have been submitted to the FBI for multiple purposes. For example, fingerprints could be submitted for immigration purposes and then later for civilian employment or security clearance. Therefore, individuals who misrepresent their citizenship and/or immigration history would be detected. Additionally, individuals who attempt to submit different names, places and dates of birth, and physical characteristics than are on file with the FBI will be detected					
15. SUBJECT TERMS:					
16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES: 31	19a. NAME OF RESPONSIBLE PERSON: James A. Riedel, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-657-3000
Standard Form 298 (Rev. 8/98) Prescribed by ANSI td. Z39.18					

PREFACE

In the wake of 9-11, greater emphasis has been placed across the U.S. government on developing more secure means of vetting the identities of individuals applying for access to federally controlled facilities, information systems, and classified information. Traditional vetting entails fingerprint-supported checks of the Federal Bureau of Investigation's (FBI) criminal file. For this study, PERSEREC and the FBI collaborated to explore options for use of the FBI's civil fingerprint file to corroborate the identities of individuals who do not have criminal records. The results of this effort demonstrate the potential value of tapping into this resource. Automating the use of this file and making it available to authorized end-users should provide an effective and efficient tool for helping protect U.S. assets from individuals who misrepresent their identity and intentions in order to gain unauthorized access for purposes of doing harm.

James A. Riedel
Director

PREFACE

EXECUTIVE SUMMARY

INTRODUCTION

When fingerprints are submitted to the Federal Bureau of Investigation (FBI) as part of U.S. government background investigations for security clearances, military accessions, and other positions of trust, the prints are searched against the FBI's criminal file. Fingerprints that do not have a match in the criminal file are stored in a Civil File. The Civil File is not presently searchable, however, through efficient and automated means. Consequently, the U.S. government is not using one of its best potential resources for detecting identity fraud committed by individuals who attempt to gain access to government facilities, materials, information systems, and classified information. The purpose of this study was to explore the feasibility of including checks of the FBI civil fingerprint file in background investigations.

METHODOLOGY

Fingerprints for 1,144 applicants who processed through the Los Angeles Military Entrance Processing Station (LA MEPS) between December 2004 and May 2005 were submitted to the FBI for searching against their civil fingerprint file. The FBI conducted the searches and returned the results to PERSEREC for analysis. Results were compared to determine discrepancies in personally identifying information associated with applicants with multiple Civil File fingerprint submissions. Eleven of the submissions were rejected due to quality of the fingerprint capture. The FBI did not receive 129 submissions as expected from OPM and these 129 applicants had not had prior fingerprint submissions to the Civil File. Therefore, they were excluded from the analysis. Of the remaining 1,004 applicants, 113 had criminal records with no Civil File on record. For the remaining 891 sets of fingerprints, 72 fingerprint submissions were already on file from these applicants' prior investigations or entry into the country. For the remaining 819 prints forwarded by PERSEREC to the FBI, matches were tested against the same prints submitted for these applicants via OPM. While no discrepancies were expected, the latter group permitted analysis of whether more than one applicant was using some of the same personal identifiers (e.g., social security number).

FINDINGS

- Of the 72 subjects with multiple civil submissions on file with the FBI, eight had two submissions prior to the fingerprint submission used for this study. One subject had three civil submissions.

EXECUTIVE SUMMARY

- Twenty-six subjects had prior civil fingerprints on file that had been submitted by the Immigration and Naturalization Service (INS).¹
- Five subjects had name inconsistencies between different civil fingerprint file submissions.
- For the 26 INS submissions, the places of birth from in the INS fingerprint file submissions were different than the places of birth in the LA MEPS submission for four applicants. Place of birth was missing for three LA MEPS applicants.
- In four cases, date of birth (DOB) for the LA MEPS submission did not match DOB for the prior fingerprint submission. Two appear likely to be typographical errors. The differences in the other two are more difficult but not impossible to associate with typos.
- Height and weight differences can be expected depending on the time elapsed between fingerprint submissions. For this study, one applicant had illogical changes in height and weight that would be hard to explain based on typical aging or fitness changes.
- Two applicants had a different race in the LA MEPS submission from their prior fingerprint submission.
- Three applicants had discrepancies in at least three different types of personal identifiers.
- For fingerprint submissions where the LA MEPS established the first record, no subjects with different identifiers were using the same names or social security numbers.

RECOMMENDATIONS

- (1) The FBI should place a high priority on developing automated Civil File search capability.
- (2) Submitting agencies should ensure that all physical descriptors and other identifying information (date of birth, place of birth, citizenship, social security number, alien registration number) are provided accurately and completely with the fingerprint submission.
- (3) The FBI should parse fields pertaining to physical descriptors and other identifying information in Civil File checks to enable them to automatically compare fields across fingerprint submissions to identify and report discrepancies in the results that are returned.
- (4) Department of Defense (DoD) should develop policy and procedures for reviewing discrepancies and, as appropriate, ruling out identity fraud as a reason for the discrepancies.

¹ The INS is now called United States Citizenship and Immigration Services (USCIS).

- (5) After the program has been established, the FBI should track the number of times it detects (a) different sets of fingerprints associated with a single set of personal identifiers (e.g., name, SSN, POB, DOB), and (b) different sets of personal identifiers associated with a single set of fingerprints. While these incidents will be relatively rare, the FBI's ability to detect their existence in its civil fingerprint file will help reduce the nation's vulnerability to people acquiring access to classified information, weapons, military training, and sensitive duties by posing as another person.

EXECUTIVE SUMMARY

TABLE OF CONTENTS

INTRODUCTION _____ **1**
 PURPOSE _____ 1
 BACKGROUND _____ 1
 LEGAL AUTHORITY _____ 3
METHODOLOGY _____ **5**
RESULTS _____ **7**
 WITHIN-SUBJECTS ANALYSIS _____ 7
 Submitting Agencies _____ 7
 Name Inconsistencies _____ 7
 Place of Birth _____ 7
 Citizenship _____ 7
 Date of Birth _____ 8
 Physical Descriptors _____ 8
 Multiple Discrepancies _____ 9
 BETWEEN-SUBJECTS ANALYSIS _____ 10
 Based on Last Name, First Name, and Civil File Features _____ 10
 Based on Other Personal Identifiers _____ 10
DISCUSSION _____ **11**
REFERENCES _____ **13**
APPENDIX A : PILOT STUDY DATA FLOW _____ **A-1**

LIST OF TABLES

Table 1 Date of Birth Discrepancies _____ 8
 Table 2 Largest or Illogical Changes to Height and/or Weight _____ 9

LIST OF FIGURES IN APPENDICES

Figure A-1 DoD Civil File Search Data Flow _____ A-3

TABLE OF CONTENTS

INTRODUCTION

PURPOSE

The purpose of this report is to present findings from a collaborative study conducted by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) division's Identification and Investigative Services Section (IISS) and the Defense Personnel Security Research Center (PERSEREC) to assess the feasibility of conducting Civil File searches for all Department of Defense (DoD) fingerprints submitted for background investigations. This report describes the background, methods, and results for the pilot. Based on the findings, recommendations for continuing and improving Civil File search capability are offered.

BACKGROUND

When fingerprints are submitted to the FBI as part of background investigations for security clearances, military accessions, and other positions of trust, the prints are searched against the FBI's criminal file. If a record is not found, a result of "No Match" is returned to the submitter, and the prints are stored in a Civil File.

Even though they do not have criminal records, the Civil File is likely to contain fingerprints of individuals who would be of significant interest to background investigators and adjudicators. Examples include the following:

- Those employed in positions of trust requiring fingerprint checks who engaged in misconduct and were dismissed, possibly with the option of either resigning or being criminally prosecuted.
- Those employed in positions of trust who were accused of criminal acts but fled before they could be arrested and booked.
- Those employed in positions of trust who were arrested and booked for criminal acts but their prints were not forwarded to the FBI.
- Those who have either never been arrested and booked in the United States or whose fingerprints were not forwarded to the FBI who:
 - had been previously employed in positions of trust requiring fingerprint submissions,
 - were fingerprinted for alien registration and naturalization purposes, or
 - submitted their fingerprints and requested they be made available for personal identification purposes.

In a briefing to the Standards Committee of the National Crime Prevention and Privacy Compact Council in 2003, PERSEREC (2003) highlighted several cases that

INTRODUCTION

demonstrate the importance and value of developing capability for FBI Civil File searches. They are as follows:

- James David Land AKA James Pantera AKA James Sabre Pantera AKA Robert Michael Binkin enlisted two different times in the armed services under two different names.
- After being discharged for fraudulent enlistment, Wayne Hudson AKA David Pecard AKA ? created new identities and reenlisted at least seven more times.
- An employee at the D. C. Cook Nuclear Power Station used fraudulent ID to conceal the fact that she had been denied unescorted access previously to the Cook plant in January 1999 and to a Tennessee nuclear plant in November 1998.
- A member of a ring of bank thieves got himself hired at two different banks at the same time by using different names.
- Texas bars child care operations for two years that have had their licenses revoked from reapplying. But officials say some simply obtain new licenses under different names.

The online Civil File became an operational part of the Integrated Automated Fingerprint Identification System (IAFIS) in May 2000. The file currently houses more than 8 million subjects and has been populated on a day-one-forward basis. The IISS is in the process, however, of converting 1.5 million hardcopy military fingerprint cards as resources permit.

The Civil File consists of three segments: the civil subject index master file, the civil ten-print image file and the civil ten-print features data file. The civil subject index master file contains physical and biographical identifiers for each civil subject stored by IAFIS along with an index pointer indicating where each civil subject's fingerprint images can be located. Multiple records can be maintained for a single subject within this segment. The civil ten-print image file contains ten-print images and a searchable image locator that is associated with each subject entry. The civil ten-print features data file stores fingerprint features for each entry into the file in the same manner that is done for criminal data.

Currently, the FBI has the legal authority to deposit civil submissions into the electronic Civil File if the prints are forwarded for federal employment, military service, alien registration, or naturalization purposes, or by individuals desiring to have their fingerprints placed on record with the FBI for personal identification humanitarian purposes. Once retained, IAFIS issues a unique civil record number for each subject indexed in the Civil File. Conversely, the FBI does not retain noncriminal justice applicant fingerprints for those applying for licensing or nonfederal employment.

Of the various electronic ten-print types of transactions (TOT), only the unknown deceased (DEK), missing person (MPR), and amnesia victim (AMN) TOTs are able to search the electronic Civil File for noncriminal justice purposes. The DoD has

indicated security vulnerabilities are created by the failure to check civilian fingerprint files when conducting background checks for new or continued access to classified information, military enlistment or reenlistment, and for assignment to sensitive federal duties. A proposal by the DoD to allow the search of the IAFIS Civil File for background checks of applicants for positions of trust was presented to the CJIS Advisory Policy Board (APB) at the Spring 2003 session. This topic was also discussed at the Compact Council Standards Committee meetings in August 2003.

The FBI Civil File contains fingerprints of military applicants, security clearance applicants, and foreign nationals who do not have criminal records. As such, it is an excellent potential resource for identifying applicants who do not have criminal records but who may be engaging in identity fraud. For example, individuals can desert or be dishonorably discharged from the military without incurring criminal records. Similarly, security clearances can be revoked or personnel can be offered the option of resignation instead of prosecution for misconduct without incurring criminal records. They could create or steal an alternate identity and attempt to reenlist or reapply for another position of trust. Noncitizens who are processed into the United States through legitimate channels can later obtain or manufacture U.S. birth certificates and use these to gain acceptance in positions of trust for which they would otherwise be disqualified. If searches of the Civil File were possible, the fact that these individuals already have fingerprints on file and that the prints are associated with different personal identifiers could be detected. Without such capability, the United States needlessly risks granting ineligible persons access to sensitive information, materials, and facilities.

LEGAL AUTHORITY

The Privacy Act requires federal agencies to publish Systems of Records notices that let the public know what information is being stored in federal databases, under what authority that information is being collected, how long that information will be used and retained, how it is routinely used, and to whom it is provided. The public is given an opportunity to challenge any inappropriate collection, storage, or use of data that is reflected in those notices. The FBI's *Fingerprint Identification Records System (FIRS) System of Records Notice* authorizes disclosure of personally identifying information associated with civil fingerprints submitted by federal agencies and by individuals who opt to have their fingerprints placed on record for personal identification purposes:

To a federal, state, tribal, or local criminal or noncriminal justice agency/organization; or to other entities where specifically authorized by federal statute, state statute pursuant to Pub. L. 92-544, Presidential executive order, or regulation of the Attorney General of the United States for use in making decisions affecting employment, security, contracting, licensing, revocation, or other suitability

INTRODUCTION

determinations. Examples of these disclosures may include the release of information as follows:

- (a) To the Department of Defense, Department of State, Office of Personnel Management, or Central Intelligence Agency, when requested for the purpose of determining the eligibility of a person for access to classified information or assignment to or retention in sensitive national security duties. 5 U.S.C. 9101 (1990);
- (b) To federal agencies for use in investigating the background of present and prospective federal employees and contractors (Executive Order 10450), including those providing child-care services to children under age 18 at each federal agency and at any facility operated or under contract by the federal government. 42 U.S.C. 13041 (1991);
- (c) To state and local government officials for purposes of investigating the background of applicants for noncriminal justice employment or licensing purposes if such investigation is authorized by a state statute that has been approved by the Attorney General of the United States. (The Attorney General has delegated to the FBI the responsibility for approving such state statutes.) Examples of applicants about whom FIRS information may be disclosed include: providers of services/ care for children, the elderly, or disabled persons; teachers/school bus drivers; adoptive/foster parents; security guards/private detectives; state bar applicants; doctors; and explosive dealers/purchasers. Pub. L. 92-544, 86 Stat. 1115.

In early 2003, PERSEREC submitted a request to the FBI Advisory Policy Board for consideration of developing Civil File search capability. The CJIS Division determined those searches would be technically feasible and legally permissible. Subsequently, they agreed to work with PERSEREC in conducting a pilot test of Civil File searches. The following section describes the methodology used in the pilot. Results and discussion follow.

METHODOLOGY

The Los Angeles Military Entrance Processing Station (LA MEPS) agreed to assist PERSEREC and the FBI with the pilot by providing fingerprints for a sample of subjects. Between December 2004 and May 2005, the LA MEPS provided fingerprint cards to PERSEREC at a rate of approximately 100 per week. For these same subjects, the LA MEPS forwarded electronic fingerprint submissions to the FBI via OPM, according to standard procedure. Most of the electronic fingerprint submissions sent via OPM were received and stored by the FBI in advance of their receipt of the fingerprint cards from the LA MEPS via PERSEREC.

The IISS provided the hard card submissions to an internal CJIS Identification Services unit, which had the capability to conduct a civil search of the electronic civil repository. Although the goal of the project was to conduct an electronic civil search, a criminal search was conducted prior to the civil search. The employees processing the hard card submissions documented the criminal search results, and then conducted the search of the electronic civil repository by the subject's descriptors. Once the subject search results were documented, a search of the civil repository was conducted utilizing the fingerprint images. All results were verified by a second employee for quality assurance purposes. No civil or criminal records were updated as a result of this project.

Employees processing the searches of the IAFIS Civil File repository for the pilot required access to an internal processing log, with the utilization of IAFIS Service Provider Workstations. The research was conducted by accessing the Identification Tasking and Networking transaction histories utilizing the Transaction Control Number assigned to each processed card. The employees provided results to PERSEREC via the Law Enforcement Online system. Excel and WordPerfect software were used to generate reports. Printers were used to generate hard copies of reports for mailing, and a facsimile machine was specifically dedicated to the pilot project staff. The complete pilot data flow is provided in Appendix A.

In anticipation of increased demands on the MEPS to process summer enlistments, PERSEREC and the LA MEPS agreed to terminate fingerprint submissions in May. The resulting pilot sample consisted of 1,200 submissions, of which 56 were duplicate submissions (i.e., there were two cases for the same subject). In some cases, it appears the LA MEPS may have sent duplicate prints. In other cases, it appears the FBI created a new case for each search, such that if an initial civil file search did not identify a record and a subsequent search did, then two cases were stored in the data sent to PERSEREC. Removing these duplicates resulted in a final sample of 1,144 nonduplicate submissions.

Of these 1,144 unique subjects, 11 fingerprint submissions were rejected due to problems with the quality of the fingerprint card prints. No OPM submission was

METHODOLOGY

found for 129 of the fingerprint cards that were submitted for the pilot. Excluding these subjects from the analysis resulted in a sample size of 1,004.

Of these 1,004 cases, 117 subjects had criminal records. Civil File records are not established for subjects with criminal records, if the criminal arrest causes the first submission of an individual's fingerprints to the FBI. It is also possible for subjects to have Civil File records established and then subsequently have an arrest record established. Of the 117 subjects with criminal records, only four had evidence of Civil File descriptors. For the other 113 subjects, the FBI conducted civil searches to determine whether prints were also stored in the Civil File, but the results from these were "No Record." As such, these subjects were excluded from the analysis consistent with other "No Record" events.

Nonduplicate fingerprint submissions that returned Civil File data for analysis totaled 891 subjects. Of these subjects, 8% (n=72) already had civil prints on file at the time that the LA MEPS submitted fingerprints for this pilot. The FBI provided summary sheets listing identifiers for these 72 subjects. These 72 cases were used to assess within-subject differences in personally identifying information provided by applicants each time that they were fingerprinted.

For the 819 subjects for whom the LA MEPS submission was the first instance of establishing a civil print record, "between subject" analyses were also possible, but these used only name and civil print features as comparison points. For these subjects, possible identity fraud could be evident in different names being associated with the same civil fingerprint features or different civil fingerprint features being associated with subjects of the same name. Due to the small sample size and narrow time period during which prints were submitted, we did not expect to find evidence of identity fraud in the between-subjects analyses. At the same time, providing results of these analyses demonstrates the potential utility of Civil File searches for purposes of detecting identity fraud. Comparisons between the 72 subjects with multiple civil print submissions were possible using the full range of personal identifiers provided to PERSEREC by the FBI.

RESULTS

WITHIN-SUBJECTS ANALYSIS

Of the 72 subjects with multiple civil submissions on file with the FBI, eight had two submissions prior to the fingerprint submission used in this study. One subject had three civil submissions on file.

Submitting Agencies

Twenty-six subjects had fingerprints on file that were submitted by the INS. For 22 of these subjects, the INS submission was the oldest civil record on file. If these subjects did not report immigrating to the United States and at approximately the same date as the INS fingerprint submissions, then these submissions could indicate potential fraud.

The oldest civil fingerprint record on file was dated June of 2000 and was submitted by the Defense Investigative Service (DIS). The oldest INS submission was dated July of 2003. The oldest OPM submission was January of 2003.

Name Inconsistencies

Five subjects had name inconsistencies between their fingerprint submissions. Three of these were females who may have married between their first and subsequent fingerprint submissions. The investigating agency should determine whether these women reported marriages. If not, then these name inconsistencies could indicate identity fraud. For the fourth subject, the last name and first name were inverted between two submissions. For the fifth, the first name was missing one letter.

Place of Birth

Data on places of birth were available in the oldest fingerprint record on file for all 26 of the subjects with INS fingerprint submissions. All had recorded places of birth outside the United States. In the second submission, four place-of-birth codes were different and three place-of-birth codes were missing. Where place-of-birth codes were inconsistent between submissions, investigators should determine whether information was withheld or altered intentionally.

Citizenship

Information about citizenship was missing from all fingerprint submissions for 30 of the 72 subjects with multiple civil fingerprint files. An additional 27 fingerprint cards were missing citizenship information at the time of the second fingerprint card submission. All but nine of these subjects were born outside the United States. Four subjects were missing both place of birth and citizenship in their second civil submission. For optimal effectiveness of Civil File search capability,

RESULTS

place of birth and citizenship information should be complete for every Civil File submission.

Date of Birth

Of the 72 subjects for whom multiple submissions were found, ages at time of first Civil File submission ranged from 15 to 38 years, with 50 percent age 21 or less. Ages ranged from 17 to 40 years at the time the second Civil File record was established. For the seven subjects with three fingerprint records, ages ranged from 20 to 32 years.

As shown in Table 1, there were four cases where the date of birth for the second fingerprint submission did not match the date of birth for the first fingerprint submission. All represent possible data entry errors, either in the mistyping of a digit, or in the reversal of the position of months and days. Individuals who wish to misrepresent their identities often insert faulty dates that can later be explained as innocent data entry errors if detected. Thus, even apparent data entry errors should be investigated to at least correct the errors.

Table 1
Date of Birth Discrepancies

<i>DOB for Record 1</i>	<i>DOB for Record 2</i>
11 / 07 / 1983	07 / 10 / 1983
11 / 03 / 1983	03 / 11 / 1985
01 / 02 / 1971	01 / 02 / 1973
12 / 16 / 1977	12 / 06 / 1977

Physical Descriptors

Height and Weight. Height and weight differences for this study were not uncommon due to the relative youth of the sample and the fact that some had military training that could either reduce fat or add to muscle weight, depending on the physical condition of subjects upon submitting to fingerprints for the first time. For example, a change in height of one or two inches between fingerprint submissions is reasonable for someone who was a teenager at the time of first submission. Improvements to posture through military training could also be reflected in changes to height for relatively older subjects. A loss of height, however, should be cause for added investigation, as should other radical changes to height and weight.

For the 72 subjects for whom multiple fingerprint submissions were available for analysis, there were some cases of relatively dramatic changes to height and/or weight that could possible warrant further investigation to eliminate the possibility of identity fraud. Table 2 provides more information about these cases. In three cases, subjects were shorter the second time they submitted fingerprints. A decrease of 1 inch could be due to misinformation being provided by the applicant at one point in time and/or to measurement error on the part of a military medical examiner.

Large weight gains or losses are quite possible depending on changes in health or fitness. Or, in some cases, they could be due to misrepresentations of applicants who are trying to meet weight standards, at least on paper, for military service or public safety positions. Or large differences could be due to typographical and data entry errors. At the very least, illogical changes in height or weight could be evidence of identity fraud. An example is the subject in Table 2 who appears to have gained 10 inches in height and 48 pounds between the first and second submission of fingerprints. In this case, only 2.5 years had elapsed between fingerprint submissions.

Table 2
Largest or Illogical Changes to Height and/or Weight

<i>Age of Subject at Time of First Submission</i>	<i>Change in Height</i>	<i>Change in Weight</i>	<i>Time Elapsed</i>
16	Shorter by 1 inch	Lighter by 16 pounds	1 year, 5 months
16	Shorter by 3 inches	Heavier by 8 pounds	1 year, 9 months
17	Shorter by 2 inches	Lighter by 7 pounds	1 year, 5 months
21	Taller by 10 inches	Heavier by 48 pounds	2 years, 5 months
22	Taller by 1 inch	Heavier by 55 pounds	2 years, 2 months
27	Taller by 1 inch	Heavier by 47 pounds	2 years, 6 months
31	Same height	Heavier by 52 pounds	2 years, 4 months

Race. Most of the discrepancies in race were due to race not being indicated in at least one fingerprint submissions (n=6). In two cases, subjects were noted as “B” at the time of the first submission and “W” in a subsequent submission. Again, while these may be data entry errors, they would warrant extra attention to rule out the possibility of identity fraud.

Eye and Hair Color. Discrepancies in hair and eye color were typically benign differences such as brown versus black (n=3), green versus hazel (n=1), or grey versus green (n=1) for eye color and brown versus blond for hair color.

Multiple Discrepancies

As mentioned above, any one discrepancy is probably more likely due to human error rather than identity fraud. When multiple discrepancies are found for one subject, however, investigators should be especially sensitive to the possibility that identity fraud has been committed. Out of the 72 subjects for whom multiple fingerprint submissions were available for comparison, three cases had multiple discrepancies. These cases are as follows:

Subject 1

- Weight at Time 1: 163 versus Weight at Time 2: 195
- DOB Time 1: 3 NOV 83 versus DOB Time 2: 11 MAR 85

RESULTS

Subject 2

- Weight Time 1: 190 versus Time 2: 165
- Eye color Time 1: BLK versus Time 2: BRO
- Place of birth Time 1: BR (Brazil) versus Time 2: BL (Bolivia)
- Citizenship Time 1: BR (Brazil) versus Time 2: SU (Sudan)
- Last name different between submission 1 and submission 2

Subject 3

- Date of Birth Time 1: 2 JAN 71 versus Time 2: 2 JAN 73
- Weight Time 1: 167 versus Time 2: 219
- Hair Color Time 1: BL versus Time 2: BR

While none of the above discrepancies may be explained by intentional fraud, the number and nature of the differences may justify subjecting these cases to further scrutiny.

BETWEEN-SUBJECTS ANALYSIS

Based on Last Name, First Name, and Civil File Features

None of the submissions were characterized as matching on civil print features but differing by name. Nor did any of the submissions match on name but differ in civil print features. The FBI did not return data sheets where civil searches were conducted on first-time fingerprint submissions; therefore, further analysis on other subject characteristics was not possible.

Based on Other Personal Identifiers

Of the 72 subjects with multiple civil records, there were zero cases where multiple subjects' SSNs were associated with a single name and zero cases where more than one subjects' SSNs matched but their names did not match.

DISCUSSION

This study has demonstrated the promise of FBI civil fingerprint file search capability for detecting identification fraud on the part of persons applying for positions of trust. Through receipt of prints, FBI personnel demonstrated the technical feasibility of conducting such searches. Through analysis of the results of the searches, the FBI and the DoD have demonstrated the value of the information for detecting identity fraud. The prevalence of missing data described throughout the report, however, underscores the importance of the completeness and accuracy of information provided by agencies that submit fingerprints for background screening purposes. Based on these considerations, it is recommended that:

- (1) The FBI should place a high priority on developing automated Civil File search capability.
- (2) Submitting agencies should ensure that all physical descriptors and other identifying information (date of birth, place of birth, citizenship, social security number, alien registration number) are provided accurately and completely with the fingerprint submission.
- (3) The FBI should parse fields pertaining to physical descriptors and other identifying information in Civil File checks to enable them to automatically compare fields across fingerprint submissions to identify and report discrepancies in the results that are returned.
- (4) DoD should develop policy and procedures for reviewing discrepancies and, as appropriate, ruling out identity fraud as a reason for the discrepancies.
- (5) After the program has been established, the FBI should track the number of times it detects (a) different sets of fingerprint associated with a single set of personal identifiers (e.g., name, SSN, POB, DOB), and (b) different sets of personal identifiers associated with a single set of fingerprints. While these incidents will be relatively rare, the FBI's ability to detect their existence in its civil fingerprint file will help reduce the nation's vulnerability to people acquiring access to classified information, weapons, military training, and sensitive duties by posing as another person.

REFERENCES

REFERENCES

Buck, K. R. (2003, August 25), *Civil fingerprint searches for combating identity falsification among people applying for positions of trust*. Paper presented to the Standards Committee of the National Crime Prevention and Privacy Compact Council, Pittsburgh, PA.

**APPENDIX A:
PILOT STUDY DATA FLOW**

APPENDIX A

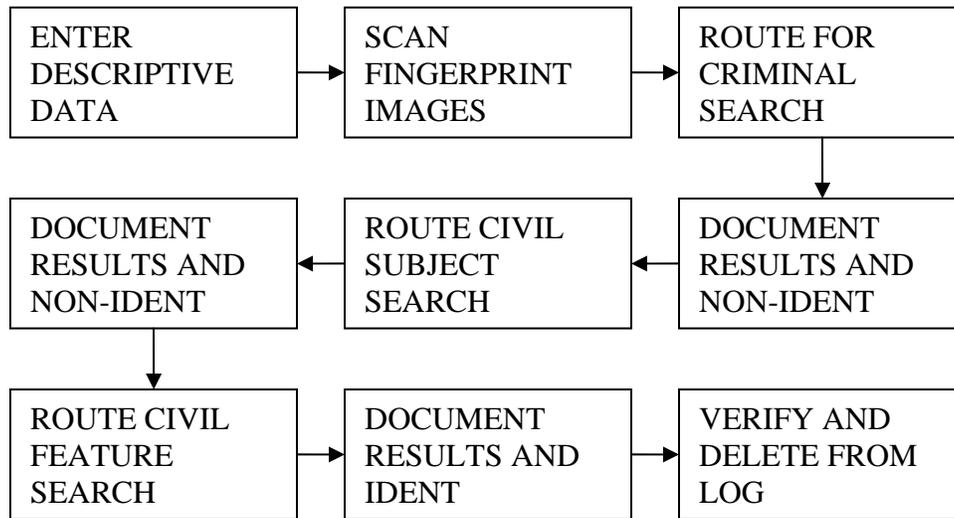


Figure A-1 DoD Civil File Search Data Flow

- Enter the Descriptive Data from card exactly as it appears on the card.
- Scan the fingerprint images.
- Route the transaction to perform a Criminal File Search.
- If candidates are generated in the criminal search, document candidates and route for the Civil File Search.
- Perform a Civil Subject Search based on descriptive data; document results and route for a Civil Feature Search.
- Perform a Civil Feature Search based on fingerprint minutia; document results and verify results
- Provide completed documentation for entry into spread sheet and delete transaction