U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services (CJIS) Division

CJIS Information Letter April 6, 2001

MISUSE OF III VIA PURPOSE CODE C

Introduction

With some notable exceptions, access to the Interstate Identification Index (III) is limited to criminal justice agencies for criminal justice purposes. Periodically, the Director of the FBI and the Assistant Director of the Criminal Justice Information Services (CJIS) Division have warned that misuse of the III and other CJIS-managed systems may constitute a federal criminal violation and expose the offending agency to termination of services. (See *Letter to All Fingerprint Contributors* dated October 21, 1977; December 9, 1988; and November 30, 1989.) A recent increase in the reporting of misuse warrants the need to reaffirm the limitations under which access to III via Purpose Code C operates and to outline the potential criminal and administrative responses to misuse of III.

History of FBI-Managed Criminal History Record Information (CHRI)

Since 1921, the FBI has been statutorily authorized to collect and disseminate CHRI to certain recipients. Effective June 11, 1930, such authority was codified at 5 *United States Code* (U.S.C.) §340. That section was revised and renumbered effective August 31, 1964, as 5 U.S.C. §300, which in turn was revised and renumbered in 1966 as the current 28 U.S.C. §534. Pursuant to Executive Order 10450, effective April 27, 1953, the FBI was also authorized to provide CHRI to federal agencies for employment purposes.

Before 1971, there were many instances in which the FBI responded to inquiries for CHRI for noncriminal justice purposes. At that time, the Bureau's largest clients were federally regulated and insured financial institutions, which are precluded by 12 U.S.C. §1829 from allowing certain convicted persons to participate in the operation of a bank. This practice ceased with the decision of the United States District Court for the District of Columbia in *Menard* v. *Mitchell*, 328 F. Supp. 718 (D.D.C. 1971), in which the court determined that the FBI was without authority to disseminate arrest records outside the federal government for employment, licensing, and other noncriminal justice purposes.

As a result of that decision, the FBI stopped disseminating CHRI for nonfederal, noncriminal justice purposes until December 26, 1971, when the President signed Public Law (Pub. L.) 92-184, 85 Stat. 627, 642 (1971). In addition to authorizing FBI exchanges of CHRI with federally chartered or insured banking institutions, Pub. L. 92-184 provided statutory authority to disseminate FBI-maintained CHRI "for the purposes of employment and licensing if authorized by State statute and approved by the Attorney General." On November 29, 1972, Pub. L. 92-184 was superceded by Pub. L. 92-544, 86 Stat. 1115 (1972), which contains similar provisions and is still in effect.[(1)] In the *Letter to All Fingerprint Contributors* dated January 20, 1972, the FBI announced the enactment of Pub. L. 92-184, including the requirement of a state

statute approved by the Attorney General in order to access FBI-maintained CHRI.

Criminal vs. Noncriminal Justice Use of III

The National Crime Information Center (NCIC) operates under the authority of 28 U.S.C. §534, which permits the exchange of information "with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions." The dissemination of CHRI contained in the III system is further governed by 28 *Code of Federal Regulations* (C.F.R.) §20.33, which is principally limited to "criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies . . . ." This restriction similarly agrees with NCIC policy.[(2)]

The distinction between criminal justice and noncriminal justice--and, therefore, the authority to access III in the absence of additional statutory authority--depends upon satisfaction of any of the "administration of criminal justice" functions listed at 28 C.F.R. §20.3(b).[(3)] Of these, the function of "detection" most often invites misuse from overly broad interpretation.

For the detection function to be triggered, there must be an "articulable suspicion" or "reasonable basis" to run III on a particular subject. As FBI Director Louis J. Freeh stated in correspondence to a federal agency requesting broad authority to background individuals, he was concerned about access "without any specific criminal activity identified or even alleged . . . . [Rather, III should be used] when specific criminal activity has been identified and is being investigated . . . . [The requirement demands] specific evidence of a particular crime [as] the basis for the . . . checks, not the ever present potential for criminality."

Consequently, "detection" is typically specific to the individual and is interpreted narrowly. As previously mentioned, although federally chartered or insured banking institutions had an obligation to avoid hiring certain individuals, it required the enactment of Pub. L. 92-544 to expressly authorize such access. What has been popularly termed "preventive law enforcement" cannot serve as an "administration of criminal justice function," whether one attempts to characterize it as "detection" or otherwise. The screening of a particular population in the absence of a particularized suspicion, in an effort to detect prohibited persons or criminal activity, is not considered "detection" and is unauthorized.[(4)]

As the banking industry example illustrates, a mere legal obligation, prohibition, or administrative responsibility unaccompanied by statutory authority to access FBI-maintained CHRI precludes access to such information to enable the agency to fulfill its mission. For example, the Adoption and Safe Families Act of 1997, 42 U.S.C. §671(a), obligates the states to ensure that adoptive or foster care parents do not receive federal assistance if they have a "felony conviction for child abuse or neglect, for spousal abuse, for a crime against children (including child pornography), or for a crime involving violence, including rape, sexual assault, or homicide, but not including other physical assault or battery . . . ." However, both the FBI and the Department of Health and Human Services agreed that there was no accompanying authorization to access the FBI's records to determine an applicant's suitability.

Similar to the quandary faced by the banking industry, 18 U.S.C. §1033(3)(1)(A) makes it a felony for anyone previously convicted of a felony involving dishonesty or breach of trust to

engage in the sale or business of insurance. Such statute, however, would not entitle state insurance commissioners (or criminal justice agencies acting on their behalf) to access NCIC III to "run" insurance agents to discover violations of this law. This is not an administration of criminal justice function, and there is no federal statute authorizing such checks.[(5)] Likewise, 29 U.S.C. §504 prohibits most felons from holding office in a trade union, a violation of which is punishable by a fine up to $10,000 and/or imprisonment up to 5 years. Yet this prohibition would not give the National Labor Relations Board (or local law enforcement) the right to access NCIC III to "detect" violators.

As a result of these limitations, about a dozen federal statutes have been enacted authorizing access to FBI-maintained CHRI for such purposes as screening employees in the nuclear power, aviation, and Indian gaming industries. Each of these uses--because they do not involve the administration of criminal justice--required legislation.

Furthermore, with rare exception, access to FBI-maintained CHRI for noncriminal justice purposes must be made by submitting fingerprints. In 1986, the CJIS Advisory Policy Board (APB) (created pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. 2) published the *Concept for the Exchange of Criminal History Records for Noncriminal Justice Uses by Means of the III*. The FBI endorsed and adopted the concept paper. Among other things, it mandates the submission of fingerprints to access FBI-maintained CHRI for noncriminal justice purposes.[(6)]

Conversely, for a request for CHRI to be for a "criminal justice purpose" it must be for an "administration of criminal justice" function as outlined in 28 C.F.R. 20.3(b). If the request does not fall within one of these functions--and, therefore, would be covered by the FBI's generic authority provided by 28 U.S.C. 534--there must be specific federal or state statutory authority for legal access to FBI-maintained CHRI.

In part, this result is mandated by the Privacy Act (5 U.S.C. §552a), which regulates dissemination of records by federal agencies and obligates these agencies to record each instance of and the purpose for dissemination. (See *Federal Register* of September 28, 1999 [the FBI's most recent notice under the Privacy Act]). The FBI also created NCIC purpose codes and maintains an automated system to log each inquiry and dissemination of a III record and the purpose for which it was accessed. Thus, when Purpose Code C is indicated, it must accurately reflect that the access was for a Section 20.3(b) purpose (as those terms are properly used). The FBI also uses the automated logging system to conduct compliance audits of agencies with access to III.

Remedies Available

All agencies with NCIC access sign user agreements with the state Control Terminal Agency which, in turn, signs a user agreement with the FBI. These agreements acknowledge that local and state agencies' personnel are familiar with, and will comply with, federal law and policy regarding proper use of NCIC III. The CJIS APB Sanctions Subcommittee has the authority to recommend administrative penalties for misuse, including termination of service. This administrative penalty is consistent with the language of both 28 U.S.C. §534 and Pub. L. 92-544.

Additionally, depending upon the nature of the offense and the identity of the

offender, several crimes could be charged for misusing III, including 18 U.S.C. §641 (theft of government property); 18 U.S.C. §1029 (fraudulent use of an access device), 18 U.S.C. §1030 (misuse of a protected computer), 18 U.S.C. §1343 (wire fraud, including false pretense or misrepresentation), 18 U.S.C. §1951 (misuse of public office duties), and 5 U.S.C. §552a (violation of the Privacy Act). Furthermore, several recent prosecutions have been based upon state criminal code violations similar to the federal offenses cited.

In summary, it is incumbent upon the user community to access III consistent with federal law and policy or risk administrative and criminal sanctions.[(7)]

FBI USER FEES TO BE IMPOSED UPON PRIVATE CONTRACTORS PERFORMING AN ADMINISTRATION OF CRIMINAL JUSTICE FUNCTION

Several states have inquired about the FBI's User Fee Policy as it relates to applicant fingerprint submissions of individuals employed by private concerns under contract with criminal justice agencies to perform activities described in 28 C.F.R. §20.33. Specifically, several agencies have asked whether private contractors would be subject to the user fee (consistent with the FBI practice of imposing fees regarding private sector employees under the authority of Pub. L. 92-544) or whether the FBI would provide such service for free (consistent with the past practice involving the background investigation of applicants for employment with governmental law enforcement agencies).

Traditionally, Congress has directly funded the FBI to provide fingerprint and other criminal justice information services to local, state, and federal criminal justice agencies for the administration of criminal justice, which has been interpreted to include the hiring of criminal justice employees. With privatization, the question arises whether a private, for-profit company that has a contract with a law enforcement agency may receive free fingerprint-based criminal history checks of its employees.

28 C.F.R. §20.33(a)(1) includes within its purview the screening of employees or applicants for employment hired by criminal justice agencies, and the fingerprint submissions of these employees and applicants are processed at no charge. The recent change to the C.F.R. permitting private contractors to engage in activities in support of criminal justice agencies does not change the status of such contractors. Employees of a contractor, while performing an administration of criminal justice function, do not become criminal justice employees. They remain employees of the private contractor and are not converted to governmental employees (nor is the company converted to a criminal justice agency) merely because they have access to criminal history record information to perform their duties similar to that available to criminal justice governmental agency employees. For FBI billing purposes, private contractor employees are considered private employees regardless of assignment. Since private contractor employees falling within the scope of Section 20.33(a)(7) are not criminal justice governmental employees, they cannot receive free FBI criminal history background checks.

Therefore, the FBI has concluded that a private company may not receive no-cost fingerprint checks of its employees even though its contract is in support of a criminal justice agency. Those private contract employees performing an administration of criminal justice function pursuant to 28 C.F.R. §20.33(a)(7) are assessed a fee of $22 for billing and $24 for nonbilling states and U.S. territories. All states and territories other than Massachusetts,

Pennsylvania, Kentucky, and Guam are billing states. The *FBI Security Addendum*, Sections 6.01 and 6.02, dated October 1999, and the *CJIS Security Policy*, dated August 2000, particularly when read together, reflect that the contracting governmental agency **must** perform these required checks. The applicant fingerprint cards must bear the ORI number of the contracting governmental agency, and to avoid confusion, the words "Contract Employee" must be clearly indicated in the "Reason Fingerprinted" block.

Recently, the FBI received applicant fingerprint cards bearing the ORI number of a private contractor for the purpose of performing criminal background checks of its employees. These cards have been processed. However, future submissions must be submitted as stated above. Effective June 4, 2001, all applicant fingerprint card submissions for private contractor background checks will be subject to the appropriate user fee.

PUBLIC LAW 92-544 CRITERIA CLARIFIED

As noted earlier, before 1971, the FBI exchanged records with local, state, and federal agencies for both criminal and noncriminal justice uses; however, this practice was curtailed by the decision in *Menard* v. *Mitchell*, 328 F. Supp. 718 (D.D.C. 1971), which held that "Congress never intended to or in fact did authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks. . . . Thus the Court finds that the Bureau is without authority to disseminate arrest records outside the Federal Government for employment, licensing or related purposes whether or not the record reflects a later conviction." 328 F. Supp. at 726-27.

Congress remedied the situation by enacting Pub. L. 92-184, 85 Stat. 627, 642 (1971), superceded by Pub. L. 92-544, 86 Stat. 1115 (1972), which states:

> The funds provided for Salaries and Expenses, Federal Bureau of Investigation, may be used hereafter, in addition to those uses authorized thereunder, for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions, and, if authorized by State statute and approved by the Attorney General, to officials of State and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of any such official and subject to the same restriction with respect to dissemination as that provided for under the aforementioned appropriation.[(8)]

Since 1972, the FBI, with the assistance of the Department of Justice, has determined the parameters for approving state statutes under Pub. L. 92-544. The criteria are:

1. The statute must exist as a result of a legislative enactment.

2. It must require that applicants be fingerprinted.

3. It must, expressly or by implication, authorize the use of FBI records for the screening of applicants.

4. It must identify the specific category(ies) of licensees/employees falling within its purview, thereby avoiding overbreadth.

5. It must not be against public policy.

6. It must not identify a private entity as the recipient of the results of the record check.

As a result of a motion made by the CJIS APB at its meeting of December 6-7, 1995, the FBI notified all NCIC Control Terminal Officers of these standards[(9)] in a February 8, 1996, letter.

However, the third criterion has proven problematic. In applying that criterion, the FBI's historic position has been that a state statute must, on its face, require submission of candidate fingerprints to the FBI rather than merely permit such submission. This insistence upon backgrounding all applicants discouraged rather than encouraged use of FBI services, an unexpected result inconsistent with the congressional intent of again making such services available for noncriminal justice licensing and employment purposes after *Menard*. This inconsistency was highlighted by the passage of the Volunteers for Children Act (VCA), Sections 221 and 222 of Pub. L. 105-251 (1998). Under the VCA, a qualified entity's decision to request a background check is discretionary.

The FBI has therefore reviewed the third criterion and has determined that, inasmuch as Pub. L. 92-544 merely requires that access to FBI CHRI be "authorized" by an approved state statute--rather than "required" by such statute--discretionary language ("may") is acceptable in lieu of mandatory language ("shall") regarding applicant submissions to the FBI.[(10)] Statutes recently rejected solely because of language making applicant submissions to the FBI discretionary should be resubmitted to the Access Integrity Unit for review.

---

1. Additionally, federal statutes authorize access to FBI-maintained CHRI in specific areas, e.g., the securities industry (15 U.S.C. §78q), the commodities and futures industry (7 U.S.C. §12a and 21(b)(4)(e)), nuclear regulatory licensees (42 U.S.C. §2169), the aviation industry (42 U.S.C. §44936), private railroad and college police (28 U.S.C. §534), parimutuel betting (28 U.S.C. §534 note), and federal child care facility employees (42 U.S.C. §13041).

2. For example, although federal agencies are authorized to receive CHRI for the purpose of noncriminal justice employment, FBI policy does not permit access to III for this purpose; instead, the fingerprints of prospective federal employees must be submitted to the FBI.

3. Section 20.3 states in pertinent part:

> Administration of criminal justice means performance of any of the following activities: Detection, apprehension, detention, pre-trial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

4. The other "administration of criminal justice" functions listed at 28 C.F.R. §20.3(b) involve persons who are already "participants in" the criminal justice system. By its nature, "detection" occurs at the start of the process and, hence, would be limitless in scope were it not constrained by the requirement that a reasonable basis particular to the individual be articulable.

It should also be noted that the requirement of a "particularized suspicion" does not rise to the level of "probable cause" necessary to obtain an arrest or search warrant but is a lesser standard consistent with the minimal invasiveness of the III check.

5. A number of states have Pub. L. 92-544 statutes authorizing such checks of insurance agent applicants by fingerprint submission. See Arizona (Ariz. Rev. Stat. Ann. §20-142), California (Cal. Ins. Code §704.5), Florida (Fla. Stat. §626.171), and Idaho (Idaho Code §41-1043).

6. In October 1998, Pub. L. 105-251 (the National Crime Prevention and Privacy Compact) was enacted. This Interstate Compact, of which the FBI and an increasing number of states are members, governs use of CHRI for many noncriminal justice purposes. A principal requirement of the Interstate Compact is that the submission of fingerprints is required for noncriminal justice purposes.

7. This *CJIS Information Letter* is not meant to address access to III via purpose codes other than C which, as administrative (and not investigatory) purpose codes, are governed by different rules. Nonetheless, users of these other purpose codes are subject to audits and exposed to criminal and administrative sanctions for misuse.

8. The referenced provision in the appropriation bill warns that "such exchange to be subject to cancellation if dissemination is made outside the receiving departments or related agencies" and that restriction is incorporated into the licensing and employment provisions of Pub. L. 92-544.

9. Although some state statutes require that fingerprints be initially submitted to the state identification bureau (for a check of state records) and then forwarded to the FBI for a "national" criminal history check, this is not a criterion and is not found in most state statutes. It does, however, agree with FBI policy and is adhered to by the states.

10. Resolution of the "may/shall" distinction should not be confused with the requirement that a check of FBI-maintained CHRI for licensing and employment purposes pursuant to Pub. L. 92-544 be fingerprint-based. Hence, if applicants are to be subjected to an FBI background check, then they must be fingerprinted and the fingerprints submitted to the FBI.

ACCESS TO CRIMINAL HISTORY RECORDS BY NON-GOVERNMENTAL ENTITIES

PERFORMING AUTHORIZED CRIMINAL JUSTICE FUNCTIONS

Non-governmental entities performing authorized criminal justice functions under contract with government law enforcement agencies may be granted access to criminal history records maintained under the authority of 28 U.S.C. § 534, subject to effective controls to guard against unauthorized use and to insure effective oversight by the Department of Justice.

Because Department of Justice regulations implementing 28 U.S.C. § 534 do not affirmatively authorize dissemination of criminal history records to non-governmental entities under contract to assist law enforcement agencies, those regulations should be amended to provide such authorization before access is granted to those entities.

June 12, 1998

LETTER OPINION FOR THE DEPUTY DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION

This responds to your request for our legal opinion concerning the circumstances in which non-governmental entities performing criminal justice functions under contract with government law enforcement agencies may be granted access to criminal history records information ("CHRI") subject to the provisions of 28 U.S.C. § 534 (1994).[(1)] We conclude that the Attorney General, or her delegee,[(2)] may permit such access in appropriate circumstances under § 534. Should the Attorney General decide to do so, we believe that the governing regulation, 28 C.F.R. pt. 20 (1997), should be amended in accordance with the rulemaking requirements of the Administrative Procedure Act ("APA"), see 5 U.S.C. § 553 (1994), for the reasons discussed below. Finally, any proposal to permit contractor access to CHRI must incorporate effective controls to guard against unauthorized use or release of CHRI by the contractors and to insure that the Department can maintain effective oversight.

I.

Section 534 directs the Attorney General to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records" and to "exchange such records and information with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and

other institutions."[(3)] 28 U.S.C. § 534(a)(1), (4). The statute thus requires the Attorney General to collect, maintain, and exchange criminal identification records with federal, state, and local criminal justice agencies. Although the statute does not expressly preclude such agencies from sharing these records with third parties, it provides that "[t]he exchange of records and information authorized by subsection (a)(4) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies." Id. § 534(b). This office has previously construed the phrase "related agencies" to include only those agencies expressly authorized under § 534(a) to receive CHRI directly from the Department. See Memorandum to Files, from Mary C. Lawton, Deputy Assistant Attorney General, Office of Legal Counsel, Re: Railroad Police Access to FBI Criminal Identification Records at 5 (June 22, 1978) ("Lawton Memo").

As we read the statute, it does not on its face forbid the government agencies that are authorized to receive CHRI from sharing it with private contractors assisting them in the performance of their duties. However, § 534(b) provides an enforcement mechanism that enables the Attorney General to oversee the use of CHRI by recipients. This statutory provision, which vests authority in the Attorney General to cancel CHRI exchange arrangements, contemplates that she may invoke that authority in order to guard against the improper use or redissemination of the CHRI that the FBI provides. Accordingly, as further discussed below, the statute would permit the Attorney General to authorize the disclosure of CHRI to private contractors performing criminal justice functions for government agencies that are authorized to receive CHRI, but any such authorization would have to impose controls on the recipients and their contractors to preserve the Attorney General's statutory oversight authority.

Rather than expressly prohibiting categories of CHRI disclosures, § 534(a)(4) merely limits mandatory CHRI exchanges to those that are for the "official use" of the designated "authorized officials." The text of § 534 does not address whether a private contractor acting under the direction, or on behalf, of such "authorized officials" could be said to be engaged in, enabling, or facilitating the "official use" of the CHRI by those officials.

On the other hand, § 534(b) pointedly discourages the "dissemination" of covered records outside "the receiving departments or related agencies," by providing that such dissemination "subject[s]" the noncompliant agency or department to possible cancellation of its exchange privileges under the statute. 28 U.S.C. § 534(b). Moreover, it is clear that this provision was intended "to protect the privacy of rap-sheet subjects,"Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989), and should be applied in a manner consistent with this purpose.[(4)] Finally, as this office has previously observed, the only enforcement mechanism expressly authorized by § 534 is the Department's authority to cancel the direct recipient's authority to receive the information, and the statute should be construed to preserve this oversight

authority. See Memorandum for Joseph H. Davis, Assistant Director, Legal Counsel Division, Federal Bureau of Investigation, from William P. Barr, Assistant Attorney General, Office of Legal Counsel, Re: Proposal by Federally Chartered or Insured Financial Institutions to Disseminate FBI Criminal History Record Information to CARCO Group, Inc. at 6-7 (Sept. 1, 1989) ("CARCO Memo"); Lawton Memo at 5. To the extent those recipients are permitted to disclose CHRI to their contractors, however, the Department's sole recourse under current regulations would be to rely on "the relationship between the local agency and the third party" to prevent abuses. Lawton Memo at 5. Thus, at least in the absence of effective controls over possible redissemination by the contractors, the Department's ability to limit the use of CHRI by recipients might be impaired if recipients were permitted to pass CHRI on to those contractors.

None of these considerations, however, compel a construction of the statute that precludes authorized criminal justice agencies from sharing CHRI with non-governmental contractors performing law enforcement functions where the arrangements are subject to appropriate controls. First, in providing that the exchange of CHRI is "subject to cancellation" if disseminated beyond the receiving agency or related agencies, Congress has delegated considerable discretion to the Attorney General to determine whether cancellation is appropriate in a given context. The statute does not require the Department to "terminate exchange relationships with users authorized under section 534(a)(1) if those users disseminate FBI criminal history records to unauthorized third parties." CARCO Memo at 6 n.12. This discretion would seem to carry with it the authority to determine that a particular class of disclosures -- i.e., those made to contractors for law enforcement purposes and subject to appropriate controls -- is consistent with the statutory purpose of facilitating law enforcement and not inconsistent with its purpose of protecting relevant privacy interests.

In addition, a strong argument can be made that disclosures of the sort contemplated would not constitute "dissemination" of the information, within the ordinary meaning of that word. Indeed, the dictionary defines "dissemination" to mean "to spread or send out freely or widely as though sowing or strewing seed: make widespread." Webster's Third International Dictionary 656 (1986). Sharing information with contractors who are assisting in law enforcement and who are subject to carefully drawn controls would not appear to fall within this definition. Moreover, although the meaning of the phrase "dissemination" may well vary based on context,[(5)] it is clear that, at a minimum, the Attorney General could exercise her regulatory authority to define the term in a manner that would permit disclosures to contractors who are assisting law enforcement and who are subject to appropriate controls. See Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984). Such an interpretation would be consistent with both the language and purpose of the statute.

Although opinions issued by this office have at times taken a restrictive view of § 534, see, e.g., Lawton Memo, we have not interpreted the term

"dissemination" to encompass all disclosures of CHRI to non-governmental personnel.[6] Some of these opinions, however, have indicated that CHRI disclosures to non-governmental entities may be made only when the entity "is the only agency, public or private, performing a criminal justice function under public auspices." See Lawton Memo at n.5. In our view, these opinions overstate the statutory limitation on permissible disclosures made by authorized criminal justice agencies in this context. We believe that the proper interpretation is expressed in subsequent OLC opinions, which more aptly state that the receiving private entity must be one that "perform[s] quasi-governmental functions under strict governmental control." CARCO Memo at 4-5; Memorandum for Joseph H. Davis, Assistant Director, Legal Counsel, Federal Bureau of Investigation, from Douglas W. Kmiec, Deputy Assistant Attorney General, Office of Legal Counsel, Re: Creation of a Public Registry of Law Enforcement Officers Killed in the Line of Duty at 2 (July 1, 1988).

Finally, to the extent the Department must retain the ability adequately to control the use of CHRI, and to cancel the privileges of those who make or permit improper disclosures, we note that regulatory measures may be developed that would serve this purpose, while still allowing contractors to access relevant information.

Accordingly, we believe that disclosure of CHRI to authorized criminal justice contractors would not be forbidden by the provisions of § 534 itself. If carefully controlled, moreover, such disclosures would also be compatible with the statutory purpose of facilitating law enforcement while protecting the privacy interests affected.

II.

In addition to § 534 itself, however, it is necessary to consider the currently existing regulations that implement the statute. See 28 C.F.R. pt. 20 (1997) (governing "Criminal Justice Information Systems") ("Part 20" or "CJIS Regulations"). Subpart C of Part 20 applies to the CHRI systems maintained by the Department of Justice, other federal agencies, and by state and local criminal justice agencies insofar as they use the services of federal CHRI systems. See 28 C.F.R. § 20.30. The regulations provide that CHRI contained in systems maintained by the Department of Justice "will be made available":

> (1) To criminal justice agencies for criminal justice purposes; and
>
> (2) To Federal agencies authorized to receive it pursuant to Federal statute or Executive order.
>
> (3) Pursuant to Public Law 92-544 (86 Stat. 1115) for use in connection with licensing or local/state employment or for other

> uses only if such dissemination is authorized by Federal or state statutes and approved by the Attorney General of the United States
>
> . . . .
>
> (4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses.

Id. § 20.33(a). The regulations further provide, consistent with § 534(b), that an agency's right to receive CHRI "is subject to cancellation if dissemination is made outside the receiving departments or related agencies." Id. § 20.33(b).

Nothing in the Subpart C regulations authorizes the dissemination of CHRI to private entities acting on behalf of government criminal justice agencies. Closest is the authorization to disclose CHRI to "criminal justice agencies for criminal justice purposes," id. § 20.33(a)(1), but those agencies are expressly defined to include only "courts" and certain "government agencies [and] any subunit thereof," id. § 20.3(c). They do not include non-governmental agencies, even when under contract to perform criminal justice functions. Particularly when read in light of the regulatory purpose of protecting "individual privacy," id. § 20.1, it appears that section 20.33(a) was intended as an exhaustive list of the categories of authorized exchange for the covered records, and this office has previously construed the provision in this manner.[(7)] Thus, section 20.33(a) does not affirmatively authorize dissemination of CHRI to non-governmental entities under contract to assist federal, state or local law enforcement agencies.

A more difficult question is whether such disclosure of CHRI to private contractors, where subject to strict controls over the handling and use of the CHRI, would constitute a "dissemination" for purposes of the regulation. Although one might plausibly argue that it would not, see supra n.5 and accompanying text, for a number of reasons we believe that such disclosures should not be authorized without first amending the regulations. Although we cannot say with certainty that such an action is legally required, the risks of not doing so are substantial.

At the outset, we note that it is more difficult to construe the regulation's use of the word "dissemination" in a manner that would allow contractor access than the statute's use of the same word. In particular, Subpart B of the regulations, which sets forth the rules governing certain state and local (as opposed to federal) criminal history record information systems, expressly authorizes disclosure to "individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice. . . ." 28 C.F.R. § 20.21(b)(3). Because no similar provision appears in Subpart C, which governs here, one might reasonably infer that such disclosures are not currently permitted under that provision.

Further, as noted in your memorandum of October 3, 1997, earlier opinions of this office have taken a restrictive view of the Department's authority to release CHRI to recipients not specifically identified in § 534,[8] and the Department historically has not permitted third-party access to CHRI. The courts have indicated that when an agency changes its interpretation of a regulation so fundamentally that it is equivalent to an amendment of the regulation, the change must be accomplished through notice-and-comment rulemaking. See Shalala v. Guernsey Memorial Hosp., 514 U.S. 87 (1995); Paralyzed Veterans of America v. D.C. Arena L.P., 117 F.3d 579, 586 (D.C. Cir. 1997).

Finally, by proceeding by notice-and-comment rulemaking, the Department will insure that its interpretation of § 534 receives the full weight of Chevron deference. Although the question is unsettled, a court might well provide less deference to an "interpretative" rule, which is not subject to formal rulemaking, than to a "legislative" rule, which is subject to the notice-and-comment process.[9] Compare Martin v. Occupational Safety & Health Review Comm'n, 499 U.S. 144, 157 (1991) (interpretative rules "not entitled to the same deference as norms that derive from the exercise of the Secretary's delegated lawmaking powers")(dicta) with Elizabeth Blackwell Health Center for Women v. Knoll, 61 F.3d 170, 182 (3d Cir. 1995) (Chevron deference is appropriate "even though the Secretary's interpretation is not contained in a 'legislative rule'"). Receiving full Chevron deference, moreover, may prove important to sustaining the Department's position in potential litigation.

In light of all these considerations, we believe that to proceed without first amending the regulations in accordance with the APA would invite significant legal challenge.

III.

If a decision is made to amend the regulations to authorize provision of CHRI to criminal justice contractors, it is essential that this goal be achieved in a manner that will subject contractor access to effective controls against unauthorized use or further dissmenination. As the Supreme Court has observed, Congress intended that § 534 be applied in a manner that is protective of "the privacy of rap-sheet subjects." Reporters Comm. for Freedom of the Press, 489 U.S. at 749, 765. Moreover, § 534(b) provides for Department of Justice oversight of the dissemination of CHRI, by giving the Attorney General the authority to cancel the exchange of CHRI if an authorized dissemination is made. The Department's responsibility to protect the privacy of CHRI will require, in our view, that it have at its disposal the means of controlling the use of this information.

The precise form of such controls will depend upon a variety of factors. As a starting point, however, the Department might consider whether the provisions governing CHRI access agreements between states and criminal justice contractors set forth in Subpart B of the regulations would provide an appropriate

model. The Subpart B regulations require that such agreements shall "limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violations thereof." 28 C.F.R. § 20.21(b)(3). We would, of course, be happy to consider whether any particular proposal satisfies statutory requirements.

Finally, we note that authorizing the provision of federal criminal history records to the entities in question would require compliance with the Privacy Act. See 5 U.S.C. § 552a. The criminal history records maintained by the FBI and provided through the NCIC are part of a system of records that is subject to the Privacy Act. Accordingly, covered agencies may not disclose such records to other agencies or institutions unless the subject of the records consents or one of the statute's exemptions apply. Id. § 552a(b).[(10)]

Here, the criminal justice or law enforcement uses for which the information would be provided would likely qualify for the issuance of a "routine use" exception to the Privacy Act's prohibitions against unconsented disclosures. See 5 U.S.C. § 552a(b)(3). A "routine use" means, with respect to the disclosure of a record, "the use of such record for a purpose which is compatible with the purpose for which it was collected." Id. § 552a(a)(7). We think that the uses of CHRI indicated in the examples you have submitted would generally be compatible with the law enforcement and related purposes for which it was collected by the FBI and other agencies. We have not undertaken, however, to determine whether these particular uses would qualify under any of the existing published routine uses applicable to the relevant systems of records. See, e.g., Privacy Act of 1974; Modified Systems of Records Notice (Fingerprint Identification Records System), 61 Fed. Reg. 6385 (1996); Privacy Act of 1974; Modified System of Records Notice (NCIC), 60 Fed. Reg. 19,774 (1995). Before actually authorizing the disclosure of CHRI to private criminal justice contractors, the Justice Department should issue any new routine use notifications necessary to cover the particular disclosures in question.

RANDOLPH D. MOSS
Deputy Assistant Attorney General
Office of Legal Counsel

---

1. Memorandum for Acting Assistant Attorney General, Office of Legal Counsel, from Robert M. Bryant, Deputy Director, FBI,Re: Access to and Dissemination of Information from the Department of Justice (DOJ) Criminal History Record Information (CHRI) System (Oct. 3, 1997) ("FBI Memo").

2. The Attorney General has delegated her CHRI exchange responsibilities to the Federal Bureau of Investigation ("FBI"). See 28 C.F.R. §§ 0.85(b) and 20.31(b).

3. The reference to "other institutions" does not generally provide for disclosure to non-governmental entities. See Memorandum for John Mintz, Legal Counsel, Federal Bureau of Investigation, from Robert Shanks, Deputy Assistant Attorney General, Office of Legal Counsel, Re: Proposed Access to NCIC Files by National Center for Missing and Exploited Children at 2 (July 31, 1984) ("NCMEC Memo"). Rather, only certain "railroad police departments" and "police departments of private colleges or universities" are identified as entities "include[d]" within the meaning of that term. 28 U.S.C. § 534(d).

4. Although at one time this privacy interest was thought to raise potentially significant constitutional limitations on the use of CHRI, thus requiring a narrow construction of the statute, see Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), rev'd sub nom. Menard v. Saxbe, 498 F.2d 1017 (D.D.C. 1974) and Lawton Memo at 4-5, subsequent developments in the law have made clear that the limitation is not constitutionally derived. See United States Secret Service Use of National Crime Information Center, 6 Op. O.L.C. 313, 322 (1982). As a result, it is not necessary to construe the statute narrowly in order to avoid a significant constitutional problem. Cf. Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575 (1988); NLRB v. Catholic Bishop of Chicago, 440 U.S. 490, 500 (1979).

5. Compare Zimmerman v. Owens, 561 N.W.2d 475 (Mich. Ct. App. 1997) (holding that placement of a confidential child protective service report in public court file did not constitute a dissemination) with Essential Information, Inc. v. United States Information Agency, 134 F.3d 1165, 1168 (D.C. Cir. 1998) (rejecting argument that the term "dissemination" connoted a much broader dispersal of materials than mere "disclosure" under the particular statute in question, but acknowledging that "the terms may be so distinguishable under some circumstances").

6. See, e.g., NCMEC Memo at 3 (authorizing CHRI disclosure to private non-governmental entity, such as the National Center for Missing and Exploited Children, under limited circumstances and "subject to substantial governmental controls").

7. See Federal Bureau of Investigations -- Disclosure of Criminal Record -- Admission to the Bar, 3 Op. O.L.C. 55 (1979); see also Utz v. Cullinane, 520 F.2d 467, 477 n.20 (D.C. Cir. 1975) ("regulations set apparently stringent standards as to the maximum extent of dissemination").

8. See FBI Memo at 4 n.3 (citing,e.g., Lawton Memo and CARCO Memo).

9. In our view, the availability of Chevron deference should turn on whether Congress intended for deference to apply, and not on whether a rule is "interpretative" or "legislative." We cannot say with any certainty, however, that a reviewing court would adopt this same view.

10. In defining covered "agencies," see 5 U.S.C. § 552a(a)(1), the Privacy Act adopts by cross-reference the Freedom of Information Act's definition of "agency," which "includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." 5 U.S.C. § 552(f)(1).