

Department of the Interior Departmental Manual

Effective Date: 10/4/00

Series: Law Enforcement and Security

Part 446: Law Enforcement

Chapter 14: Computerized Criminal Information Systems

Originating Office: Office of Managing Risk and Public Safety

446 DM 14

14.1 Purpose. This chapter prescribes guidelines for the use and/or development of computerized law enforcement information systems. The objective is to increase the effectiveness of law enforcement through the efficient handling and exchange of criminal information.

14.2 Policy. The policy of the Department is to encourage the exchange of law enforcement information between Federal, State, and local agencies.

14.3 Scope. The use of computer-based crime information systems is restricted to authorized law enforcement bureaus/offices.

14.4 Responsibilities.

A. The Assistant Secretary - Policy, Management and Budget is responsible for developing Departmental guidelines and monitoring Department-wide use of the computerized law enforcement information systems.

B. Each bureau/office head shall administer a program that ensures strict adherence by all employees to the Computer Security Act of 1987 and Departmental Manual 375 DM 19.

C. Each bureau/office Law Enforcement Administrator shall ensure that all persons utilizing or having access to the computerized law enforcement information systems have successfully completed a suitability background investigation and received favorable adjudication.

D. Each law enforcement bureau/office will establish internal policies and procedures for accessing the information systems commensurate with their needs.

E. Users of accessing system terminals must ensure that necessary measures are implemented to secure the terminal and protect the information from unauthorized use.

14.5 Identification Coding. An originating agency identifier code (ORI) is permanently assigned by the Federal Bureau of Investigation (FBI) to a bureau/office authorizing access to

information in the National Crime Information Center (NCIC) and for entry into the National Law Enforcement Teletype System (NLETS). Most State, local, and Federal law enforcement organizations operate NCIC and NLETS, as well as other computerized systems. All law enforcement bureaus/offices assigned an ORI may use these informational systems in accordance with policies and procedures established by the agencies in control of the applicable systems. The Director, Office of Managing Risk and Public Safety (MRPS), shall be advised of all requests for assignment of ORI's and/or connections and additions to either NCIC, NLETS or any other law enforcement computerized systems.

14.6 Standards. Each law enforcement bureau/office utilizing NCIC, NLETS or any other authorized computerized information systems will adhere to the following minimum standards:

- A. The bureau/office originating a computerized record or message through an authorized information system is responsible for its accuracy, completeness, and correct status at all times.
- B. A bureau/office which has entered information in a computerized system is obligated to reply promptly to an inquiring agency regarding confirmation and other pertinent details of information so entered.
- C. A bureau/office must insure that teletype and computer terminals on line with various information networks are inaccessible to unauthorized persons.
- D. A bureau/office must insure that all persons utilizing or having access to the computerized law enforcement information systems have successfully completed a suitability background investigation and received favorable adjudication.
- E. Each bureau/office must insure that the information on file in authorized computer systems is accurate and up-to-date.
- F. All computer operators must read and understand the appropriate user guides to assure all input messages and inquiries are properly formatted.
- G. Off-site terminals will be accessed via the most secure telephone link available. The data stored in information systems such as NCIC, NLETS and other authorized computerized systems is confidential and may only be released in strict accordance with the provisions of the Privacy Act and other applicable laws. Should any information be verified that a bureau/office has received criminal history information and has disclosed that information to an unauthorized source, immediate action may be taken by the Department and NCIC to discontinue criminal history service to that bureau/office, through the control terminal, if appropriate, until the situation is corrected.
- H. Criminal history data on an individual from the NCIC computerized file will be made available to Federal agencies authorized under Executive Order or Federal statute and to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing or local or State employment, other than with a criminal

justice agency or for other uses unless such dissemination is pursuant to Federal or State statutes. Such State laws may not conflict with Federal Law. There are no exceptions.

I. Bureaus/offices are reminded that computerized information networks are investigative tools only and may occasionally contain erroneous information. Therefore, law enforcement action must be based on professional police judgment taking into account the totality of the circumstances. When possible, criminal information received from computerized networks should be confirmed prior to taking law enforcement action.

J. Bureaus/offices are advised that their rights to direct access encompass only requests reasonably connected with their criminal justice responsibilities.

14.7 Security. Each law enforcement bureau/office shall establish and disseminate procedures to ensure that:

A. All information resources are properly protected and that information technology resources are used only by authorized personnel.

B. All information resources of the Department shall be protected against loss, theft, natural disasters, such as fire or floods; improper use, unauthorized access or disclosure, alteration, manipulation, violation of confidentiality, physical abuse; or unlawful destruction, as applicable (375 DM 19.5(A)).

C. The bureau/office shall establish and administer a program which provides for an appropriate level of protection for the information resources under its control and that conforms to applicable legislation and Federal and Departmental guidance on information resources security (375 DM 19.5(B)).

D. All employees shall receive adequate training so that they may fulfill their security responsibilities (375 DM 19.5(D)).

E. All suspected, actual, or threatened security incidents are immediately reported to the proper authorities.

F. Failure to adhere to Federal and Departmental regulations pertaining to information resources security shall result in appropriate administrative, disciplinary or legal action being taken against the violator (375 DM 19.5(E)).

14.8 Implementation of System. The Director, MRPS, will be consulted prior to and advised of all requests for major program changes, additions or deletions to any of the computerized law enforcement information systems.

10/4/00 #3339

Replaces 9/21/93 #446-1