



August 4, 2005

Department of Justice
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Re: Criminal History Background Checks: Request for Comments

To Whom It May Concern:

We are writing on behalf of the **National Association of Professional Background Screeners (NAPBS)**, with the assistance of Seyfarth Shaw LLP,¹ to offer our association's comments on the Attorney General's planned report to Congress relating to criminal history background checks conducted by the Department of Justice (DOJ).

NAPBS exists to promote ethical business practices, promote compliance with the **Fair Credit Reporting Act (FCRA)** and foster awareness of issues related to consumer protection and privacy rights within the background screening industry. The Association provides relevant programs and training aimed at empowering members to better serve clients and to maintain standards of excellence in the background screening industry. NAPBS is active in public affairs and provides a unified voice on behalf of members to local, state and national lawmakers about issues impacting the background screening industry.

NAPBS commends the DOJ for undertaking the task of improving, standardizing and consolidating the process for conducting criminal history background checks, and hopes that the information obtained from these and other comments will help make such background checks more accurate and usable. In creating these comments, we have polled NAPBS members and rely on their years of experience dealing with currently available systems and databases to conduct background checks.

General Comments

- Most NAPBS members obtain criminal background information from publicly available criminal history data maintained by United States Counties, Statewide Criminal Record Repositories (where access is legally permitted), and Federal

¹ Seyfarth Shaw LLP is a prominent national law firm with one of the country's most widely known management labor and employment practices. Over 250 of Seyfarth's 600 attorneys are solely dedicated to the practice of labor and employment and employee benefits law. Seyfarth's labor and employment attorneys practice out of offices in Chicago, Atlanta, Boston, Houston, New York, Washington, D.C., Los Angeles, San Francisco, and Sacramento. Seyfarth also is a member of NAPBS and has a nationwide task force dedicated to litigation defense and compliance counseling under the Fair Credit Reporting Act (FCRA) and state background screening laws.

Districts. This data is sometimes supplemented with a search of third-party criminal record databases, which contain hundreds of millions of records. Because of FCRA requirements, information from a third-party database is typically used as a “pointer” to search in the jurisdiction of record origination.

- Although the request for comments appears to presume that most employers (and background screening companies, for that matter) use the Integrated Automated Fingerprint Identification System (IAFIS) to conduct criminal background checks, in fact, very few employers are legally permitted to obtain fingerprint-based criminal histories (e.g., financial securities) from that source, except in limited circumstances. Should IAFIS accessibility be expanded to a broader range of employers, the effectiveness of this criminal search for employment screening purposes would greatly depend on response time. Employers typically require information within three (3) days as part of an employment decision. An extended response time would render such criminal record checks unusable. Therefore, in addition to commenting on the changes we recommend for the IAFIS to make it usable for a broader range of entities, we also have endeavored to discuss the relative merits of other repositories of criminal history information, and have identified areas that need improvement in order for criminal background checks to be completed in an efficient and accurate manner.
- Most employers use third party consumer reporting agencies (many of whom are NAPBS members) to conduct criminal background checks for hiring purposes. Because these searches require expertise and nationwide resources, they are rarely done by the prospective employer.
- Given the variety of sources available to employers, some NAPBS members argue that the most thorough criminal background check would include researching numerous databases, including a review of the local and state repositories of information received from various courts, one or more of the handful of major private commercial databases of criminal history information, and the federal IAFIS system. Whether this is a practical alternative depends upon:
 - Legal requirements, both federal and state;
 - Response time to provide information; and
 - Recourse available to the applicant who is the subject of the criminal record search.

In addition to these general comments, NAPBS offers the following responses to the Attorney General’s specific areas of inquiry:

1. The effectiveness and efficiency of utilizing commercially available databases as a supplement to IAFIS.

As a point of clarification, using a commercially available database as a “supplement” to IAFIS presupposes that employers or their agents are permitted access to IAFIS. As a very

limited number of employers have the legal basis for such access, most employers would have nothing to “supplement.” The paramount concerns are:

- Enabling users of these databases to quickly verify the accuracy of such information so that they can meet the practical time-limits of employment screening,
- Accuracy requirements of the FCRA,
- State laws regulating criminal history information, and
- Manageable dispute resolution processes available to the subject of the criminal record search.

Larger privately owned databases perform upwards of eight million background checks per year, with the majority of those including criminal history information. As explained below, assuming the implementation of appropriate quality controls, the use of commercial databases as a supplement to IAFIS is ideal, because a well-maintained and updated private database contains certain information that is not available at the federal level. This is especially true because the majority of information obtained by IAFIS relates to arrest records – not conviction information – and may not differentiate between an arrest without subsequent action and one that includes a formal charge and further processing. Further, evidence collected by NAPBS suggests that even when criminal background information is available at the state or county level, it may be absent from the federal database. One informal study of job applicants with criminal history information revealed that IAFIS missed nearly 20% of convictions that were picked up by the performance of a county search. The majority of the “missed hits” concerned DUI convictions and other misdemeanors.

The main problem with the use of commercial databases at this point is the fact that they are not regulated (other than under the FCRA) and, thus, there is no way to confirm the accuracy or thoroughness of the information contained therein. For example, there is no regulation – governmental, self-regulatory or otherwise – requiring that a “hit” in a commercial database be confirmed by the originating jurisdiction before the information is conveyed to an end-user. As one aspect of its “best practices” initiatives, NAPBS is trying to establish standards requiring consumer reporting agencies to cross-check hits in a commercial database by accessing the local public record. Likewise, until IAFIS accurately captures and makes accessible state and local criminal record data, the best practice for consumer reporting agencies and end-users accessing IAFIS will be to review hits in the federal system at the local, state and federal level. Thus, even if IAFIS data is released more broadly to the general public, accuracy may only be obtained through confirmation searches in the originating jurisdiction.

From our perspective, another problem with the use of an “IAFIS plus commercial databases” search – without any public record searches in appropriate jurisdictions – is that of *false security*. As noted earlier, IAFIS does not include all criminal conviction records found in originating jurisdictions. While broad in scope, commercial databases also do not include all criminal records.

2. Any security concerns created by the existence of these commercially available databases concerning their ability to provide sensitive information that is not readily available about law enforcement or intelligence officials.

As discussed above, without a regulating body, security concerns exist both for IAFIS and commercially available databases. NAPBS believes, however, that the security concerns regarding commercially available databases are not limited to information about law enforcement or intelligence officials or even to their use as an IAFIS supplement. A proliferation of criminal background information and search tools are available on the Internet with the providers and content being generally unregulated. Further, commercial databases are prime targets for identity theft. While this is a relevant topic, these security concerns need to be addressed on a broader scale than the use of databases to supplement IAFIS.

For example, a best practices approach might require a formal contract between the provider of the background information and the end-user, to insure that the end-user has a permissible purpose for the information pursuant to the FCRA and, additionally, that the user will safeguard the privacy of the information. Additional safeguards would include websites with programs to encrypt information, password protected websites, and strictly enforced document destruction procedures. Many of these protections exist by virtue of contracts between consumer reporting agencies and the credit bureaus, but NAPBS wants to broaden the scope of these preventative measures to reach all aspects of the background screening industry.

3. The effectiveness of utilizing State databases.

Nearly all NAPBS members who contributed to these comments agree that the current inconsistency among the State databases would make it difficult to effectively use them on a nationwide level. More importantly, this means that to the extent that IAFIS uses information collected from or submitted by the states, that information itself may be inconsistent.

NAPBS recently commissioned a review and evaluation of the National Crime Information Center (NCIC) by Craig N. Wilson, Assistant Professor of Criminal Justice at Sonoma State University, both in an effort to create best practices and also as a means of responding to the DOJ's request for comments. (A copy of this review is attached to these comments as Exhibit A). This review identifies a number of problems and issues associated with using state databases, including the following:

- The type of criminal history information maintained differs from state to state. For example, many states do not maintain information on dispositions, declination to prosecute, failure to charge after fingerprints have been submitted and expungements;²

² NAPBS member BRB Publications detailed some of the specific inconsistencies in the state systems in its own submission to the DOJ in a letter dated June 27, 2005. Specifically, BRB noted that:

Only 32 states require prosecutors to report to state repositories a decision to decline prosecution of a case.

Only 35 states and DC require law enforcement officials to notify the state repository when an arrested person is released without formal charging, but after fingerprints were submitted.

Only 42 states use computer edit and verification programs as part of data quality procedures.

- States have different reporting requirements, and variations in states' criminal codes means that identical crimes may be reported differently from state to state (for example, as a felony in one state and a misdemeanor in another). Added to this is the problem that many states underreport misdemeanor convictions to their repositories, so valuable criminal background information (such as petty larceny or assault and battery), which may be relevant to an individual's employment, are excluded;
- In some jurisdictions, it can take several weeks or longer for criminal history information to be reported to and then entered in the state depository, an amount of time that makes the information almost useless for employment purposes;
- There is no standardized process for linking individuals with the correct information or for linking dispositional information to the proper case and charge. Mistakes and "false positives" or "false negatives" are common when fingerprints are not used to verify information;
- Each state uses a different format for collecting data, which makes it difficult to share information from state to state.

Aside from this, many states effectively prevent most private employers and their agents from accessing the information housed in their central database or, alternatively, place such onerous requirements on the use of the data that it is inefficient or impractical for employers to utilize the state resource. For example, several states require an original notarized signature authorizing the employer to obtain criminal background information from a state repository. This issue needs to be resolved before state databases can be considered fully secure, accurate and reliable sources of criminal background information, and before a DOJ sponsored database can be effectively used for employment-related background and criminal history checks.

Despite these shortcomings, state repositories are an important tool used by consumer reporting agencies to achieve accurate and complete criminal record screening. Many consumer reporting agencies utilize such repositories as "pointer files," identifying the appropriate county to check for their subject. This is important because often times state records have few personal identifiers for the subjects in their system. Consequently, a search for "Willie Williams" may turn up many records and it can be difficult, if not impossible, to separate the subject of the report from the other "Willie Williams." Similarly, using state repositories as pointer files can help narrow the scope of searches involving (1) subjects from metropolitan areas, where the "hometown" of the subject covers several counties; and (2) numerous counties for a population that has become increasingly mobile. Without state repositories, employers are forced to guess which county might be the appropriate county to check for their subject, and county checks can be quite expensive. For the equivalent price of a county search the requester can receive a pointer for potential records in other counties and courts. As one commentator has said – a state record is a mile wide and inch deep but county records may be an inch wide and a mile deep.

Only 21 states report they receive final felony trial court dispositions for 70% or more arrests within the last 5 years.

Only 10 states report they receive 100% of final trial court dispositions.

4. Any feasibility studies by the DOJ of the resources and structure of the FBI to establish a system to provide criminal history information.

NAPBS has no comment on this issue.

5. Privacy rights and other employee protections.

Although most parties agree that information regarding our judicial proceedings must be made available to the public, there are many differing opinions as to the degree of access that should be afforded. Placed in this context, NAPBS has attempted to address below the specific points raised in the Department's request for comments. In short, NAPBS recommends that the privacy protections established in the FCRA be applied when and if more general access to IAFIS is allowed.

(A) Employee Consent;

The Federal Trade Commission (FTC) has provided a framework to balance the rights of prospective employees (consumers) and private enterprise. The FCRA, 15 U.S.C. § 1681 et seq. is a historical framework for protecting the rights of individuals while supporting the needs of private enterprise. The interested parties are not suggesting that the DOJ become a credit reporting agency, yet some portions of the FCRA offer a relevant working model that could be easily adapted to address many of the parties' concerns. The DOJ has an opportunity to set a standard that specifically addresses the practice of conducting background verifications completely separate and apart from the credit reporting industry. To date, the primary focus of the FTC in the FCRA has been on consumer credit, making its application to employers an exercise in fitting a square peg into a round hole.

Protecting an individual's right to privacy is made much easier by the practice of obtaining consent for the completion of a background verification as described in § 604. Permissible purposes of consumer reports, 15 U.S.C. § 1681b, where the requirement to obtain written consent from the prospective employee is stated if a consumer report is being obtained for employment purposes.

(B) Access to the records used if employment is denied;

Under § 604 of the FCRA, the employer must also advise the consumer of his or her right to dispute information and the right to be notified if any adverse information contained in the report results in adverse action; such as, a decision not to hire, a declination of an offer to hire or a decision to terminate. This requirement works because all parties' interests in making fact-based decisions are served. Employers want to hire qualified candidates that have been recruited and interviewed for open positions, a costly and time consuming process, and they want to hire individuals that do not pose a threat to their current employees and customers.

Public records, like all records, are prepared and maintained by humans who are error prone. Even in an electronically enabled file system, there are misspellings, misfiling and failures to update records that could lead to an unintended outcome in the employment process, should a decision be made based on outdated or erroneous information. For this reason, NAPBS favors an adverse action process similar to that detailed in § 604. In cases where negative information in an employment related inquiry may result in adverse action as described above, the employer must provide a copy of the report and a summary of the consumer's rights

including the name of the information provider and their contact information so that the consumer can clarify any erroneous or outdated information in his or her file.

(C) The disposition of the fingerprint submissions after the records are searched;

While the FCRA provides some protection for individuals' privacy rights, it does not extend to the provision or use of fingerprints or otherwise cover the government. Accordingly, there are privacy concerns relating to this type of information. At a minimum, the standards for the proper and effective disposal of such information, like the document destruction rule recently issued by the FTC, should be instituted as it relates to accessing the federal database.

(D) An appeal mechanism;

The FCRA appeal process is defined in § 611 - Procedure in case of disputed accuracy. The information provider has a defined period of time, 30 days in most cases, to reinvestigate disputed information and respond to the consumer. Without recounting the entire section, suffice it so say that there are provisions for a myriad of contingencies that may arise during the dispute and reinvestigation process, including a process for requesting additional information from the consumer. This process takes the human error element into the reporting equation and gives all parties an opportunity to correct an error. It is critical that the DOJ consider whether or not it wants to impose the burden of correcting its records in a timely manner on the FBI. There will be a significant financial burden associated with receiving the contacts associated with challenges to the FBI data. There will also be the cost of sending employees or vendors to the jurisdiction in which the judicial proceeding is recorded to clarify or update information in the FBI database. In order to protect the rights of the job applicant, it is essential that the individual have the right to challenge information included in the background verification.

(E) Penalties for misuse of the information.

Liability for errors is limited to the correction process unless parties fail to follow the requirements set forth in the Act in § 617. Civil liability for negligent noncompliance, 15 U.S.C. § 1681o. Essentially, this section provides the consumer with the ability to recover actual damages in addition to attorney's fees for either party depending on the outcome of the claim.

6. The scope and means of processing background checks for private employers utilizing data maintained by the FBI that the Attorney General should be allowed to authorize in cases where the authority for such checks is not available at the State level.

At this time, every state has different laws relating to what information can be obtained and/or used by consumer reporting agencies and end-users with permissible purposes. While many States may individually require that employers conduct criminal history background checks for a particular job type (e.g., childcare, healthcare, etc.), these requirements are not uniform from state to state. In any event, the availability of IAFIS-based criminal background checks should not be dependent on criminal background check availability at the state level. To do so would create logistical problems for multi-state employers and further perpetuate inconsistent background screening due to inconsistent record availability from the states. In this area, as in many others, the federal government's intervention should be in the interest of uniformity and consistency, and should not further the burdensome and confusing roadblocks put up by the multiplicity of different standards found at the state level.

Should IAFIS be expanded to offer criminal background checks to private employers (or consumer reporting agencies hired by employers) who seek them, a decision would have to be made whether to authorize such checks only for certain industries/jobs or for any private employer who wants such a check. Additionally, a fee schedule would have to be established, and privacy and security protections, similar to those addressed in the FCRA, would need to be created.

7. Any restrictions that should be placed on the ability of an employer to charge an employee or prospective employee for the cost associated with the background check.

This question raises several issues: 1) whether an employer may charge employees only for a background check performed using IAFIS ; 2) whether an employer may charge employees for any background check, no matter what database(s) are accessed; and 3) does the analysis change if the employer is required by statute to perform the background check.

Taking all those issues into account, in NAPBS' experience, it is not common in the industry for employers to directly charge employees for the cost associated with a background check. The common practice is for the cost to be absorbed by the employer as a cost of doing business. Furthermore, multiple states (e.g., California), have laws prohibiting employers from charging employees for background checks. Therefore, the DOJ may be interested in viewing the legislative history regarding these laws.

Allowing such charges could create additional problems as well. First, prospective employees may balk at paying for a background check from the employer's choice of provider in favor of a less expensive consumer reporting agency. Of course, allowing employees to choose the entity that runs their background check could create serious concerns about consistency, accuracy and security, and furthermore, begs the question, how is this different from letting the employee have the check run and then bringing it into the employer – a scenario that we are sure most if not all employers would agree would not be the wisest solution.

Even more troubling is that requiring employees to pay for their background checks could create financial difficulties for unemployed individuals, particularly those seeking lower-paying jobs, and could potentially have a disparate impact on certain employees. This result could set up employers for lawsuits or discrimination charges alleging disparate impact on protected groups of individuals disadvantaged by having to pay for their own background checks.

8. Which requirements should apply to the handling of incomplete records?

This question seems to support our earlier contention that the records at state repositories, in national database files, state Departments of Justice or the FBI database (NCIC), may be and probably are at times both incomplete and inaccurate, such that this should be a concern for the DOJ.

Given that access to such criminal record files is available through various sources, such as state and local public record repositories, by paying a third party CRA to conduct the search, or from the federal government, NAPBS believes it is important that the DOJ address how to deal with incomplete information obtained from each of these sources.

We will give consideration to four issues: (1) the protection of the privacy rights of the consumer who is the subject of the report, (2) protecting the consumer from those who may use inaccurate or incomplete information, (3) providing procedures to avoid the reporting of inaccurate or incomplete information, and (4) creating methods to simply correct inaccurate or incomplete records. We believe that no matter how an organization accesses records, the same protections should be adopted.

The FCRA was adopted to give notice to consumers when organizations or individuals seek to investigate their backgrounds, and contains provisions regarding privacy and the use of incomplete information, when such information is provided by a CRA. The FTC has issued various opinion letters indicating that licensed private investigators and companies who call themselves record search firms (such as NAPBS members) are CRAs under the FCRA. Additionally, several states have adopted their own "fair credit" laws. Therefore, we need to address what procedures the states have legislated to require accuracy of reporting.

A company who researches court records for a fee and provides such information to an employer so the employer can make an intelligent hiring decision is clearly a CRA. The question becomes: "is the state or federal government a CRA when they provide criminal records to an employer through fingerprinting?" In a phone call to the FTC, a staff attorney verbally has advised that the government is **not** a CRA. Under this theory, any report of either "no criminal convictions" or of a "criminal conviction," or any other information issued by IAFIS likely would fall outside the auspices of the FCRA. NAPBS believes this is an incorrect and inadvisable result; a government actor functioning as a CRA should be subject to the compliance requirements of the FCRA.

To protect consumers, the FCRA requires that prior to any organization requesting a criminal background check on a consumer for employment purposes, the employer must first disclose that they may request a background check and obtain written authorization. In addition, before an employer takes adverse action based on information contained in the report, it must give the consumer/applicant a copy of the report and allow him or her a reasonable period of time to dispute the information within the report. Further, the FCRA has specific procedures the CRA must follow should the consumer dispute the information in the report.³

If the FCRA does not apply to those accessing IAFIS, consumers simply will not have the protections described above. No prior disclosure of an impending criminal background check is required and no requirements or procedures exist to allow the consumer to dispute the record. Likewise, no requirements exist regarding accuracy or completeness. The FCRA contains procedures that help ensure accuracy and completeness that, in NAPBS' opinion, should be

³ Several states have adopted disclosure and adverse action requirements much like the FCRA. California, however, has gone further to protect the rights of consumers. In California whether or not you are requesting a credit report or just a consumer report (called an investigative consumer report in California), the disclosure form must (1) name the consumer reporting agency performing the search along with their toll free phone number, (2) indicate that the information may bear on the consumers character, general reputation, personal characteristics, or mode of living, (3) contain a box that the consumer may check should they want a copy of the report, (4) indicate that the consumer may obtain a copy of their report from the CRA from various means, (5) indicate that the CRA must have someone available who could answer questions or explain the codes in the report, and (6) have another person present should they desire to go to the CRA for their report.

adopted for all criminal background checks, regardless of who searches for or provides the information. Specifically, when an employer accesses criminal records through a CRA, the CRA must conform to Sections 603, 606 and 613 of the FCRA. Section 606 says that except for Section 613, a CRA must not report records which have not been verified to be accurate within the 30 days prior to the report. Section 613 says that a consumer reporting agency must have procedures in place to assure accuracy, or the CRA may report inaccurate information as long as the CRA notifies the consumer that they are reporting public record information and who they are reporting it to. These protections and standards should be equally applicable if the general public is granted access to the government's criminal database.

Additionally, some NAPBS members would argue that the best practice for its members to use when conducting background checks would be to include, in addition to a check of private databases and IAFIS, a search directly at the courts of the jurisdiction where the consumer has lived for a minimum of seven years of his or her name along with other names used. In order for this type of search to be as accurate as possible, a national mandate should be made to maintain all the consumers' identifiers within a criminal file (e.g., date of birth, driver's license number, and social security number) and make this information accessible to qualified consumer reporting agencies.

Finally, we would expand on the procedures for correcting inaccurate or incomplete information by requiring any organization selling criminal record information to provide clear and accurate notice disclosing the scope of their reports, including in particular what records are NOT contained in their files. For example, NCIC should publish a list of all the courts and counties that do not report to them, and which misdemeanors from each state are reported and which are not. State repositories also should publish what jurisdictions do not report, report on a sporadic basis, or report only felonies or "serious" misdemeanors. They also should be required to state whether the record is fingerprint based, disposition based, or not based on anything but the report. Companies who maintain data for sale must not hold themselves out to be "national" record providers, and should only provide records which are complete and up to date. It is important to note, however, that CRAs cannot be responsible for the inaccuracies contained in the public records they accurately report.

9. The circumstances under which the criminal history information should be disseminated to the employer.

It is NAPBS' understanding that this question seeks information relating to what specific type of information should be disseminated to employers and when that information is allowed to be so disseminated. Both the FCRA and related state laws are in place to address this specific question. For example, the FCRA contains practices and procedures for obtaining and using background checks for employment purposes, when such checks are performed by a CRA, as explained in the answer to question eight. Additionally, many state laws regulate what type of information can be used by an employer in making employment decisions. This begs the question, should CRAs be allowed to give employers information that the employers are not allowed to use in making employment decisions? For example, many states prohibit employers from using arrest record information in making employment decisions. And even in those states that do not have outright prohibitions, the Equal Employment Opportunity Commission and similar state agencies have published guidance that using arrest records in employment decisions may have a disparate impact on minority groups. Allowing employers to have access to this information on the federal level may thwart these purposes.

It is important, however, not to lose sight of why employers conduct background checks in the first instance, namely, because past behavior is a predictor of future behavior. Therefore, any regulation prohibiting dissemination of criminal history information to employers must take into account the need for this information balanced with the privacy rights of individuals.

10. The type of restrictions that should be prescribed for the handling of criminal history information by an employer.

Again, the FCRA places specific requirements on employers who use criminal background information for employment purposes, and these safeguards should be required by entities not covered by the law. Some states also limit or prohibit employers from obtaining or using criminal history information. It is extremely important that any restrictions on the handling or use of criminal history information give the applicant the opportunity to dispute the information prior to any employment decision being made or finalized.

11. The range of Federal and State fees that might apply to such background check requests.

A number of states have repositories of information with ranges of fees for accessing such information. As discussed in the answer to number seven, any fees imposed by state or federal repositories should not be passed on to the consumer, as such a procedure could create numerous problems. The DOJ may want to conduct a survey of access fees charged by currently available public and private databases to determine a reasonable access fee for IAFIS.

12. Any requirements that should be imposed concerning the time for responding to such background check requests.

Within the background screening industry, the average time requested by employers seeking criminal background checks from a third-party screening company is three business days. To extend response time beyond this time period likely would be to disregard employer requirements and business conditions.

Employers seek the results of a criminal background check before an applicant becomes an employee and starts work. If background checks routinely take longer than three days, employers risk losing good applicants and critical positions remain vacant. Or worse, if employers hire on a contingent basis and allow the employee to begin work pending the completion of the background check, the employer puts the company, its employees, and its customers at risk. This is especially crucial in the case of healthcare and childcare positions, where employees may have direct care responsibilities.

13. Any infrastructure that may need to be developed to support the processing of such checks.

As explained elsewhere in these comments, there are serious concerns about the accuracy and consistency of the criminal background information as it exists from state to state, and also with respect to IAFIS. Therefore, as a preliminary matter, the process must be standardized, so that a request for criminal background information from the federal repository will be the same -- and will give the same results -- no matter where the request originates.

A) The means by which information is collected and submitted in support of the checks;

Assuming the issues detailed above have been fully resolved, the DOJ should establish strict standards for how data is to be uploaded to the central repository, as well as how authorized entities in the private sector can access it. The ideal means for doing this is via XML. The currently defined Global Justice XML Data Model (Global JXDM) can be utilized for uploading data to the central repository. However, in order to support requests for data to be used for employment and tenant screening purposes, the Global JXDM should be reconciled against the HR-XML Background Check specification, which is becoming the standard for employment and tenant related background checks.⁴

All updates should be uploaded to the DOJ on a daily basis, using the Global JXDM. Where possible, the states should take on responsibility for collecting and consolidating county and local data and providing a single upload to the DOJ.

Authorized entities in the private sector should be able to access this single repository, via HR-XML requests, by presenting electronic credentials issued and authenticated by the DOJ. Authorized persons in the private sector should be able to access this single repository via a User Interface, by presenting individual electronic credentials issued and authenticated by the DOJ.

(B) The system capacity needed to process such checks at the Federal and State level.

If the central repository described above were available at a reasonable cost, it would quickly become a standard component of the vast majority of all employment and background checks performed in the country. There is insufficient data available to project the actual system need at the federal and state levels. However, it is certain that most states would be unable to fund the requirements and implement the system, using existing resources.

14. The role that States should play.

The role that states play in this process is nothing short of critical. States (and their constituent counties) are the essential source of the information everyone wants to obtain. The problems associated with the states as the source of information have been discussed in detail above. In short, there are issues with consistency and accuracy in the reporting of state criminal information, and there are issues with when and how access to state repositories of information is allowed. Nevertheless, as discussed above, state repositories do perform the important function, of directing investigators to the appropriate counties or other courts relevant to the search, saving time and effort. With improvement, the state repositories can be a key element to accurate criminal records.

⁴ Link to Global JXDM specification: <http://it.ojp.gov/jxdm/3.0.2/index.html>; Link to HR-XML Background Reports specification: http://ns.hr-xml.org/2_3/HR-XML-2_3/Screening/BackgroundReports.html.

States are sovereign entities and, as such, their cooperation in federal endeavors to compile information is based on little more than their sense of community spirit and an interest in maintaining a central repository of all criminal record information for the greater good. In order to facilitate state interest in these goals, assistance should be given to assist the integration of court records into the centralized repository. Such assistance should take the following form:

- a) Funds must be available for the states/counties/cities to purchase computer equipment, build databases and design systems whereby data is automatically transferred to the state to minimize labor expense. States are strapped for funds and systems must be designed that rely upon automatic input rather than people. In 2001, a DOJ survey noted that twenty-seven (27) states simply were not efficiently inputting data because of backlogs. An automatic system of data entry would eliminate the people expense and time delays associated with some current systems. This technology is currently available, as private background screening companies now have databases that automatically update themselves when new information is supplied.
- b) Consistency in reporting. States should be encouraged to achieve:
 - i) Input from all courts;
 - ii) Reporting of misdemeanors as well as felonies;
 - iii) The development of systems that allow dispositions to track previously supplied information;
 - iv) The provision of current status of a subject, *i.e.*, administrative release, probation, parole etc.; and
 - v) As mentioned above, the inclusion of sufficient identifiers in the record to help investigators match the subject to the record. Identifiers such as date of birth, race, gender, hair/eye color, height and the like should be uniformly available in the record so searchers and users can identify those records that relate to the subject.

The use of fingerprints is the best identifier, but this has practical limitations. Namely, fingerprints may not be available due to time constraints, the lack of available law enforcement to take prints and/or transportation problems for the subjects to go to and from law enforcement to obtain fingerprints. In addition, many employers are not sophisticated enough and/or do not have established processes and procedures in place to insure that the fingerprints provided by the subject are, in fact, the subject's fingerprints.

In sum, state repositories are and likely will continue to be a key element in developing a complete and accurate criminal record system. As a result, the states should contribute to this process by ensuring the integrity and completeness of the criminal information communicated from the counties to the state databases. The ripple effect should be a higher degree of reliability for the information ultimately housed in federal databases like IAFIS.

15. Any other factors that the Attorney General determines to be relevant to the subject of the report

NAPBS has no comment on this issue.

We hope that these comments are responsive to the questions asked and that you find them useful. Please feel free to contact the undersigned at any time if you have any questions or seek additional information. Thank you for your consideration.

Respectfully,

NATIONAL ASSOCIATION OF PROFESSIONAL BACKGROUND SCREENERS

Jason Morris

Jason Morris
NAPBS 2005-2006 Co-Chair
President
Background Information Services, Inc.
24500 Chagrin Blvd.
Cleveland, OH 44122
Phone: 216-514-2800

Mary Poquette

Mary Poquette
NAPBS 2005-2006 Co-Chair
Executive Vice President, Compliance
Verifications, Inc.
6900 Wedgwood Road North
Minneapolis, MN 55311
Phone: 763-420-0606

EXHIBIT A

**The National Crime Information Center
A Review and Evaluation
August 3, 2005**

Statement of Purpose

This report was prepared on behalf of the National Association of Professional Background Screeners (NAPBS) by Craig N. Winston, under the direction of Lester S. Rosen and Mike Sankey, both members of the Board of Directors of NAPBS.

Its stated purpose was to review the National Crime Information Center and the Interstate Identification System in order to evaluate its effectiveness in maintaining accurate and complete criminal history records.

About the Author

Craig N. Winston is an Assistant Professor of Criminal Justice at Sonoma State University, Rohnert Park, California. He received his Juris Doctor from the University of Akron, Akron, Ohio and his Master of Criminal Justice from the University of North Florida located in Jacksonville, Florida. He also completing post-graduate work at the University of Cincinnati, Cincinnati, Ohio in criminology, research methods and statistics.

His research interests include constitutional law and civil liberties, criminal law and procedure, and community policing. His work has been published in *Police Quarterly* and the *Journal of Crime and Justice*.

INTRODUCTION

The availability of accurate and up-to-date criminal history records is vital to the criminal justice system. The use of this information is also relative for agencies and organizations outside the criminal justice system. Employers such as banks and securities organizations have statutory authority to obtain criminal history information and rely upon it in making their hiring decisions.

Notwithstanding the increased importance and reliance upon criminal history records, a recent report by the Bureau of Justice Statistics (2001) pointed out that many experts suggest that the “accuracy and completeness of criminal history records is the single most serious deficiency affecting the Nation’s criminal history record information systems.”

The report that follows presents a brief overview of the history and development of criminal history records in the United States. The various state and Federal databases are discussed. The accuracy and completeness of the information as well as other attendant problems are then addressed. Finally, current programs established to monitor and improve criminal history records are reviewed and summary of the findings of the study are presented.

HISTORY AND DEVELOPMENT OF CRIMINAL HISTORY RECORDS

In 1908, the U.S. Department of Justice established the Identification Bureau to develop and maintain a fingerprint-based criminal history information system. This system was expanded in 1924, when the FBI, the successor to the Identification Bureau,

was directed by the U.S. Congress to develop an "Identification Division" to maintain manual criminal history records and use fingerprint information for criminal identification and related purposes. Despite these efforts, the Wickersham report, published in 1931, determined that the system was inadequate and recommended that the government undertake major revisions.

A concentrated and organized effort to make improvements in the information compiled by the Identification Bureau did not begin until the 1967 President's Commission on Law Enforcement and Administration of Justice published a report evaluating the Nation's criminal justice system. Crime, the Commission reported, was a serious problem in the United States and the criminal justice system was not equipped to deal with the current crime problem. The Commission called for the establishment of a national criminal history system.

In response to Commission recommendations, the U.S. Department of Justice Law Enforcement Assistance Administration (LEAA) created Project Search. This program was a consortium of states charged with the responsibility of developing a "computerized system for the interstate exchange of criminal history record information" (Use and Management of Criminal Justice Record Information, 2001, 26).

In 1972, LEAA established the Comprehensive Data Systems (CDS) program to encourage states to establish criminal justice information systems. These efforts resulted in the development of the Computerized Criminal History (CCH) component of CDS. CCH contains criminal histories for both Federal and state offenders. By 1976, 26 states joined CCH and began creating criminal history repositories.

Currently, all states maintain some form of criminal history records. A recent study by the Bureau of Justice Statistics indicated that the criminal history records for over 59 million offenders were stored in these repositories. As a general rule, these records contain information including the name of the individual, demographic information such as sex and race, physical characteristics, and driver's license or auto registration information. In addition, the charges and a full set of fingerprints for felonies and serious misdemeanors are maintained. This information is sent to the state repository by reporting jurisdictions.

Similar to state efforts, new developments were also taking place at the Federal level. In 1967, the National Crime Information Center (NCIC) was developed to replace the manual criminal history files maintained by the Identification Division with a computerized criminal history records system. NCIC contained information on stolen vehicles, missing persons, guns, and license plates. A complete listing of the NCIC records can be found in Appendix A. As aforementioned, in the early 1970s, the information available through NCIC was expanded through the creation of the CCH to include criminal history records of persons arrested for Federal and state crimes.

The FBI also maintains the Interstate Identification Index system (III). III does not contain criminal history records, but provides an automated index of names and other identifiers of individuals whose criminal history records are in computerized files. If an authorized agency wishes to learn if an individual has a criminal record, they can query III through NCIC. If the results of the query indicate that the individual has a criminal record (a "hit"), then a second inquiry through NCIC and the National Law Enforcement Telecommunications System can be made to obtain the criminal history. As of 2001, III

contained 52.3 million criminal history files. These files represent 174 million arrest cycles (i.e., some criminal history files contain information related to multiple arrests).

In July of 1999, the FBI implemented NCIC 2000. This revision expanded the type of information available through NCIC (see Appendices B and C). Another aspect of NCIC 2000 was the decentralization of criminal history records. Under NCIC, state records were maintained in both the state and the Federal criminal history repositories. In order to avoid duplication of records, states who participate in the III under NCIC 2000 assume full responsibility for providing criminal history records. If an inquiry results in a hit, III directs the inquiry to the state criminal history record repository, which sends the pertinent information to the agency requesting the information. As of 2004, 47 states were participating in III system. This figure represents an increase of four states since 2000.

The FBI and state repositories also contain “master name indexes” (MNI). An agency wishing to check a criminal history can query the system by using the individual’s name or other identifiers such as sex, race, date of birth, height, weight, and/or hair color. If the query indicates that the individual has a record, the agency can request the individual’s complete criminal history.

Notwithstanding the increased participation in III, access to state criminal history records, a key component to the success of NCIC 2000, continues to be a problem.

A recent report by the Bureau of Justice Statistics indicated that as of 2001, 22 reporting jurisdictions indicated that at least 75% of their criminal history records were accessible through III; 15 reported that 50 – 75% of their records were accessible; and 14 indicated that less than 50% of their records were III accessible.

One additional point bears review. Automation is an integral part of the effectiveness of III. While significant strides have been made in this regard, as of 2001 only 30 states had at least 90% of their records automated (27 of these states indicated that their criminal history records were fully automated). Six states reported that less than 70% of their criminal history records were automated.

As pointed out previously, the accuracy of state and Federal criminal history databases is vital to law enforcements agencies, courts and other components of the criminal justice system, and select industries that have access to this information. The importance of valid records was emphasized by Richard Thornburgh, former U.S. Attorney General when he stated in the *Use and Management of Criminal History Record Information, 2001*, “[There is a] ‘straight-line relationship’ between high-quality criminal history information and the effectiveness of the Nation’s criminal justice system.” Despite the obvious importance of precise data, there are serious deficiencies in the information contained in state and therefore Federal criminal history records. These concerns include accuracy and completeness, timeliness, method of inquiry, and linking/tracking capabilities.

It is also imperative to emphasize that the validity of criminal history records concerning state crime, and therefore the information available through NCIC, is totally dependent upon the reporting policies and practices of the various states. It is this area that the majority of problems arise.

EVALUATION OF DATA QUALITY

Content

The content of state repositories is governed by state law and is dependent upon the reporting practices of the state. State laws do vary in relation to the reporting requirements. While the laws in all states and the District of Columbia require that arrest and charge information be reported to their state criminal history repository, research indicates that problems with accuracy and completeness of this information, as well as the timeliness of transmission to the state repositories persist.

In order for a criminal history record to be complete it should include the following:

1. arrest and charge information
2. identifying information including fingerprints
3. prosecutor declinations
4. final dispositions (including dismissal and reduction in charge)
5. admission/release of felons and perpetrators of serious crimes
6. probation and parole information
7. modification of felony conviction

Though, as pointed out above, all states report arrest and charge information, there is some variation in the reporting laws concerning issues such as disposition, declination to prosecute, and failure to charge after fingerprints and case information have been forwarded to the state repository. Thirty-five states require that dispositions be forwarded to the state repository, but of the 174 million arrest cycles on file only 45% have dispositions. In 47 states, information concerning declination to prosecute is sent to

the state repository. As of 2001, however, only 5 states reported that all prosecutorial declinations were transmitted to their respective repositories. In addition, only 31 states require updated information to be sent to the state's repository if a person is not charged after the individual has been arrested and their fingerprints have been submitted. Reporting requirements related to expungements, pardons, restoration of rights, and other issues also vary from state to state. These variations have a significant impact on the quality of data available.

A second issue related to accuracy and content is the lack of uniformity in the criminal codes of the various states. As a general rule, the types of activities that are prohibited are consistent throughout the states. There are, however, some inconsistencies that could influence the validity of the criminal history records due to differences in classifications of behaviors. These records contain information related to serious misdemeanors and felonies. Whether a state defines a particular act as a misdemeanor or a felony may impact the reliability of the criminal history records.

Theft provides a good illustration of this problem. One of the criteria, which is used to distinguish between a misdemeanor theft and a felony theft is the value of the item(s) stolen. This amount differs greatly from state to state. In Florida, the theft of an item worth more than \$300.00 is a felony. In California, the threshold amount for a felony theft is \$400.00; while in Ohio and Maryland \$500.00 delineates the difference between a misdemeanor and a felony.

Crimes related to controlled substances present a similar problem. In Wyoming, possession of more than 85 grams of marijuana is a felony, while the same act in Texas, Ohio, New York, or California would be a misdemeanor. Sale of any amount of

marijuana is a felony in California and Texas, but the sale of up to 25 grams in New York or 20 grams in Ohio would be a misdemeanor. These and similar discrepancies can impact which crimes are reported to the state repository and therefore the accuracy of the information that is available through the state and Federal criminal record history systems.

Timeliness

The timeliness of transmission of data relevant to a criminal case is a significant issue and clearly impacts the validity of the information. Table 1 summarizes the major findings of a recent Bureau of Justice report (2005) concerning the timeliness of the data contained in state criminal history records.

TABLE 1. Average Number of Days for Repositories to Receive and Process Criminal History Data.

ACTIVITY	DAYS
Arrest information	24
Court disposition	46
Prison admission	31

Source: *Improving Access to and Integrity of Criminal History Records, 2005*

The utility of a criminal history record is dramatically affected by the lack of up-to-date information. This fact was emphasized by an administrator in a correctional facility in a Mid-Western state. When discussing the importance of accurate criminal history records, he stated that the biggest problem he experienced was the fact that dispositions were not generally available. He went on to point out that this presented problems when hiring new employees or evaluating rehabilitation efforts. In addition to the problem of timely transmission of dispositions, linking the disposition to the proper file is also a major concern. This issue will be explored in more detail in the next section.

Linking Case Histories and Individuals

One of the most serious data quality issues is linking the data to the proper individual and case. When an individual is arrested for the first time, he or she is assigned a unique number. This number should allow accurate storage and retrieval of criminal records associated with this individual. Unfortunately, due to the use of aliases, false identifiers, and clerical errors, duplicate records can be created. These problems are generally remedied when fingerprints are used to process subsequent cases, but discrepancies may still be present. A more serious problem arises when attempts are made to integrate correctional dispositions with information related to the arrest and charge. This situation is exacerbated when the individual has more than one pending case or the disposition information does not match the charge data due to plea bargaining agreements or reduction in charges.

Many states have successfully overcome the problem of linking information related to the charge and disposition by implementing a "case tracking" system that integrates the individual's name with a case identification number. According to a recent report published by the Bureau of Justice Statistics, however, there are still significant problems linking dispositions with the appropriate case. In 2001, 14 states estimated that over 700,000 of their final court dispositions could not be linked to arrest or charging files. This represents an average of over 50,000 per state. Sixteen additional states estimated the percentage of dispositions that could not be linked to the appropriate case. Table 2 sets forth this information..

TABLE 2. Percentage of Dispositions Not Linked to Charge or Arrest Information

Number of States	% of Dispositions
2	50%
3	30 – 40%
2	25%
9	10%

Source: *Improving Access to and Integrity of Criminal History Records, 2005*

In addition, problems persist when attempting to integrate arrest information with disposition when the case has been modified by factors such as plea-bargaining or other modifications of the charge reported at the time of arrest. The use of a charge-tracking system has been able to reduce the problem, but efforts to improve its implementation are still underway.

Format and Terminology

Two additional concerns have been raised related to the quality of the data contained in criminal history records. First, the formats that are used by the various states are not consistent. These inconsistencies can create a situation where some records may contain blank data fields or fields that simply contain the word “unknown.” Differences in terminology can create difficulties for individuals attempting to interpret the data. The implementation of the III program in 1999 has increased the magnitude of these problems. Prior to 1999, the FBI provided the information requested in national searches. Problems in interpretation were eliminated since the FBI incorporated state information into a standard format. Despite the fact that the new system relies upon the states to provide criminal history records, some states are not formatting their information according to FBI standards. This problem and others have created the need for reforms in the content and format of criminal history records.

False Positives/Negative

Clearly, the lack of consistency in the data reported and the timeliness of reporting and entering the data are significant problems. Another problem is presented when the inquiry is based upon the individual's name and other personal identifiers other than fingerprints. These types of inquiries are typically done by noncriminal justice organizations including Federal and state agencies that have been authorized by law to obtain criminal history records.

To illustrate, the records maintained in the III index are those of individuals who have been arrested or formally charged with a serious misdemeanor or felony. A name search should result in a "hit" if the individual's name is found in the index due to some previous involvement with the criminal justice system. Studies have indicated, however, that name searches can result in two types of errors. The first, a "false positive," occurs when the search indicates that the individual's name is in the MNI and therefore has a criminal record when, in fact, he or she does not. The other possible error is a "false negative" or an indication that the individual does not have a criminal record when in fact he or she does.

In order to obtain a clear picture of the accuracy of name searches, a task force was formed during the late 1990s consisting of the Bureau of Justice Statistics, the Florida Department of Law Enforcement, the Department of Housing and Urban Development, and the FBI. The purpose of this task force was to compare the accuracy of identifications made using name checks through III and those using a fingerprint-based search of the FBI's records. The task force analyzed the results of 93,274 background checks from Florida licensing or employment applicants, 323 public housing applicants,

and 2550 volunteers. The results indicated that when compared to fingerprint-verified criminal histories, name-checks yielded 11.7% false negatives and 5.5% false positives. In other words, of the 10,673 subjects who were found to have a criminal record by fingerprint-verified search, the name check search indicated that 1,252 did not have records (false positives). Similarly, of the 82,610 individuals who were determined not to have a criminal record by the fingerprint-verified search, the results of the name check indicated that 4,562 had criminal records (false negatives).

Based upon the findings of this study, the 6.9 million fingerprint-verified background checks conducted by the FBI in 1997 would have resulted in 346,000 false positives and 70,200 false negatives if a name check verification had been used.

It becomes apparent that name checks alone would result in large numbers of persons being improperly disqualified for employment. In addition, persons who may pose some risk because of their criminal record are not discovered.

In order to deal with this problem, NCIC 2000 contains an "enhanced name search" database. For example, a search under the name of "James" will also return records on a "Jim", or "Jimmy". Notwithstanding this improvement, cases where the individual is using an alias or a false identity remain problematic. One of the reasons cited for the continued use of name checks is the time it takes to process fingerprint identification. The implementation of the Integrated Automated Fingerprint Identification System (IAFIS) in 1999 addressed this problem and can provide responses to fingerprint identification requests within 24 hours.

The use of fingerprints, though more accurate, does have privacy and logistic problems associated with it. The III index and the Integrated Automated Fingerprint

Identification System (IAFIS) contain information on individuals who have been arrested. In order for a fingerprint search to return accurate results, the individual's prints must be on file.

THE NATIONAL CRIME PREVENTION AND PRIVACY COMPACT

The recent move to NCIC 2000 signaled a change in the way in which criminal history records are maintained and utilized. When it is fully implemented, each state will be responsible for providing criminal history records through III. State laws regarding the dissemination of these records create problems in this regard. Though all states provide access to the criminal history records for criminal justice agencies, the laws of many states do not authorize access to these records by noncriminal justice agencies and organizations. In order to deal with this problem, the U.S. Congress passed Senate Bill 2002 that established the National Crime Prevention and Privacy Compact. The stated purpose of the Compact is "to facilitate authorized interstate criminal history record exchanges for noncriminal justice purposes" (Section 212, paragraph 4). The states are also required to review each request and response and delete any information that may not be released according to state law. It is interesting to note that as of 2003, 44 states were participating in the Interstate Identification Index Program, but only 16 were members of the National Crime Prevention and Privacy Compact (See Appendix D). Until all states take part in the Compact, access to criminal history records will not be consistent throughout the country.

CONCLUSION

The purpose of this report was to provide summary information concerning the NCIC and to examine the quality of the state data accessible through NCIC. In order to accomplish this, a brief history of the development of criminal history records was presented as well as a discussion of the current criminal history and related databases maintained by the states and the Federal government.

Since the establishment of the first nationwide criminal history repositories, there have been numerous revisions in an effort to upgrade the accuracy of the information contained therein. Today, the FBI and all 50 states maintain criminal history repositories to aid the criminal justice system and select noncriminal justice agencies and organizations. Recently, changes such as the revision to the NCIC and III have been made to improve the content and accessibility of the information. In 1995, the National Criminal History Improvement Program (NCHIP) was established. This program provides grants to states to work on the improvement of NCIC and increase participation in the III program. This program has been successful in many regards. The number of automated records increased 35% from 1995 to 2001. The number of states participating in the III program increased from 26 in 1993 to 47 in 2004. In addition, under NCHIP, participating states have been able to improve their information pertaining to domestic violence and sex offender registries and take advantage of the latest technology.

Despite these ongoing efforts, significant problems in the accuracy and validity of the information contained in the state criminal history depositories remain. These problems can be summarized as follows:

- Many states do not report information concerning dispositions, declinations to prosecute, failure to charge after fingerprints have been submitted, and expungements.
- Inconsistency in the various states' reporting requirements and criminal codes impacts the completeness and accuracy of the records.
- The timeliness of transmission by the local jurisdictions to the state criminal history repositories remains problematic.
- There are still significant time lags between the time information is transmitted to the state repository and entry into the criminal history records.
- The process used to linking data to the proper individual and case is still ineffective.
- Serious problems remain in the process to link dispositional information to the proper case and charge.
- The format and terminology used by the various states creates problems of interpretation for individuals in other states who are using the information.
- The use of name checks has been proven create serious identification problem.
- Differing laws related to dissemination of criminal history records pose significant problems for the implementation of the III program.

It cannot be overemphasized that the deficiencies in state criminal history records present serious problems for the various agencies and organizations that are dependent upon the information they provide. Continued efforts are needed in order to insure that the problems discussed in this report are addressed and the reliability of these records improved.

Sources Consulted

- Criminal Justice Information Services (CJIS) Division(2003). *National Crime Information Center*. Web site: www.fas.org/irp/agency/doj/fbi/is/ncic.
- Criminal Justice Information Services (CJIS) Division(2003). *National Crime History Improvement Program*. Web site: www.fas.org/irp/agency/doj/fbi/is/ncic.
- Date, Shruti. (2005). FBI network prevails over early glitches. Retrieved from, http://appserv.gen.com/state/vol_5no10/news/482-1.html
- FBI National Press Release. (July 15, 1999) Retrieved from, www.fbi.gov/pressrel/pressrel99/ncic2000.htm.
- Federal Bureau of Investigation. National Crime Information Center (1993) *a snapshot of the future*. Web site: www.fbi.gov
- Giles, Frederick G. (2002). The Myths and Realities of On-line Criminal History Databases. Retrieved from <http://www.ci-wackenhut.com>
- Hinton, Derek. ((2004). *The Criminal Records Manual*. Tempe, AZ: Facts on Demand Press
- Illinois Criminal Justice Information Authority. (2003) *Sharing criminal history record information: the Interstate Identification Index*. Web site: www.Icjla.org.
- Illinois Criminal Justice Information Authority. (2003) *Results of the 2003 Criminal History Record Information Audit*. Web site: www.Icjla.org.
- Loesch, David R. (May 18, 2000). *Statement for the Record of David R. Loesch...on Crime Regarding HR 3410 and Name Check Efficacy* Retrieved from www.fbi.gov/congress/congress/loesch062100.htm<http://lcweb2.loc.gov/mster/minerva/107/senate/www>.
- Loesch, David R. (June 21, 2000). *Statement of David R. Loesch...Before the Committee on the Judiciary*. Retrieved from, http://judiciary.senate.gov/oldsite/6212000_drl.htm
- McCue, C., Stone, E.S., and Gooch, T.P. (November 2003). Data Mining and Value-Added Analysis." *FBI Law Enforcement Bulletin*, 1 – 6.
- Rosen, Lester S. (2005). *The Safe Hiring Manual*. Tempe, Arizona: Facts on Demand Press
- Sprecher, Milford H. (1995) States Gearing up for NCIC 2000. Retrieved from, www.govtech.nte/magazine/gt/1995/jan/ncic.php

- Tillett, Scott L. (1999). FBI turns on new crime-fighting system. Retrieved from, www.fcw.com/fcw/articles/1999/fcw_7151999_fbi.asp
- U.S. Department of Justice. Office of Justice Programs. (2005) *Improving Access to and Integrity of Criminal History Records*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Federal Bureau of Investigation. (2004). *Interstate Identification Index (III) National Fingerprint File (NFF) Program*. Washington DC: Government Printing Office.
- U.S. Department of Justice. Bureau of Justice Statistics. (2002) *Linking Uniform Crime Reporting Data to Other Datasets*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. (2001). *Increasing the Utility of Criminal History Record: Report of the National Task Force*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services. (2001) *Interstate Identification Index Status Report*. Washington, DC: U.S. Government Printing Office.
- U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services. (2001). *The Investigative Tool*. Washington, DC: U.S. Government Printing Office.
- U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services. (2001). *Areas of Liability for the Criminal Justice System Administrator*. Washington, DC: U.S. Government Printing Office.
- U.S. Department of Justice. Bureau of Justice Statistics. (2001). *Survey of State Criminal History Information Systems 2001*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. (2001). *Use and Management of Criminal Justice Record Information: A Comprehensive Report, 2001 Update*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. (2000). *Continuing Criminal History Records Improvement Evaluation, Final 1994 – 98 Report*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Federal Bureau of Investigation. (2000). *National Crime Information Center (NCIC) NCIC File Reference Card*. Washington DC: Government Printing Office

- U.S. Department of Justice. Federal Bureau of Investigation. (2000). *NCIC: An Overview*. Washington DC: U.S. Government Printing Office.
- U.S. Department of Justice. Bureau of Justice Statistics. (1999). *Intestate Identification Index*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. (1999). *Interstate Identification Index Name Check Efficacy: Report of the National Task Force to the U.S. Attorney General*. Washington, D.C. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. (1997). *Implementing the National Incident-Based Reporting System: A Project Status Report*. Web site: www.usdoj.gov/bjs/pub
- U.S. Department of Justice. Bureau of Justice Statistics. *Integrated Automated Fingerprint Identification System or IAFIS. What is it?* Web site: www.fbi.gov.
- U.S. Department of Justice. Bureau of Justice Statistics. *National Conference on Criminal History Records: Brady and Beyond*. Web site: www.usdoj.gov/bjs/pub
- Woodmacy, Donald A. (1989) *National Crime Information Center. Law Enforcement System is Getting a Major Face-lift*. Government Technology Magazine.

**APPENDIX A
NCIC Databases**

**Stolen Articles
Foreign Fugitives
Stolen Guns
Criminal History Queries
Stolen License Plates
Deported Felons
Missing Persons
Criminal Justice Agency Identifier
Stolen Securities
Stolen Boats
Gang and terrorist members
Unidentified Persons
United States Secret Service Protection File
Stolen Vehicles
Persons Subject to Protective Orders
Wanted Persons
Canadian Police Information Center**

APPENDIX B NCIC 2000 Databases

Stolen Articles
Foreign Fugitives
Stolen Guns
Criminal History Queries
Stolen License Plates
Deported Felons
Missing Persons
Criminal Justice Agency Identifier
Stolen Securities
Stolen Boats
Gang and terrorist members
Unidentified Persons
United States Secret Service Protection File
Stolen Vehicles
Persons Subject to Protective Orders
Wanted Persons
Canadian Police Information Center
Enhanced Name Search
Search of right index finger prints
Mugshots
Other identifying images such as scars, tattoos
Sexual Offenders
Persons on Probation or Parole
Persons incarcerated in Federal prisons
User manuals
Information linking
Improved data quality
On-line as hoc searches
Maintaining five days of system inquiries to allow agencies to be notified if they are looking for information on the same case

APPENDIX C
Information on File in NCIC
(Federal Bureau of Investigation, 2005)

Criminal History Files:	52.3 million criminal history records (containing 174 arrest cycles)
Convicted Sex Offender Registry File:	395,250
Gang and Terrorist Members:	165,200
National Protection Order Files:	924,000
Wanted Persons/Wants and Warrants: (not including juveniles, Canadian warrants, foreign fugitives)	1,195,000

APPENDIX D
Compact States
2003

Alaska
Arizona
Arkansas
Colorado
Connecticut
Florida
Georgia
Iowa
Kansas
Maine
Minnesota
Montana
Nevada
New Jersey
Oklahoma
South Carolina