

63 OAG 197

CRIMINAL JUSTICE INFORMATION SYSTEMS

CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS)—
FEDERAL AND STATE REQUIREMENTS FOR DATA CENTERS SERVING CRIMINAL JUSTICE INFORMATION SYSTEMS.

January 10, 1978.

Honorable Robert J. Lally,
Secretary, Department of Public Safety and
Correctional Services.

In your recent letters you advised:

The Department of Budget and Fiscal Planning has made a proposal to the Department of Public Safety and Correctional Services to the effect that the Public Safety Data Center be consolidated with the Baltimore Computer Utility (operated by the State of Maryland). Since the Public Safety Data Center stores criminal history data and there exists both State laws and Federal laws and regulations pertaining to the storage of criminal history data, I seek your legal opinion regarding this proposal.

Thereupon you have requested our opinion and advice on the following questions:

1. Do the existing Federal and State laws and regulations permit the consolidation of the Public Safety Data Center, a Criminal Justice Agency, into a shared computer data center; namely, the Baltimore Computer Utility, which is not under the management and control of a Criminal Justice Agency?

We advise: Federal law does not prohibit a criminal justice agency from using a shared computer located in a data center operated by a non-criminal justice agency if the criminal justice agency has approval authority with respect to (a) access to system facilities (manual or automated); (b) storage of information; (c) destruction or modification of information; (d) assignment of responsibility for physical security of information; (e) protection of central repositories from natural or man-made disasters; and (f) personnel screening. State law

and effect."); Iowa Code Ann. § 204.201 ("Annually, within thirty days after the convening of each regular session of the general assembly, the board shall recommend to the General Assembly any deletions from, or revisions in the schedules of substances, enumerated in [the statute]."); 63 Okla. Stat. Ann. § 2-201(B) ("The Board of Pharmacy by rule may classify new products determined to have a potential for abuse as controlled dangerous substances after notice and hearing; provided that such rule shall be submitted to the next regular session of the legislature, and such rule shall remain in force and effect unless a concurrent resolution of disapproval is passed."); Tex. Rev. Stat. Ann., Art. 4476-15, § 2.09(a) ("The Commissioner may not add any substance to the schedules if the substance has been deleted from the schedules by the legislature but failed to pass when considered by a quorum of either house."); W. Va. Code § 60A-2-201(a) ("The state board of pharmacy shall * * * on the first day of each regular session, recommend to the legislature which substances should be added to or deleted from the schedules . . .").

* By definition, uniform state laws operate in areas in which exclusive federal preemption either is not constitutionally available or, if possible, is not seen as a practicable legislative remedy. Furthermore, neither uniformity nor "cooperative federalism" requires that the several states strip themselves altogether of their sovereign right to legislate in this area.

does not prohibit the use of a data center operated by a non-criminal justice agency so long as the criminal justice information system central repository is operated by the Maryland State Police under the administrative control of the Secretary of Public Safety and Correctional Services with the advice of the Criminal Justice Information Advisory Board.

2. If the answer to question number one is affirmative, please specify the privacy and security "minimum assurances" that would be imposed on the shared computer center and set forth the type of State agency that would be required to operate such a center.

We advise: The applicable federal regulations specify the privacy and security requirements for shared data centers. See, 20 CFR Part 20, *infra*. See also, in explanation thereof, *Privacy and Security Planning Instructions, Criminal Justice Information Systems* (LEAA Revised April 1976); *Privacy and Security of Criminal History Information, SUMMARY OF STATE PLANS* (U.S. Dept. of Justice, LEAA National Criminal Justice Information and Statistics Services) (undated); *National Crime Information Center, Computerized Criminal History Program, Background, Concept and Policy* (FBI, approved by the NCIC Advisory Policy Board, October 20, 1976). In our opinion, the consolidation proposed in the *Phase I Plan, infra*, is conceptually capable of meeting such requirements. Of course, whether the ultimate consolidation will meet such requirements will depend upon the specific manner in which the presently preliminary plan is implemented, and, as you know, the specific details thereof have yet to be developed.

3. What degree of "management control" must legally be retained by the Department of Public Safety and Correctional Services? With respect to this question, your views are solicited as to whether the General Assembly in enacting the CJIS Law (Article 27, Sections 742-755), intended the Secretary of the Department of Public Safety and Correctional Services to direct the operation and management of criminal information data to the exclusion of any other agency of the State. Would the CJIS legislation indicate an

intent on the part of the General Assembly to mandate management and control of criminal justice information by the Department of Public Safety and Correctional Services; while Article 15A, Section 23B would mandate control by the Secretary of the Department of Budget and Fiscal Planning of data processing other than that in the field of criminal justice?

We advise: Insofar as federal law is concerned, the "degree" of management control required is that necessary to insure compliance with the security and privacy regulations of the Department of Justice. See, 20 CFR Part 20, *infra*. Insofar as Maryland's CJIS statute (Article 27, Sections 742 *et seq.*) is concerned, while it clearly intends that the Secretary of Public Safety and Correctional Services direct the operation and management of Maryland's criminal justice information system, it also clearly subjects the automatic data processing portion thereof to the central data processing authority of the Secretary of Budget and Fiscal Planning. Consequently, as a matter of State law, these responsibilities are compatible.

4. In the event you conclude that the consolidation referred to in question one is appropriate, is the Director of the Baltimore Computer Utility the "custodian" of criminal records and thus the official charged with the responsibility of granting or denying the right of inspection to the material identified in Article 76A, Section 3(b)(i-v), which would be contained in the computer "on the ground that disclosure to the applicant would be contrary to the public interest"?

In our opinion, if the proposed consolidation takes place, the Secretary of Public Safety and Correctional Services would continue, for the purposes of the Public Information Act, to be the "official custodian" of the criminal history records stored in the shared system and the Maryland State Police would continue to be the "custodians" of such records.

5. If there should be any conflict between the Federal Rules and Regulations promulgated on March 19, 1976 and August 18, 1976 and the Maryland Security and Privacy Plan, the Privacy

and Security Planning Instructions, the NCIC Computerized Criminal History Program, Background, Concept and Policy dated October 20, 1976, which prevails—the Federal Rules and Regulations that have been promulgated, or the supporting documents enumerated above?

We advise: While the question of the relative "supremacy" of the U.S. Department of Justice Regulations, the Maryland Security and Privacy Plan, and various federal agency publications is more properly the province of the Department of Justice, we think it clear that the Regulations prevail to the extent of conflict or inconsistency. Indeed, to the extent of such conflict or inconsistency, any purported "requirement" of any of the other documents is invalid.

6. As outlined in Secretary Schmidt's letter to me of September 26, 1977 he proposed 1) to consolidate the PSDC and BCU through the budgetary process (FY 79 Budget) and further to assign the BCU to the Office of the Comptroller of the Treasury. Therefore, your opinion is solicited as to whether both of these procedures can be accomplished through the budgetary process or would each of them require specific legislative action?

In our opinion, the consolidation of the data centers and the assignment of the resulting consolidated center to the Office of the Comptroller may be accomplished through the Budget, although either an Executive Order or legislation may present a preferable vehicle.

7. Inasmuch as the CJIS Law of Maryland (Article 27, Sections 742-755) provides for the storage of some criminal history data by the various courts of this State, what, if any, authority does the Secretary of Budget and Fiscal Planning and/or the Office of the Comptroller of the Treasury have in stating the means or manner that such criminal history data will be stored?

In our opinion, the Judicial Branch's storage of criminal history data in the CJIS central repository presents no legal impediment to the transfer of the central processing function

as proposed in the Phase I Plan. Under the Plan: (a) the Secretary of Budget and Fiscal Planning would continue to have the central data processing authority which he presently has with respect to all Executive Branch data processing, including the present, Public Safety Data Center; and (b) the Comptroller would acquire central processing responsibility which, insofar as the Court's portion of the CJIS central repository is concerned, would be subject to the superior authority of the Court of Appeals and its Chief Judge in much the same manner as the responsibility of the operator of the Public Safety Data Center presently is subject to that judicial administrative authority.

8. Who has the ultimate authority to promulgate and enforce rules and regulations related to the collection, reporting, and dissemination of criminal history records information stored in the computer?

In our opinion, under federal and State law the Court of Appeals and the Secretary of Public Safety and Correctional Services have the ultimate authority to promulgate and enforce rules and regulations relating to the collection, reporting and dissemination of criminal history records information, whether stored in an automated or manual system.

9. Who has the ultimate authority to promulgate and enforce rules and regulations relating to the security of criminal history records information? The word "security" as used is intended to embrace physical, personnel, and data penetration security. Personnel would, of course, include possible violations of security by Merit System employees.

In our opinion, under present federal and State law, the Court of Appeals and the Secretary of Public Safety and Correctional Services have the ultimate authority to promulgate and enforce rules and regulations relating to the security of criminal history records information, whether stored in an automated or a manual system.

Our opinion and advice is founded upon the following understanding of the Phase I Plan and analysis of applicable law.

THE PLAN AND ITS BACKGROUND

I.

We understand that the plan to consolidate the Public Safety Data Center with the Baltimore Computer Utility is rooted in former House Bill 459, which passed the General Assembly in its 1977 Session, but was vetoed by the Governor on May 26, 1977. According to the veto message, the Governor preferred a phased approach in which: (1) the special needs and circumstances of agencies such as the Department of Public Safety and Correctional Services could be addressed and considered; and (2) reasonable time limits could be established for such centralization as is found to be desirable. See, *Laws of Maryland* (1977) 3851-3854. On June 1, 1977, in separate letters to the Comptroller of the Treasury and the Secretary of Budget and Fiscal Planning regarding the veto of House Bill 459, the Governor referred to a suggestion that the objectives of the Bill could better be achieved on a phased-in basis and requested that the Secretary and the Comptroller develop methods for achieving that objective. See, *Phase I Report, infra*, at pp. A-3 and A-4 thereof.

Pursuant to this gubernatorial direction and with the oversight of the House Committee on Appropriations' Subcommittee of State Data Processing (the framers of H.B. 459),¹ the Office of the Comptroller and the Department of Budget and Fiscal Planning undertook to accomplish, on a phased-in basis, the objective of House Bill 459 with respect to the consolidation of the data centers.² On October 5, 1977, these offices issued a *Plan for Redirection of Data Processing, Phase I Report* (hereinafter *Phase I Report*).³

In pertinent part, the Phase I Report recommends the consolidation of the Public Safety Data Center (PSDC) into the workload of the Baltimore Computer Utility (BCU) and the transfer of the latter from the Department of Budget and Fiscal Planning to the Office of the Comptroller. As we understand it, the proposed consolidation will leave a communications controller, with various terminal connections,⁴ in place at the PSDC. All systems personnel, all programming personnel, all data entry personnel and certain managerial and clerical personnel will remain in the employ of the Department of Public Safety and Correctional Services and stationed at the Department. All other PSDC personnel will

be transferred to the BCU and all other PSDC computer equipment will either be transferred or declared to be "excess." A remote job entry terminal will be installed at the Public Safety site and will be connected to the communications controller, thus enabling the systems and programming employees of the Department of Public Safety and Correctional Services to continue developing, implementing and operating the criminal justice information system, *albeit via* the BCU computer. The BCU computer configurations will not change, except that a communications controller will be tied via telephone lines to the Public Safety controller and some disc storage files will be moved to the BCU.⁵

Thus, we are told, the technical results of the consolidation could be such that the Department of Public Safety and Correctional Services: (1) would authorize only a relatively few BCU personnel to access the criminal justice information system data base;⁶ (2) would have the authority to require the implementation of software security techniques⁷ and site security which could limit BCU personnel access to the criminal history data; and (3) would continue to *operate* the Criminal Justice Information System Central Repository.

The impact of the consolidation is said to include: (1) the elimination of one State data center, (2) the elimination of two medium scale computer systems; (3) a significant reduction in personnel, and (4) a substantial annual savings. *Phase I Report*, p. 7. Moreover, these cost benefits are said to be achievable without detriment to the security or privacy of the Criminal Justice Information System and without the Department of Public Safety and Correctional Services losing management control thereof.⁸

Finally, we understand that approximately one year is required to implement the consolidation and phase-out of the Public Safety Data Center once the implementation process is started. *Ibid*, p. 8. "It is anticipated that the majority of the recommendations will be implemented via the fiscal year 1979 budget process." *Ibid*, p. 2. "Other actions will be implemented through administrative processes." *Ibid*, p. 15.

II.

APPLICABLE FEDERAL LAW

At the outset, we recognize that the U.S. Department of

Justice certainly is the more appropriate agency for the rendering of advice regarding the application and effect of: (1) acts of Congress which it administers, (2) regulations promulgated by it, and (3) the policies of its constituent agencies. Nevertheless, in view of our constitutional and statutory responsibility as legal advisor to the State agencies and officials involved in this consolidation,⁹ it is proper for us to address your questions of federal law insofar as they impact the duties, responsibilities and authority of such agencies and officials.

There are only two areas of federal law which arguably impact the Phase I Plan, *viz.*, those provisions which authorize, implement and regulate the privacy and security aspects of criminal justice information systems funded by the Law Enforcement Assistance Administration (LEAA) of the U.S. Department of Justice, and those which regulate the Identification Division and the Computerized Criminal History Program of the National Crime Information Center (NCIC) of the Department's Federal Bureau of Investigation. Although ultimately implemented via somewhat differing policy expressions, the requirements for participation in these federal programs are set forth in comprehensive Department of Justice regulations. The language and history of these regulations leave no doubt about the permissibility of a shared computer system operated by a non-criminal justice agency.

On May 20, 1975, pursuant to the authority vested in the Attorney General of the United States¹⁰ and the Law Enforcement Assistance Administration,¹¹ and based on a notice of proposed rule making published at 39 FR 5636 (2/14/74), the Department of Justice issued regulations governing data contained in criminal history record information. 40 FR 221-14. Subpart A thereof applied to both the LEAA and the NCIC programs; Subpart B provided requirements for State and local criminal history information systems funded in whole or in part with funds made available by LEAA subsequent to July 1, 1973, pursuant to Title I of the Omnibus Crime Control and Safe Streets Act. Subpart C regulated, in pertinent part, State and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems, *i.e.*, the National Crime Information Center's Computerized Criminal History (CCH) File.

A. LEAA Requirements

In pertinent part, Subpart B provided for each State to submit to LEAA a Criminal History Record Information Plan which, *inter alia*, set forth operational procedures to:

Insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated, a criminal justice agency shall—

* * *

Assure that where computerized data processing is employed, the hardware . . . to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice;¹²

Have authority to set and enforce policy concerning computer operations;

Have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area where such information is stored, collected or disseminated;

Select and supervise all personnel authorized to have direct access to such information * * *.

40 FR 22115 [to have been codified as 28 CFR 20.21 (f)(2)-(5)].

As had been the case with their proposal,¹³ so too the adoption of these regulations caused a hue and a cry to be raised on behalf of the States.¹⁴ On behalf of Maryland in particular, the Governor wrote to the Attorney General of the United States asserting that dedication was unnecessary and requesting that the regulations be amended to permit the States to integrate data processing systems.¹⁵ Although the Attorney General initially disagreed,¹⁶ Section 20.21(f) was eventually reopened for comment and ultimately substantially revised.¹⁷ See, 41 FR 11718.¹⁸ According to the Law Enforcement Assistance Administration:

[t]he most significant revision was the deletion of the "dedicated hardware" requirement contained in Section 21.21(f)(2) of the May 20, 1975 regulations.

*The comments received during hearings supported the view that adequate system security could be maintained through use of software alternatives to dedicated hardware. Furthermore, it was noted that current state fiscal constraints frequently required the development of facilities on a share-system basis.*¹⁹

[Consequently, a]s amended, the Regulations direct states to adopt procedures, developed or approved by participating criminal justice agencies, in the following areas: access to system facilities (manual or automated); storage of information; destruction or modification of information; assignment of responsibility for physical security of information; protection of central repositories from natural or man-made disasters; and personnel screening. Additionally, the Regulations provide that automated systems shall utilize technologically-advanced software and hardware. Furthermore, knowledge of software programs is required to be strictly limited.

Privacy and Security of Criminal History Record Information, SUMMARY OF STATE PLANS, U.S. Department of Justice, I.E.A.A., National Criminal Justice Information and Statistics Service, (undated) p. 31 (*State Plan Summary*) (emphasis supplied).

Thus, it is [now] possible to satisfy the regulations with a system that is neither dedicated nor under the direct control of a criminal justice agency, provided the criminal justice agency users have the right and capability of assuring that operational policies and procedures are adequate to achieve an acceptable level of security.

Privacy and Security Planning Instructions, Criminal Justice Information Systems (Revised August 1976), U.S. Dept. of Justice, LEAA, National Criminal Justice Information and Statistics Service, p. 42 (*LEAA Instructions*) (emphasis supplied).²⁰

For example, the operational programs and procedures for computerized data processing required by Section 20.21(f)(3) may be developed and im-

plemented by a noncriminal justice EDP division [e.g., the Department of Budget and Fiscal Planning or the Office of the Comptroller] operating a shared computer system with a criminal justice component, provided the procedures are approved by the participating criminal justice agencies [e.g., the Department of Public Safety and Correctional Services] and they are afforded the right to monitor the operations of the system to assure that the procedures are being properly implemented.

Ibid., p. 41 (emphasis supplied).

According to LEAA, although several States have indicated that they would maintain a dedicated system, at least at the State central repository level, "[t]he bulk of the [State] plans indicated that the States would opt for a shared system." *State Plan Summary*, p. 32. Furthermore, "[i]n view of the specificity of Section 20.21(f) and the technical nature of the methods of compliance for automated systems, most states in their plan did not attempt to describe the exact methods to be used to comply with the specific requirements." *State Plan Summary*, p. 32. This certainly is true of Maryland's Plan. Indeed, the security portion of Maryland's Plan presently is broad enough to accommodate a change from a dedicated to a shared system. See, *Maryland Security and Privacy Plan*, Governor's Commission of Law Enforcement and the Administration of Justice (June 19, 1976) pp. 81-96 (appended hereto as Appendix Seven).

There were two other changes in the regulations with respect to security requirements. First,

[t]he original requirement that a criminal justice agency "have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area" (Section 20.21(f)(4); May 20, 1975 version) was clarified by identifying the criminal justice agency's right to (A) Screen and have the right to reject for employment, based on good cause, all personnel authorized to have direct access to criminal history record information; [and] (B) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such

information where such personnel violate the provisions of these regulations or other security regulations. (Section 20.21(f)(4)).

In this regard several states did identify this as a problem area, although not an insurmountable one. Reasons given dealt with state administrative and civil service practices and the autonomy of state data processing centers.²¹

Secondly, and significantly, under the revised regulations "each State shall insure that the . . . [security] requirements [set forth therein] are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State." 28 CFR Section 20.21(f) (emphasis supplied).

"This change was made in response to the requests of many concerned parties who wanted to ensure that the policies adopted reflected the views of the appropriate elected officials." *State Plan Summary*, pp. 32-33. LEAA has interpreted this regulation to require merely that the standards be adopted pursuant to such legislation or such regulations.²² Indeed, LEAA has approved a Maryland Plan under which "[r]equirements to insure the confidentiality and security of the State of Maryland's Criminal Justice Information System and all criminal history record information reported and collected in support of this system are to be developed by rule and regulation [only] of the Secretary of the Department of Public Safety and Correctional Services and the Court of Appeals and it's Chief Judge (State statute, Article 27, Section 746(b)(2))." *Maryland Security and Privacy Plan, supra*, p. 81. However, as we have learned to our detriment under other federal regulations, both LEAA and we are bound by the clear language of 28 CFR Section 20.21(f).²³ Consequently, security standards established by either State legislation or State regulations approved or issued by the Governor are necessary in order to support the security aspects of the presently dedicated computer system and, should the consolidation occur, those of the proposed shared computer system.

B. NCIC Requirements

The National Crime Information Center (NCIC) serves "as a national index and network for 50 state law enforcement

information systems." *NCIC Policy, infra*, p. 1. Its present statutory base is 28 U.S.C. 534(a), Pub. L. 89-544, Section 4(c), 80 Stat. 616 (9/6/66), which directs the Attorney General of the United States to: "(1) acquire, collect, classify and preserve identification, criminal identification, crime, and other records; and (2) exchange these records with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions."²⁴ The performance of this duty has been delegated to the Federal Bureau of Investigation (20 CFR Section 20.31), is now regulated by Department of Justice Regulations (28 CFR Part 20, *supra*) and is implemented under standards adopted by the Director, FBI, upon the recommendation of the National Crime Information Advisory Board (*NCIC Policy, infra*).

In 1971, the Computerized Criminal History (CCH) File was established as part of the operating NCIC. NATIONAL CRIME INFORMATION CENTER (NCIC), COMPUTERIZED CRIMINAL HISTORY, Program Background, Concept and Policy, As Approved by NCIC Advisory Policy Board (April 1, 1976) p. 1. (NCIC Policy). In order to acquire and retain access to the CCH File, each criminal justice agency must "execute a signed agreement with the Director, FBI, to abide by all present rules, policies and procedures hereinafter approved by the NCIC Advisory Policy Board and adopted by the NCIC." 28 CFR, 20.36(a). As you know, such an agreement was executed on behalf of Maryland effective November 29, 1971.

Like the Department of Justice regulations which fix its parameters,²⁵ this NCIC policy required that a State information system be "dedicated" to criminal justice purposes in order for the State to be eligible to participate in the CCH program. See, *NCIC Policy*, pp. 9-14. However, on October 21, 1976, in apparent response to the "shared computer" amendments to the Department of Justice regulations, the NCIC Advisory Policy Board approved a revised policy which, although continuing to endorse the position that criminal justice information systems should be limited to the function of serving the criminal justice community, expressly recognized that a dedicated system is not required for NCIC CCH participation. *NCIC Policy* (October 20, 1976). Thus, although NCIC requires that a State system meet certain

security and privacy requirements, including the vesting of "management control" of the criminal justice information system in the criminal justice agency, it's policy authorizes, but does not recommend, the use of a data center operated by a noncriminal justice agency.²⁶ However, in so doing, the revised NCIC Policy regrettably has been couched in language which does not track the DOJ regulations and which could be read to impose requirements which exceed those set by the regulations, *viz.*, for NCIC purposes:

All computers, electronic switches and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history information must be under the management control of criminal justice agencies. Similarly, satellite computers and manual terminals accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency. *Management control is defined as the authority to set and enforce (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operation of computers used to process criminal history record information insofar as the equipment is used to process, store, or transmit criminal history record information. Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the computerized criminal history program. Such management control guarantees the priority service needed by the criminal justice community. A criminal justice agency must have a written agreement with the noncriminal justice agency operating the data center assuring that the criminal justice agency has management control as defined above.*

Ibid., p. 12 (emphasis in original).

C. Conflict Between Regulations and Policy

This leads us to your final federal law question and the reasons which compel us to advise: (1) the revised NCIC Policy probably is not intended to require more than the DOJ regulations require for LEAA purposes; and (2) even if so

intended, the Policy may not validly exceed the requirements of the regulations.

As a general rule, a properly adopted substantive rule or regulation establishes a standard of conduct which has the force of law, and a general statement of policy does not. *Pacific Gas & Electric Co. v. FPC*, 506 F. 2d 33, 38 (D.C. Cir., 1974). Consequently, "a general statement of policy is entitled to less deference than a decision expressed as a rule or adjudicative order." *Ibid.*, 39-40. See, generally, Davis, *Administrative Law of the Seventies* Section 5.01 (1976). With respect to the particular documents under consideration, the *Maryland Privacy & Security Plan* is a creature of the DOJ regulations, *i.e.*, 28 CFR Section 20.21; the *LEAA Instructions* are merely explanations of the DOJ regulations;²⁷ and the *NCIC Policy* is expressly subject to the DOJ regulations, 28 CFR 20.35 (h). Thus, the language and the "legislative history" of the regulations conclusively demonstrate that they are intended to set the limits of valid federal regulatory requirements for State criminal justice information systems participating in both the LEAA and NCIC programs. Consequently, to the extent of any conflict or inconsistency therewith, the regulations prevail over the "supporting documents" which you have enumerated in your request, *i.e.*, the *Maryland Security & Privacy Plan*, the *LEAA Instructions* and the *NCIC Policy*.

D. Federal Law Summary

In summary, we read the controlling federal law to expressly authorize the use of a shared computer operated by a non-criminal justice agency and to implicitly acknowledge that such an environment is not necessarily incompatible with that degree of management control which criminal justice agencies must maintain in order to insure the integrity, security and privacy of their sensitive and most important information systems. Whether the implementation of the Phase I Plan will ultimately exceed those bounds in any respect is a determination which, of course, must await the development of a specific plan of implementation. At this stage the Plan does not offend federal law in concept.

III.

APPLICABLE STATE LAW

Pursuant to your request, we have considered the proposed

consolidation in the light of several provisions of Maryland law, *viz.*, Code, Article 15A, Section 23B (Budget & Fiscal Planning—Data Processing); Article 27, Sections 742-755 (Crimes & Punishments—Criminal Justice Information System); Article 64A (the Merit System Law); Article 76A, Section 3 (Public Information); and Article 88B, Section 7 (State Police—Communications Systems). We have also considered the provisions of Article II, Section 24, of the Maryland Constitution and those of Code, Article 41, Section 15C, both of which relate to the authority of the Governor to reorganize the Executive Branch.

A. Code, Article 15A, Section 23B

The data processing authority of the Secretary of Budget and Fiscal Planning is as follows:

The Secretary, after consultation with the State Comptroller, shall be responsible for planning and controlling data processing in the several departments and agencies of the State government. The Secretary shall continuously study the data processing function within the State in order to improve its efficiency and economy. All changes affected by any department or agency pertaining to data processing shall first be reviewed and approved by the Secretary for compatibility with existing procedures and equipment. The purchase, lease, or rental of mechanical or electronic data processing equipment for all State departments and agencies shall be reviewed and approved by the Secretary prior to the purchase, lease or rental.

On October 28, 1969, this legislation was supplemented by an Executive Order (later designated 01.01.1969.09) in which the Governor: (1) construed the statute to place primary responsibility for planning and control of the State automatic data processing (ADP) function in the Department of Budget and Fiscal Planning, in consultation with the State Comptroller; and (2) ordered, *inter alia*:

Acquisition of equipment by one agency will not preclude the use of that equipment by another agency. Where feasible, an agency will make machine time available on a regular recurring basis

to meet the requirements of the agency not having equipment. *Centralization of data processing services will be fully exploited where cost reductions without adverse effect can be achieved.*

All changes effected by any department or agency pertaining to data processing systems shall first be reviewed and approved by the Department of Budget and Fiscal Planning.

All Contracts of partnerships affecting State ADP resources will be accomplished by and through the Department of Budget and Fiscal Planning.

Centralized control of the planning and utilization of Statewide ADP resources will be accomplished by the State Central ADP Staff in conjunction with the State ADP Management Review Board.

See, Code, Volume 9A, p. 557, 558 (emphasis supplied).

This statute does not require that the Secretary of Budget and Fiscal Planning operate the Baltimore Computer Utility. Furthermore, although this Executive Order binds all Executive Branch agencies, it cannot restrain either the Governor or the General Assembly. Thus, it does not operate to require the approval of the State ADP Management Review Board for a reorganization ordered by the Governor or accomplished by an act of the General Assembly.

Consequently, we find nothing in Section 23B which would either prohibit or conflict with the Phase I Plan insofar as it contemplates the ultimate transfer of the BCU to the Office of the Comptroller. Quite to the contrary, insofar as it constitutes an attempt to improve the efficiency and economy of the State data processing function, the Plan is consistent with the letter of Section 23B.²⁸ Similarly, insofar as it constitutes the exploitation of centralized equipment and services for the achievement of cost reductions without adverse effects, the Plan is conceptually consistent with the requirements of E. O. 01.01.1969.09.

B. Code, Article 27, Sections 742-755 (Maryland's CJIS statute)

As you well know, the Criminal Justice Information System (CJIS) subtitle of Article 27 is relatively recent, comprehen-

sive legislation designed to facilitate the implementation of the federal requirements and which, together with Maryland's *M-CJIS Master Plan* and her *Privacy and Security Plan*, reportedly are "held by national interests and federal agencies as exemplary models for other States to follow." *Information Provided To The Subcommittee On State Data Processing*, Department of Public Safety and Correctional Services, (August 25, 1976) p. 2. Drafted by the Security and Privacy Subcommittee of the Governor's Commission on Law Enforcement and the Administration of Justice,²⁹ introduced, as House Bill 1106, by the Speaker of the House of Delegates at the request of the Administration, and enacted with staggered effective dates as Chapter 239 of the Acts of 1976, the express purpose of this legislation is:

to create and maintain an accurate and efficient criminal justice information system in Maryland consistent with applicable federal law and regulations, the need of criminal justice agencies in the State for accurate and current criminal history record information, and the right of individuals to be free from improper and unwarranted intrusions into their privacy.

Article 27, Section 742(a). In order to achieve this result, the General Assembly found it necessary:

- (1) To create a central repository for criminal record information;
- (2) To require the reporting of accurate, relevant, and current information to the central repository by all criminal justice agencies;
- (3) To ensure that criminal history record information is kept accurate and current; and
- (4) To prohibit the improper dissemination of such information.

Ibid, Section 742(b). Thus, the subtitle is designed to provide the statutory framework for a criminal justice information system comprised of the equipment, facilities, procedures, agreements, and personnel used in the collection, processing, preservation, and dissemination of criminal history record information by State and local criminal justice agencies throughout the State. *Ibid*, Section 743(g). The heart of the system is "a Central Repository for complete

criminal history information on all adults formally arrested and prosecuted by the criminal justice system throughout the State. . . ." *Maryland Security and Privacy Plan, supra*, p. 3. The statute requires that the Central Repository be established as of December 31, 1977, and that it be operated by the Maryland State Police,³⁰ under the administrative control of the Secretary of Public Safety and Correctional Services, with the advice of the State Criminal Justice Information Advisory Board.³¹ *Ibid*, Section 747(b).

The Central Repository would directly provide all manual services related to the collection, storage, and dissemination of criminal history record information to all criminal justice agencies in the State and would be serviced by a State data center for the provision of all automated services related to the collection, storage, and dissemination of criminal history record information to all criminal justice agencies in the State. [Presently this data center is the existing Public Safety Data Center under the Secretary for the Department of Public Safety and Correctional Services.

Maryland Security and Privacy Plan, p. 9. Every State and local criminal justice agency in Maryland is required to report criminal history record information to the Central Repository. *Ibid*, Section 747(c).

Inter alia, the statute requires the Secretary of Public Safety and Correctional Services and the Court of Appeals to develop agreements between the Central Repository and the participating agencies for the implementation of the Criminal Justice Information System. *Ibid*, Section 748(a).³² Moreover, the Secretary is directed to "adopt appropriate rules and regulations for agencies in the executive branch of government and for criminal justice agencies other than those that are part of the judicial branch of government to implement the provisions of this subtitle and to establish, operate, and maintain the criminal justice information system." Section 746(a).³³ Subject to the provisions of Article 15A, Section 23B, the rules and regulations adopted by the Secretary, the Court and the Chief Judge [are, in pertinent part, to] . . . include those:

- (1) Governing the collection, reporting, and dis-

semination of criminal history record information by the courts and all other criminal justice agencies;

(2) Necessary to insure the security of the criminal justice information system and all criminal history record information reported and collected from it;

(3) Governing the dissemination of criminal history record information in accordance with the provisions of this subtitle and the provisions of Sections 735 to 741; [34]

Against this comprehensive statutory framework, two questions arise: (1) Does the State CJIS statute require that the Maryland Criminal Justice Information System be served by a computer which is dedicated to that System? (2) Does the statute reveal a legislative intent to vest CJIS computer authority in your office to the exclusion of the Secretary of Budget and Fiscal Planning?

At first blush, the requirement that the Maryland State Police operate the CJIS Central Repository might appear to apply to the operation of all hardware and software serving the Criminal Justice Information System. See, Sections 747-(b) and 743(g).³⁵ However, in our opinion, a closer reading of both the statute as a whole and the Maryland Security & Privacy Plan which is founded thereon clearly reveals that the mandate of Section 747(b) is not that broad. For, under the CJIS statute the Central Repository is but a "part of an overall State-wide Criminal Justice Information System for the State of Maryland." *Maryland Security & Privacy Plan, supra*, II. The system consists of "the Central Repository, the data center supporting the Central Repository and the State-wide telecommunications network and associated terminals. . . ." *Ibid*, II D.2. Thus, the statute consistently uses the term "criminal justice information system" in contexts which are broader than the Central Repository. See, e.g., Section 745 regarding the broad advisory duties of the Board; and Section 746 regarding the rulemaking authority of the Secretary and the Court of Appeals. Accordingly, in our opinion the statute does not require that the Maryland State Police operate the entire system, merely the Central Repository portion thereof. Consequently, if, as we are informed, the Phase I Plan can be implemented without removing the operation of the Central Repository from the

Maryland State Police, the CJIS statute would not, in our opinion, prohibit the Repository from being supported by a data center operated by another agency.

Secondly, you have asked if the statute reveals an intention to vest CJIS authority in your office and the Board to the exclusion of the central data processing authority of the Secretary of Budget and Fiscal Planning. In our opinion, the language of Section 747(b) reveals the opposite, *viz.*, a legislative decision to subject the rule-making authority of the Secretary of Public Safety and Correctional Services to the data processing authority of the Secretary of Budget and Fiscal Planning. Moreover, the "legislative history" of this provision demonstrates that this decision was not accidental and suggests that it was founded, at least in part, upon a desire to avoid a State statutory requirement for a dedicated computer. Specifically, as introduced House Bill 1106 merely would have required the promulgation of CJIS rules which, in pertinent part, included those "necessary for the coordination of all data and information processing activities in a manner consistent with the provisions of Article 15A, Section 23B."³⁶ Moreover, under the first reader version of the bill, the Secretary of Budget and Fiscal Planning was to be an *ex officio* member of the CJIS Advisory Board and the Board was authorized to use the services of that Department in the performance of its functions.³⁷ However, as a result of amendments by the House Committee on Judiciary (which we understand to have been suggested by the Administration and which took place on the very heels of the "shared computer" amendments to the Department of Justice regulations), proposed Section 744(a)(6) and (b) was amended so as to eliminate the *ex officio* membership of the Secretary of Budget and Fiscal Planning from the Board; proposed Section 744(e) was amended so as to eliminate the Department of Budget and Fiscal Planning from among those agencies upon which the Board might call for service in the performance of its functions; and the relatively subordinating language of proposed Section 746(b)(3) was deleted in favor of the general qualification which now expressly subjects all CJIS rules to the central ADP authority of the Secretary of Budget and Fiscal Planning.³⁸ *Ibid*. See also, II *Maryland House Journal 1976*, pp. 2598-2599 (Amendments Nos. 1-6) (Legislative Day: March 24, 1976); and Appendix Five hereof.³⁹

sary thereto shall be paid by the State, except rental and/or purchase costs of terminal devices and the circuitry necessary thereto tied to the State Police computer System; all supplies and other charges connected therewith shall be paid by the law enforcement agency.

Sections 8 and 9 mandate the Maryland State Police to collect, analyze, and disseminate information relative to the occurrence of motor vehicle accidents within the State and the incidence of crime within the State. Section 10 provides for dissemination of such information to participating agencies. Section 11 mandates "at least monthly" publication of statistics concerning the occurrence and cause of all motor vehicle accidents within the State.⁴⁴ The statute does not mandate that the State Police Computer System to which it refers be served by a computer dedicated to the use of the State Police. Consequently, we perceive nothing in the Phase I Plan which would be inconsistent with or necessarily impair the performance of these duties.

E. Code, Article 64A (the Merit System Statute).

As we have indicated above, some states reportedly have expressed concerns regarding the ability, consistent with their civil service law, to permit a criminal justice agency to exercise the "security clearance" authority which is required by federal law over the computer center personnel of a non-criminal justice agency. We do not perceive such a problem under Maryland's merit system law.

At the outset, as a result of a possible discrepancy between the DOJ regulations and the Revised NCIC Policy, *supra*, the extent to which federal law requires the Secretary of Public Safety and Correctional Services to have "security clearance" authority over BCU employees is less than clear. On the one hand, the regulations merely require that the Secretary have the right to reject applicants for employment, based on good cause, and the right to initiate or cause to be initiated the transfer or removal of employees "authorized to have direct access to criminal history record information." *Ibid*, Section 20.21(5)(4)(i) & (ii).⁴⁵ As we understand it, relatively few BCU personnel would be "authorized to have direct access to criminal history record information." On the other hand, since the BCU computer will be interfaced directly with

the NCIC computer, the Revised NCIC Policy would require that it be under the "management control" of the Secretary, which control includes, *inter alia*, the authority to set and enforce "standards for the selection, supervision, and termination of [perhaps all BCU] personnel [even those not authorized to have direct access to criminal history record information]." Revised NCIC Policy, p. 12. While, as we have indicated earlier, the inhibition of 28 CFR Section 20.35(h) casts some doubt upon the validity of the NCIC Policy's apparent overbreadth; nevertheless, we assume its validity for the purposes of this discussion.

Under Maryland's Merit System statute, the Secretary of Personnel, with the approval of the Governor, has established and classified all positions in the classified service, "and shall from time to time, thereafter as may be necessary, establish additional classes and classify therein new positions created, and may combine, alter or abolish existing classes." Code, Article 64A, Section 16(2). "Each class shall embrace all positions similar in respect to the duties and responsibilities appertaining thereto and the qualifications required for the fulfillment thereof and shall be given a classification title indicative of the character and rank of the employment." *Id*, (emphasis supplied).

Pursuant to the rule-making authority vested in him under Article 64A, Section 11, the Secretary of Personnel has promulgated several rules for the purpose of implementing his classification responsibility. In pertinent part, these rules provide for an official register of existing classes and the allocation of positions to each class "on the basis of the duties, responsibilities and qualification requirements of the various positions." 6 COMAR 06.01.00.10 (emphasis supplied). Out of these requirements have evolved several documents. *Inter alia*, there is a "Specification Sheet" (MS 120A), sometimes referred to as a job description, which sets forth: (1) the classification title of the position, (2) the minimum qualifications, (3) the conditions of employment, and (4) examples of the work involved. There is also a position description form (MS 22), whereby the Secretary of Personnel, through the Department of Personnel's Division of Salary Administration and Position Classification, designates the duties and responsibilities of the position.

Although a position has been allocated to a class, it "may be changed from one class to another by action of the Secretary, provided, however, that no such change in allocation shall be final until the appointing authority and the employee concerned shall have had the opportunity to be heard if either so desires." 6 COMAR 06.01.00.10. Moreover,

[s]ubject to the approval of the Governor, the Secretary shall hereafter, as he may from time to time deem necessary, establish new classes and allocate thereto any newly created position, or any previously existing position, or any position added to the classified service by legislative act or otherwise, and may combine, divide, alter, or abolish existing classes; provided, however that before any such change shall be made which will result in the removal of any employee from the classified service, notice and an opportunity to be heard shall be given the appointing authority and the employee concerned. Each new class thus established shall be defined with respect to and shall embrace all positions in the classified service substantially similar as to duties, responsibilities, and qualification requirements and shall be given a title indicative of the character and importance of the employment.

Ibid, 06.01.00.11.

In establishing a new classification, the Secretary is authorized to set "Minimum Qualifications Required for Entrance" therein. *Ibid*, 06.01.00.20A. Indeed,

[t]he Secretary shall require such evidence as he may deem necessary that applicants possess such minimum qualifications, including education, experience, physical qualifications, and the possession of such license or other evidence of competency as may be required by Federal or State Law, for the practice of the profession, art, trade or employment involved; or any other qualifications permitted by law.

Id.

Finally, with respect to incumbent employees, the regulations provide:

A. The appointing authority may re-assign an employee from a position in a given class to another position in the same class in the same State department, provided, however, that, if change of residence of the employee is involved, change of assignment may be made only upon the recommendation of the appointing authority, approved by the Secretary. All changes of assignment, except those of a temporary nature, shall be reported to the Secretary.

B. Any changes from a position in one class to a position in another class, for which the same maximum rate of compensation is prescribed, may be granted by the Secretary upon request of the appointing authority and such action when granted, shall be considered a horizontal change. All other changes in classification shall be governed by the respective rules of demotion or promotion.

6 COMAR 06.01.00.39.

Accordingly, to the extent that State or federal law requires that the Secretary of Public Safety and Correctional Services have "security clearance" authority over BCU personnel, such requirements may be implemented via action by the Secretary of Personnel in the form of the creation of a new class of positions unique to the BCU (e.g., "Data Processing Operations Technician—BCU") and the establishment of *Minimum Qualifications Required for Entrance* therein which include "initial and continuing security clearance by the Secretary of Public Safety and Correctional Services." Thereupon, the Secretary of Personnel, upon the request of the Secretary of Budget and Fiscal Planning (or, if the BCU is transferred as proposed, upon the request of the State Comptroller) could grant, as a horizontal change, a change of personnel involved from their existing class (e.g., "Data Processing Operations Technician") to a new and specialized class for which the same maximum rate of compensation is prescribed (e.g., "Data Processing Operations Technician BCU").

Thus, regardless of the validity of the NCIC "security" requirements as a matter of federal law, we find the State's Merit System Law to be amenable thereto.

F. The Use of the Budget As The Vehicle For Achieving Phase I.

In our view, the reorganization which the Phase I Plan would achieve constitutes merely the transfer of a function (i.e., the central processing unit function) from one department to another and not the abolition or transfer of a program (i.e., the CJIS Central Repository Program or the State Police Communications Program). Consequently, if, as we believe, there is no statutory requirement that the Central Processing Unit be dedicated to the criminal justice information system or the State Police Communications System,⁴⁶ the Budget is an adequate vehicle for such a transfer, and there is ample precedent therefor.⁴⁷

Nevertheless, in order that the specific lines of authority and responsibility be clear, and there be no doubt about the validity thereof, it may be preferable that this reorganization be accomplished via either appropriate legislation or by means of an appropriate reorganization Executive Order.

G. State Law Summary

The CJIS statute is, of course the focal point of our inquiry for State law purposes. Our review thereof reveals nothing which would prohibit the implementation of the *Phase I Plan*. We also find nothing in that Plan which is inconsistent with or inhibited by: (1) the data processing authority and responsibilities of the Secretary of Budget and Fiscal Planning under Code, Article 15A, Section 23B; (2) the data communications responsibility of the Maryland State Police under Code, Article 88B, Section 7; (3) the public information responsibilities of your office and personnel under the Public Information Act; or (4) the Merit System Law. Finally, although the *Phase I Plan* may be implemented via the Budget alone, clarifying legislation or an Executive Order may be preferable.

IV.

GENERAL SUMMARY

In general, we are of the opinion that there is no federal or State law prohibiting the consolidation of the Public Safety Data Center into the Baltimore Computer Utility. We are also of the opinion that, in spite of such consolidation, both federal and State law require that the ultimate responsibility

for the collection, recording and dissemination of criminal history record information and the security thereof remain in the Secretary of Public Safety and Correctional Services.

In closing, we wish to emphasize that the foregoing opinion and advice constitute our views and judgment merely on the legal issues presented by the Plan and not on the relative wisdom thereof.

FRANCIS B. BURCH, *Attorney General*.

JUDSON P. GARRETT, JR., *Assistant Attorney General*,

Counsel to the General Assembly.

¹ *Ibid*, pp. 14 and A-11 thereof.

² A chronology of the steps to be taken was set forth in the Phase I Report's "Index of Appendix."

³ As you know, also at this point in time, the Department of Public Safety and Correctional Services was undertaking a study of the resources required for the Criminal Justice Information System and the Department of Budget and Fiscal Planning was initiating a study of the PSDC hardware requirements. See, the Phase I Report, Appendix F-1 (p. 099) and F-2 (p. 100). DBFP's plan culminated in the issuance of the "Hardware Requirements Evaluation for the Department of Public Safety and Correctional Services—Final Report." See, Phase I Report, Appendix H-1, (p. 117).

⁴ *I.e.*, the National Crime Information Center, the Motor Vehicle Administration, the Washington Area Law Enforcement System, the National Law Enforcement Telecommunication System and the State-wide law enforcement agencies.

⁵ See, A REPORT ON THE PROPOSED CONSOLIDATIONS OF THE COMPUTER OPERATIONS OF THE PUBLIC SAFETY DATA CENTER (PSDC) INTO THE BALTIMORE COMPUTER UTILITY (BCU) Dept. of Budget and Fiscal Planning, presented to the CJIS Advisory Board on November 16, 1977.

⁶ Although no BCU personnel would be authorized to disseminate CJIS information, we understand that it will be necessary for the BCU technical support personnel to be authorized to access the CJIS data in order to perform their function of protecting the integrity of all data stored in and processed by the BCU. We also understand that the limited number of BCU personnel who are authorized to enter the BCU computer room will have physical access to the CJIS disc files and tape library.

⁷ See, Criminal Justice Computer Hardware and Software Security Considerations, PROJECT SEARCH, Technical Memorandum No. 6, January, 1974.

⁸ Under the present operation of the Baltimore Computer Utility, "[each user] agency [such as the Dept. of Public Safety and Correctional Services] owns the data which it collects and is accountable for its use. Access to data is limited to individuals authorized by the owning agency. Physical access to computer installation is restricted and tightly controlled. Contemporary programming methods, such as terminal identifiers, pass words and log tapes are used to protect data against unwarranted modification or disclosure. Backup data files are maintained in off-site locations." *Ibid*, pp. 13.

⁹ See, Md. Const., Art. V, Sec. 3(4); Code, Art. 32A, §2; Art. 41, §§71(d) and 204B(d).

¹⁰ 28 U.S.C. 509, 510, 534, and Pub. L. 92-544, 86 Stat. 1115, and 5 U.S.C. 301.

¹¹ Sections 501 and 524 of the Omnibus Crime Control and Safe Streets Act of 1973, Publ. L. 93083, 87 Stat. 197 (42 U.S.C. §3701 et seq.) (August 6, 1973).

¹² In this regard, the Commentary appended to the regulation specifically noted, "[i]n the short run, dedication will probably mean greater costs for the State and local governments. How great such costs might be is dependent upon the rapidly advancing state of computer technology. So that there will be no serious hardship on States and localities as a result of this requirement, §20.23 provides that additional time will be allowed to implement the dedication requirement. For example, where local systems now in place contain criminal history information of only that State, used purely for intrastate purposes, in a shared environment, consideration will be given to granting extensions of time under this provision." 40 FR 22118.

¹³ *E.g.*, see 3/22/74 letter from Verne H. Tanner, Jr., President, National Association for State Information Services, "a cooperating agency of the Council of State Governments," to Thomas Madden, General Counsel, LEAA (appended hereto as Appendix One).

¹⁴ Numerous Governors wrote to the Department of Justice. See, "Dedicated Computer" file, National Governor's Association (formerly National Governor's Conference).

¹⁵ See, letter from Governor Mandel to Attorney General Levi, dated 6/16/75 (appended hereto as Appendix Two).

¹⁶ See, 7/11/75 letter from LEAA Administrator Velde to Governor Mandel (appended hereto as Appendix Three).

¹⁷ See, letter of 10/28/75 from Governor Ray of Iowa, as Chairman of the National Governor's Conference, advising his colleagues of successful meetings with Justice Department officials (appended hereto as Appendix Four).

¹⁸ The full text of the regulations, both as originally promulgated and as amended, is set forth in Appendix Five hereof.

¹⁹ See also, the commentary appended to the regulations which expressly acknowledged that automated systems may operate in shared environments and that the regulations provide certain minimum requirements. 41 FR at 11718 (3/19/76) and 34951 (8/18/76).

²⁰ The Security portion of these Instructions is set forth in toto in Appendix Six hereof.

²¹ For reasons which we will discuss below in connection with our analysis of applicable State Law, we believe such requirements are compatible with Maryland's Merit System law and we note that, according to the Maryland Security and Privacy Plan, the Department of Personnel shares this view. See, Appendix Seven hereof, p. A-34 (original p. 95).

²² "A . . . change in the Regulations . . . that was . . . significant was the inclusion of the requirement that the security standards adopted be *pari-passant* to State legislation or in the absence of such legislation, by regulations approved or issued by the Governor of the State." State Plan Summary, p. 32.

²³ "The principle which accords substantial weight to an agency's interpretation of its own regulation is inapplicable insofar as that interpretation is inconsistent with the requirements (in this case, mandatory re-

quirements) of its own regulation validly promulgated under authority delegated to it by the Congress." *Francis v. Davidson*, 340 F.Supp. 351, 368 (D. Md. 1972), *aff'd*, 409 U.S. 904 (1972).

²⁴ Under subsection (b), "[t]he exchange of records authorized by subsection (a)(2) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies." Under subsection (c), "[t]he Attorney General may appoint officials to perform the functions authorized by this section."

²⁵ "The Director, FBI, shall not adopt recommendations of the Board which would be in violation of these Regulations." 28 CFR Section 20.35(h).
²⁶ See, Appendix Eight hereof for a comparison of the changes made in this Policy in order to accommodate a shared system.

²⁷ Indeed, the Instructions expressly recognize, "[t]he materials contained herein do not have the force of law as [do] the regulations." Preface, p. 1.

²⁸ We take no position herein on the potential of this plan to improve the efficiency and economy of State data processing.

²⁹ Maryland Security and Privacy Plan, *supra*, at p. 3 hereof.

³⁰ Of course, under Code, Article 41, Section 204(c), the Secretary, in his discretion, may exercise or perform this function.

³¹ Effective July 1, 1976, this legislation established such a Board and, in addition to such advisory duties as may otherwise be delegated to it in accordance with law, mandated it to: "advise the Secretary and the Court of Appeals and its Chief Judge on matters pertaining to the development, operation, and maintenance of the criminal justice information system, and shall monitor the operation of the system[.] . . . propose and recommend to the Secretary, and, in conjunction with the Standing Committee on Rules of the Court of Appeals, to the Court and its Chief Judge, rules and regulations necessary to the development, operation, and maintenance of the criminal justice information system[.] . . . [r]ecommend procedures and methods for the use of criminal history record information for the purpose of research, evaluation, and statistical analysis of criminal activity; [r]ecommend any legislation necessary for the implementation, operation, and maintenance of the criminal justice information system; and [r]eport annually to the Governor and the General Assembly on the development and operation of the criminal justice information system. Section 745.

³² Subsection (b) authorizes the development of procedures for sharing criminal history record information with criminal justice agencies of other states, the United States and foreign countries.

³³ "The Court of Appeals and its Chief Judge, acting pursuant to §§ 18 and 18A of Article IV of the Constitution of Maryland, shall adopt appropriate rules and regulations for the same purposes for the judicial branch of government." Section 746(a).

³⁴ On December 22, 1976, rules were promulgated which established the criminal justice information system central repository under the name "Criminal Records Central Repository (CRCR)" in the Maryland State Police and directed it to perform "all functions heretofore assigned to the State Central Crime Records Bureau; and other tasks delegated to it by the Secretary to ensure the accuracy, completeness, and security of criminal history record information in Maryland." See, 3 Md. R. 1549, XVI COMAR 12.06.08.03. On December 2, 1977, notice of proposed further regulations was published. In pertinent part, the proposed regulations would set forth

the responsibilities of the Criminal Records Central Repository and provide rules relating to the security of criminal history record information. See, 4 Md.R. 1919.

³⁵ Section 747(b) requires that the Maryland State Police operate the criminal justice information system central repository and § 743(g) defines "criminal justice information system" to mean "the equipment (including hardware and software), facilities, procedures, agreements, and personnel used in the collection, processing, preservation, and dissemination of criminal history record information."

³⁶ Laws of Maryland (1976), Chapter 239, Sec. 1, proposed Art. 27, § 746(b) (3) (emphasis supplied).

³⁷ *Ibid*, proposed § 744(a)(6), (b) and (e).

³⁸ Although the language of § 747(b) appears to subject the rule-making authority of the Court of Appeals, as well as that of your office, to the provisions of Article 15A, § 23B, we have previously concluded that § 23B applies only to the Executive Branch of State government, 61 Op. Atty. Gen. 241 (Sept. 8, 1976). Accordingly, in our opinion, the qualification contained in § 747(b) does not apply to the rule-making authority of the courts, viz., the rule-making authority of the Court of Appeals and its Chief Judge is not subject to the central data processing authority of the Secretary of Budget and Fiscal Planning.

³⁹ Letter from Chief, MISD, Dept. of Budget and Fiscal Planning, to Chief Legislative Officer, Executive Department, regarding the desirability of such an amendment in order to avoid a State statutory requirement for dedication of computer hardware (dated 2/6/76 and appended hereto as Appendix Nine). Although we recognize the less than compelling weight which the courts might give to such an informal document, nevertheless, "where the mind labours to discover the design of the legislature, it seizes everything from which aid can be derived." *Mr. Chief Justice Marshall (for the Court) in United States v. Fisher*, 6 U.S. (2 Cranch) 358, 386 (1804).

⁴⁰ "The Governor may make changes in the organization of the Executive Branch of the State Government, including the establishment or abolition of departments, offices, agencies, and instrumentalities, and the reallocation or reassignment of functions, powers, and duties among the departments, offices, agencies, and instrumentalities of the Executive Branch. Where these changes are inconsistent with existing law, or create new governmental programs they shall be set forth in executive orders in statutory form which shall be submitted to the General Assembly within the first ten days of a regular session. An executive order that has been submitted shall become effective and have the force of law on the date designated in the Order unless specifically disapproved, within fifty days after submission, by a resolution of disapproval concurred in by a majority vote of all members of either House of the General Assembly. No executive order reorganizing the Executive Branch shall abolish any office established by this Constitution or shall change the powers and duties delegated to particular officers or departments by this Constitution."

⁴¹ Under Section 1(d), "the term 'custodian' means and includes the official custodian or any authorized person having personal custody and control of the public records in question."

⁴² See, 42 U.S.C., § 3771(b), which requires LEAA to assure that the security and privacy of all criminal history record information collected, stored, or disseminated through support of LEAA is adequately provided

for and that such information is used only for law enforcement and criminal justice and other lawful purposes. See, 28 CFR, §§ 20.21(b) & 20.33, which implement 42 U.S.C., § 3771(b) by limiting the dissemination of criminal history record information to certain agencies and individuals for specified purposes only. See also, Md. Code, Art. 27, § 742, which recognizes "the right of individuals [who are the subjects of such records] to be free from improper and unwarranted intrusions into their privacy" and finds "a need . . . to prohibit the improper dissemination of such information", § 749, which envisions the dissemination of criminal history record information by criminal justice agencies and the central repository only, and prohibits dissemination thereby except in accordance with applicable law and regulations; and § 751 *et seq.* regarding the right of an individual who is the subject of such a record to inspect it and to challenge its completeness, contents, accuracy or dissemination.

⁴³ Code, Article 41, §§ 204A and 204C.

⁴⁴ "The primary existing uses of Article 88B are to require law enforcement agencies to collect and compile crime occurrence data for submission to the State Police for the State-wide Uniform Crime Reporting System, for submission by law enforcement agencies to the State Central Crime Records Bureau of arrest, identification, and to the extent available, disposition information, and for the reporting on inmate location and status by the Division of Correction." Maryland Security and Privacy Plan, II.A.3.b.(3).

⁴⁵ "The State Department of Personnel [reportedly] has reviewed [what was published in the Federal Register as] Section 20.21(f)(4)(B) [and has been codified as §20.21(f)(4)(ii)] of the federal regulations and has concluded that existing State personnel rules and procedures appear consistent with the federal requirements. The Department of Personnel states that the requirements of Section 20.21(f)(4)(B) [may be] met by normal managerial disciplinary authority (disciplinary action may, however, be contested pursuant to grievance procedures)." Maryland Security and Privacy Plan, II.D.2(b)(2).

⁴⁶ Again, as we understand the technical aspects thereof, the Phase I Plan notwithstanding, the Central Repository will continue to be operated by the Maryland State Police, under the administrative control of your office, with the advice of the CJIS Advisory Board.

⁴⁷ *E.g.*, via the 1978 budget alone, a data entry function was transferred from the Office of the Comptroller to the Department of Natural Resources. Vol. I, THE MARYLAND STATE BUDGET FOR THE YEAR ENDING JUNE 30, 1978, submitted to the General Assembly by the Governor in January, 1977, pp. I-188 (items 27-30) and I-514 (items 10-13). Similarly, via the budget alone, the entire Energy Policy Office was transferred from the Executive Department to the Department of Natural Resources; see, *ibid*, pp. I-79, I-120, I-510 to I-542. Indeed, while the transfer of an identical function from the Department of Human Resources to the Department of Budget and Fiscal Planning was originally effected by an Executive Order because it was being implemented during a fiscal year, E.O. 01.01.1974.15 (Consolidation of Data Processing, June 11, 1974), Code, Vol. 9A, pp. 558-559, that Order has since been rescinded, E.O. 01.01.1976.04 (August 4, 1976), Code, Vol. 9A, p. 559, and that function remains with the Department of Budget and Fiscal Planning by authority of the Budget alone.

Appendices not published in this volume.