ARTICLE 5. COMMUNICATION SYSTEMS

Rule 1. Indiana Data and Communications System–Policy

240 IAC 5-1-1 General policy; restrictions on use

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 1. (a) A committee appointed by the superintendent of the Indiana state police, for the purpose of managing and controlling the Indiana data and communications system, hereinafter called "IDACS", has the responsibility for the management of the statewide system network as imposed by this article and as directed by the superintendent of state police. The committee chairman shall be selected by the superintendent. The chairman shall report activities of the committee to the superintendent for review and approval. To assure the proper operation of the system, the standards, procedures, formats, and criteria as set forth herein shall be strictly adhered to. In this respect, as in system security, the IDACS terminal agency shall not only follow the rules set forth, but shall also ensure that agencies they are servicing do the same.

(b) Accuracy is essential as is promptness in entering, modifying, locating, or clearing records in the system. Each record on file is identified with the agency originating that record, and that agency alone is responsible for the accuracy, completeness, and correct status of that record at all times. IDACS cannot assume responsibility for the accuracy of any records entered by any agency.

(c) The IDACS provides information for decision making, by investigators and patrolmen. The information furnished through IDACS shall be evaluated with other facts known to the officer and investigators at the scene. IDACS is an information tool. It is no substitute for professional police judgment.

(d) When an agency receives a positive response (wanted notice) from IDACS or NCIC, an immediate follow-up confirmation request with the agency that originated the record in the system is necessary before any enforcement action is taken. Likewise, the originating agency has an obligation to supply a substantive response within ten (10) minutes to the inquiring agency. This response shall include a confirmation or denial of the wanted notice or the length of time it will take to respond.

(e) IDACS is primarily a system for law enforcement/criminal justice users, and as such only data related to law enforcement/criminal justice shall be transacted by the system. Information furnished through the system shall be restricted to the use of authorized law enforcement/criminal justice agencies, or those authorized noncriminal justice agencies performing criminal justice responsibilities, and shall not be sold, transmitted, or disseminated to any noncriminal justice agency or person unless authorized by the state police superintendent. Such authorization for dissemination can occur when it has been determined that to do so would be in the best interest of the law enforcement/criminal justice community. *(State Police Department; Ch I, Prelim; filed Dec 20, 1978, 2:43 p.m.: 2 IR 136; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; errata, 6 IR 777; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2098; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

240 IAC 5-1-2 Audit of system transactions

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-5

Sec. 2. (a) Established IDACS committee policy requires all user agencies to maintain an audit trail for six (6) months for certain types of IDACS transactions as itemized but not limited to the following:

(1) Switched messages (both transmitted and received).

(2) Bureau of motor vehicles and department of natural resources information file data.

(3) IDACS/NCIC stolen file data.

(4) Out-of-state (NLETs) bureau of motor vehicles or department of natural resources data.

These audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. Audit trails shall be maintained manually or by automation, and shall be made available to the IDACS committee for inspection upon request.

(b) It should be noted that these are minimum requirements, and it may be necessary to keep important or case related traffic

for longer periods of time in order to properly confirm or validate IDACS/NCIC wanted entries. *(State Police Department; Ch I, Retention of IDACS; filed Dec 20, 1978, 2:43 p.m.: 2 IR 137; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2098; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

240 IAC 5-1-3 Audit of criminal history record dissemination

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6; IC 10-13-2-5

Sec. 3. 28 U.S.C. states that audits shall be kept pertaining to the dissemination of criminal history records. This includes responses from NCIC's Interstate Identification Index (NCIC III) and responses from state central repositories and other agency criminal history files (both in-state and out-of-state). Such audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. *(State Police Department; Ch I, Criminal History Record Dissemination and Retention; filed Dec 20, 1978, 2:43 p.m.: 2 IR 137; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2099; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

Rule 2. Indiana Data and Communications System – Security

240 IAC 5-2-1 "System" defined (Repealed)

Sec. 1. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-2 Who may access criminal history data (Repealed)

Sec. 2. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-3 Control of criminal justice records systems (Repealed)

Sec. 3. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-4 Use of system-derived criminal history data (Repealed)

Sec. 4. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-5 Right to challenge record (Repealed)

Sec. 5. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-6 Physical, technical and personnel security measures (Repealed)

Sec. 6. *(Repealed by State Police Department; filed Nov 5, 1982, 8:25 am: 5 IR 2495)*

240 IAC 5-2-7 Validation of records

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2

Sec. 7. (a) All IDACS user agencies shall validate, on a periodic basis, as prescribed to the user agency by IDACS, all IDACS wanted records entered on their authority. Validation of records shall be in conformity and compliance with rules set forth by IDACS.

(b) Validation obligates the originating agency to confirm the record is COMPLETE, ACCURATE, and is still OUTSTANDING or ACTIVE.

(c) Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. In the event the originating agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority shall make a determination based on the best information and knowledge available whether or not to retain the original entry on file.

(d) To ensure the validity of IDACS and NCIC records, administrative controls shall be maintained which will result in prompt updating for the benefit of system users. Agencies entering records in IDACS and/or NCIC are solely responsible for their accuracy, timeliness, and completeness. Only by conscientious validation of records can users remain assured the integrity of the system is being upheld, and inquiring officers can rely on the information in IDACS and NCIC.

(e) The Indiana control terminal (Indiana state police) is responsible to the national network (NCIC). Control terminal responsibilities are as follows:

(1) Monitor system use.

(2) Enforce discipline.

(3) Assure system procedures and policies are met by all users.

(f) Maintain validation schedule as established by NCIC/IDACS.

(g) Procedures for documentation are as follows:

(1) Each agency shall receive a validation printout in compliance with the validation schedule.

(2) It shall be the responsibility of the originating agency IDACS coordinator to cause each record to be processed according *[sic.]* subsection (c) and to ensure that any errors are corrected, inactive records are removed, and active records are kept in the system by submitting the appropriate validation transaction.

(h) Any record not appropriately validated within the authorized validation period shall be removed automatically from IDACS/NCIC.

(i) An agency that allows IDACS to purge inactive or unwanted records from the wanted files shall be subject to sanction. *(State Police Department; Ch I, Validation Policy; filed Dec 20, 1978, 2:43 p.m.: 2 IR 139; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2489; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2099; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

240 IAC 5-2-8 Terminal agency operation; coordinator; duties and responsibilities

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2-5

Sec. 8. Once operational on the IDACS system, each terminal agency is required to designate one (1) individual as coordinator to serve as liaison between that department and the IDACS committee. It is important that the person selected becomes familiar with all phases of IDACS to efficiently carry out all duties and responsibilities assigned. Duties and responsibilities are as follows:

(1) Ensure that all agency personnel (including any nonterminal agencies serviced) utilizing system information are aware of the rules and policies of the IDACS/NCIC/NLETS system.

(2) Disseminate the contents of the IDACS/NCIC newsletters to all terminal operators.

(3) Ensure that validation reports are properly processed.

(4) Ensure that terminal operators receive proper IDACS training in accordance with the IDACS certification training program.

(5) Maintain NCIC and IDACS manual revisions and disseminate information to operators.

(6) Advise IDACS of any changes in the agency head, the coordinator, agency address, or terminal site.

(7) Report all IDACS rule violations and other improper uses to IDACS.

(State Police Department; Ch I, Validation of Agency Operation–Internal; filed Dec 20, 1978, 2:43 p.m.: 2 IR 139; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2490; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2100; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)

240 IAC 5-2-9 User agreement

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 4-1-6-7; IC 10-13-2-6

Sec. 9. All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana state police and the IDACS committee. Nonterminal agencies shall complete an agreement with the terminal agency that services them. *(State Police Department; Ch I, Sample Agreement; filed Dec 20, 1978, 2:43 p.m.: 2 IR 140; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2490; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2100; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

240 IAC 5-2-10 Security; confidentiality

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2

Sec. 10. (a) "System", as used in the security and confidentiality rules, means IDACS, NLETS, and/or NCIC terminals, equipment, and any and all data accessible from or stored therein.

(b) Access, meaning the ability to obtain information from the system, shall be permitted only to criminal justice agencies in the discharge of their official mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Release of Indiana bureau of motor vehicles data to noncriminal justice agencies may occur when it is determined to be in the best interest of law enforcement/criminal justice to do so. Agencies that shall be permitted access to SYSTEM data include the following:

(1) Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.

(2) Prosecutive agencies and departments at all governmental levels.

(3) Courts at all governmental levels with a criminal or equivalent jurisdiction.

(4) Correction departments at all governmental levels, including corrective institutions and probation departments.

(5) Parole commissions and agencies at all governmental levels.

(6) Agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information.

(7) Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

(c) Approved noncriminal justice agencies may have access to SYSTEM data on a limited basis. "Limited basis" means restricted to only that data recommended through resolution by the IDACS committee and approved by the state police superintendent.

(d) All computers, electronic switches, and manual terminals (including mobile data terminals/printers) interfaced with the SYSTEM computer for the exchange of SYSTEM data shall be under the management control of criminal justice agencies. Similarly, satellite computers and manual terminals accessing the SYSTEM shall be under the management control of a criminal justice agency.

(e) "Management control" means the authority to set and enforce:

(1) priorities;

(2) standards for the selection, supervision, and termination of personnel; and

(3) policy governing the operations of computers, circuits, and telecommunications terminals used to process SYSTEM

information insofar as the equipment is used to process, store, or transmit SYSTEM 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 SYSTEM. Management control shall remain fully independent of noncriminal justice data systems, and criminal justice systems shall receive priority service and be primarily dedicated to the service of the criminal justice community.

(f) In those instances where criminal justice agencies are utilizing equipment and personnel of a noncriminal justice agency for SYSTEM purposes, they shall have complete management control of the hardware and the people who use and operate the system.

(g) The criminal justice agency shall exercise management control with regard to the operation of the equipment by:

(1) having a written agreement with the noncriminal justice agency operating the data center providing the criminal justice agency authority to select and supervise personnel;

(2) having the authority to set and enforce policy concerning computer operations; and

(3) having budgetary control with regard to personnel and equipment in the criminal justice agency.

(h) Procedures for the use of system-derived criminal history data shall be as follows:

(1) Criminal history data on an individual from the national computerized file shall be made available outside the federal government to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing (except when a federal, state, or local law/ordinance exists making the criminal justice agency responsible for the processing or issuing of the licenses/permits) applications, or local or state employment, other than with a criminal justice agency, or for other uses unless such dissemination is pursuant to state and federal statutes or state and federal executive order. There are no exceptions.

(2) Researchers using the data shall acknowledge a fundamental commitment to respect individual privacy interests by removing the identification of subjects as fully as possible from the data. Proposed programs shall be reviewed by the IDACS committee to assure their propriety and to determine that proper security is being provided. All noncriminal justice agency requests involving the identities of individuals in conjunction with their national criminal history records shall be approved by the NCIC advisory policy board through the IDACS committee. The NCIC or the IDACS committee shall retain rights to monitor any research project approved and to terminate same if violation of the above principles is detected. Research data shall be provided off line only.

(3) Upon verification that any agency has received criminal history information and has disclosed that information to an unauthorized source, immediate action shall be taken by the IDACS committee. Unauthorized use of criminal history information shall result in imposed sanctions as authorized by this article.

(4) Agencies are instructed that their rights to direct access to NCIC information encompass only requests reasonably connected with their criminal justice responsibilities.

(5) The IDACS committee shall make checks as necessary concerning inquiries made of the SYSTEM to detect possible misuse.

(i) The person's right to see and challenge the contents of his records shall form an integral part of the SYSTEM with reasonable administrative procedures. If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC III file, or the state central repository, it shall be available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Such requests shall be made by the person contacting the FBI or state central repository directly, and not through the SYSTEM.

(j) The following security measures are the minimum to be adopted by all agencies having access to the SYSTEM data and are designed to prevent unauthorized access to the SYSTEM data and/or unauthorized use of that data:

(1) Security measures for computer centers as follows:

(A) All computer sites accessing SYSTEM data shall have the security to protect against any unauthorized access to any of the stored data and/or the computer equipment including the following:

(i) All doors having access to the central processing unit (CPU) room shall be locked at all times.

(ii) A visitor's log shall be maintained of all persons entering the CPU area except those assigned to the area on a permanent basis. The visitor's name, date, time in, time out, agency represented, and reason for visit.

(B) Since personnel at these computer centers have access to data stored in the SYSTEM, they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative. This

screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigation, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as to the applicant's honesty, integrity, and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Also, convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the state police superintendent for a final approval or disapproval decision.

(C) All visitors to these computer centers shall be accompanied by a permanent full-time employee of the data center.

(D) Computers having access to the SYSTEM shall have the proper computer instructions written and other built-in controls to prevent SYSTEM data from being accessible to any terminals other than authorized terminals. These instructions and controls shall be made available to the IDACS committee for inspection upon request.

(E) Computers and/or terminals (including mobile data terminals) having access to SYSTEM data shall maintain an audit of all transactions. This audit trail shall be maintained either manually by each agency or automated by the computer center. This transaction audit shall be monitored and reviewed on a regular basis to detect any possible misuse of SYSTEM data. This audit shall be made available to IDACS for inspection upon request.

(2) Security measures for communications as follows:

(A) Lines/channels being used to transmit SYSTEM information shall be dedicated solely to SYSTEM use, i.e., there shall be no terminals belonging to agencies outside the criminal justice system sharing these lines/channels except by prior IDACS committee approval.

(B) Security of the lines/channels shall be established to protect against clandestine devices being utilized to intercept or inject SYSTEM traffic.

(C) Audio response terminals, radio devices, and mobile data terminals, whether digital (teleprinters) or voice, shall not be used for the transmission of criminal history data beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. Transmission shall be made to police officers upon his or her request.

(3) Security measures for terminal devices having access to the SYSTEM as follows:

(A) All agencies and computer centers having terminals on the SYSTEM and/or having access to SYSTEM data shall physically place these terminals in a secure location previously approved by the IDACS committee within the authorized agency. Subsequent physical location changes of terminals shall have prior approval of the IDACS committee.

(B) The agencies having terminals with access to SYSTEM data shall have terminal operators screened as in subdivision (1)(B) and restrict access to the terminal to a minimum number of authorized employees.

(C) Copies of SYSTEM data obtained from terminal devices shall be afforded security to prevent any unauthorized access to or use of that data. Copies of SYSTEM data which are no longer relevant shall be destroyed.

(D) Mobile teleprinters having access to SYSTEM data shall afford security to that data in the same manner as a fixed terminal. Any positive "wanted response" shall be duplicated at the agencies station terminal for proper interpretation and confirmation to occur. SYSTEM data shall not be transmitted to the device when it is unattended.

(State Police Department; 240 IAC 5-2-10; filed Nov 5, 1982, 8:25 a.m.: 5 IR 2492; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2102; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)

240 IAC 5-2-11 IDACS operator/coordinator certification training

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 11. (a) All IDACS terminal operators (including mobile terminals) shall be trained and tested for their proficiency at operating the IDACS terminal. All IDACS coordinators shall be trained and tested for their proficiency at operating the IDACS

terminal and for their skills as the coordinator.

(b) The objectives of training requirements shall be as follows:

(1) To ensure that terminal operators and coordinators are familiar with the laws governing IDACS/NCIC/NLETS, IDACS system rules, regulations, and procedures, and what files (functions) are available and how to utilize them properly.

(2) Create an awareness of IDACS/NCIC/NLETS system capabilities in order to allow criminal justice agencies to obtain maximum use of the system.

(c) All persons assigned a system password (operator identifier) to operate the IDACS terminal and persons designated IDACS coordinator by their agency shall be trained and tested according to the guidelines set forth by the IDACS committee and approved by the state police superintendent.

(d) Training course content shall be derived from the IDACS/NCIC/NLETS manuals and publications and be periodically reviewed for relevancy and accuracy and updated accordingly.

(e) The IDACS committee can authorize the removal of a system password or impose sanctions on an agency for noncompliance with these procedures. *(State Police Department; 240 IAC 5-2-11; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2105; errata filed Aug 10, 1990, 5:00 p.m.: 13 IR 2137; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

240 IAC 5-2-12 User agency sanctions

Authority: IC 10-11-2-10; IC 10-13-2-9; IC 10-13-2-10
Affected: IC 10-13-2-3; IC 10-13-2-4

Sec. 12. (a) The IDACS committee shall review violations of IDACS rules and make recommendations to the state police superintendent to impose sanctions on user agencies.

(b) The objectives of the sanction procedure shall be as follows:

(1) To ensure the integrity of the SYSTEM.

(2) Create an awareness among user agencies of the importance of following rules, regulations, and procedures in order to minimize the risk to liabilities that may be incurred by misuse of the SYSTEM and its data.

(c) Sanctions shall be based upon the class of violation, any previous violations, and any exposure to criminal and civil liabilities that the violation might place on the SYSTEM, its officials, and the offending agency.

(d) Violations shall be classed as either administrative (minor) or security (serious) violations. Security violations being defined as one which has or could result in access of SYSTEM data by unauthorized individuals. All other violations are classed as administrative.

(e) In determining the severity of the violation, the violation type, either administrative or security, and previous sanctions issued, if any, shall be considered. The IDACS committee may impose as sanctions one (1) of the following:

(1) Verbal warning.

(2) Written warning.

(3) Written notice of violation.

(4) Written notice of probation.

(5) Written notice of temporary suspension.

(6) Written notice of permanent suspension.

(f) Temporary or permanent suspension of service will not begin, unless an emergency exists, until fifteen (15) days after the agency head has received written notice by certified mail or personal service.

(g) An agency may after one (1) year apply to be reinstated if placed on permanent suspension. *(State Police Department; 240 IAC 5-2-12; filed Aug 6, 1990, 4:40 p.m.: 13 IR 2105; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA; readopted filed Dec 2, 2013, 10:29 a.m.: 20140101-IR-240130458RFA)*

Rule 3. Indiana Law Enforcement Emergency Network–Administration

240 IAC 5-3-1 Purpose of network; limitation on participation

Authority: IC 10-11-2-10
Affected: IC 10-11-2-10

Sec. 1. The Indiana Law Enforcement Emergency Network (ILEEN) is a system to establish a common communications bond between all Indiana law enforcement officers. It provides a secondary dedicated channel of emergency inter-department communication for each vehicle participating in the program. Participation is limited to law enforcement vehicles or portables operated by certified law enforcement officers.

ILEEN provides for coordinated assistance in emergencies and supports the concept of mutual interdependence.

Manpower shortages in Indiana law enforcement agencies point up the need of large and small agencies for assistance in coping with emergencies. ILEEN can bring such assistance rapidly when an officer advises others on the ILEEN frequency that he is in an emergency situation.

Hundreds of radio units are being installed or converted for operation on ILEEN by local, county, and state agencies. At this time, the Indiana State Police has base station transmitters and receivers on the frequency ready to begin operation. *(State Police Department; Ch I, Sec I, A; filed Dec 20, 1978, 2:43 pm: 2 IR 141; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA)*

240 IAC 5-3-2 Participation; request for authorization

Authority: IC 10-11-2-10
Affected: IC 10-11-2-10

Sec. 2. Participation is limited to those law enforcement agencies who file "Request For Authorization Forms" with the ILEEN Advisory Policy Committee, obtain State Police concurrence as demonstrated by a "Concurrence Form" properly completed, and who agree that the frequency will be used solely for the purpose intended. *(State Police Department; Ch I, Sec I, B; filed Dec 20, 1978, 2:43 pm: 2 IR 141; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA)*

240 IAC 5-3-3 Authorization of federal communications commission; advisory policy committee; duties; objective

Authority: IC 10-11-2-10
Affected: IC 10-11-2-10

Sec. 3. (1) Participating agencies must obtain Federal Communications Commission authorization by modification of their present FCC license or obtaining a new license for the frequency. Each agency can do this by submission of the proper forms to the Federal Communications Commission. The "Concurrence Form", properly completed, must accompany the forms submitted to the FCC. It is also necessary to include a cover letter attesting to the fact that operation will be under the State plan. This will eliminate the need and delay of frequency coordination.

(2) The ILEEN Advisory Policy Committee (APC) will consist of nine members appointed by the Superintendent of the Indiana State Police, serving at his discretion. The committee will be composed of representatives from local, county, and state law enforcement. A representative of the Superintendent will serve as Chairman of the APC.

(3) The APC will serve in an advisory capacity to the Superintendent of the Indiana State Police on all matters relating to the operation of ILEEN.

(4) The APC will meet quarterly with additional meetings to be called by the Chairman as he deems necessary. Meetings may be requested by a petition of at least half the members of the APC (5). Such meetings will be scheduled at the convenience of the Chairman.

(5) The Advisory Policy Committee shall monitor all facets of the operation of ILEEN and report its findings in all such matters to the Superintendent through the Committee Chairman.

(6) The objective of the Advisory Policy Committee will be to assist each participating agency and the Superintendent of the Indiana State Police in making ILEEN the efficient law enforcement tool it is intended to be. This may only be achieved through the input, cooperation, and assistance of each participating agency. *(State Police Department; Ch I, Sec I, C; filed Dec 20, 1978,*

2:43 pm: 2 IR 141; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA)

Rule 4. Indiana Law Enforcement Emergency Network–Operational Procedures

240 IAC 5-4-1 Operational procedures

Authority: IC 10-11-2-10
Affected: IC 10-11-2-10

Sec. 1. (A) General. The use of ILEEN will be confined to police related activity requiring emergency communication for police mobile units that individual agencies regular police radio facilities could not provide.

(B) Allowable Communications.

(1) Emergency

Those communications requiring coordination and cooperation of mobile units during riots, disasters, etc., or in effecting the apprehension of a person or persons suspected of being involved in a recently committed crime and who are leaving, or believed to be leaving, the jurisdiction of the police unit in pursuit. When such an emergency occurs and the operator of the mobile unit elects to use ILEEN, assistance shall be called for in the following manner.

(A) Initial Call

The message must contain enough information so that the listening units can determine whether they can or can not be of assistance.

EXAMPLE:

ILEEN, Vigo County 21 enroute South on U.S. 41 approaching Farmersburg in pursuit.

(B) Answer

A unit hearing the initial call and being in position to assist will answer.

EXAMPLE:

Vigo County 17 on U.S. 41 at Shelburn.

(C) After contact has been established, the remainder of the communications will be handled following proper police radio procedures excluding the use of any signal or code. When several units are involved in an activity, caution will be exercised so as not to overload the frequency. This will be implemented by transmitting only when the involved units have pertinent information or when they need information to properly participate.

(2) Service

Those communications which render a service to itinerant law enforcement vehicles while transporting prisoners or having other service needs. To provide this service, base stations have been installed at all State Police District Headquarters. When a service need occurs and the operator of the mobile elects to use ILEEN, service shall be called for in the following manner:

(A) Initial Call

The message must contain sufficient information so that a listening unit or station can determine who can best provide the required service.

EXAMPLE:

ILEEN SERVICE, Vigo County 5 on U.S. 40 just west of Manhattan, a property damage accident wrecker is needed.

(B) When in range and the service is such that it can be provided by a base station, the call should be directed to that specific State Police station.

EXAMPLE:

ILEEN State Police Terre Haute, Vigo County 17.

(C) After contact is established, the remainder of the communication will be handled following proper police radio procedures excluding the use of any signal or code.

(3) Broadcasts

The State Police District Headquarters will broadcast information pertaining to stolen vehicles, felony vehicles and felony acts, if the information is available within one hour of the time of the crime's commission and if information is sufficient for visual identification. No acknowledgement of these broadcasts is required or desired, and further traffic would not be called for unless

the need would develop according to an emergency situation. If a repeat or further information is needed, this must be obtained from the unit's own radio base station on that station's frequency.

(4) Testing

Ordinarily, adequate testing of the equipment will be accomplished by the technician on the service bench. Discrete operational testing will be allowed by calling the nearest State Police District Headquarters and requesting a report or by checking with another mobile unit.

EXAMPLES:

Car to Station:

ILEEN, State Police Terre Haute, Vigo County 6, signal report.

Car to Car:

ILEEN, Vigo County 16, Vigo County, signal report.

In either example, the called station or mobile will simply respond "Vigo County 6, good signal" or other appropriate short message to describe the signal.

(5) Summary

The efficiency and reliability of ILEEN will be directly under the control of each mobile unit participating in this program. Superfluous traffic will degrade the system and should be avoided by all participants. Likewise, all participants should monitor the system with the purpose of reminding violators that their superfluous transmissions are not desirable. The system will function only as well as the users wish.

(A) Bear in mind that all calls will be heard by monitors, as well as mobile units. No immediate response does not necessarily indicate that the transmission was not received; however, the transmission should be repeated. This will allow a monitoring station to alert a mobile unit that may be in the vicinity but not in service. Also, a request for service may be monitored and the necessary service dispatched by the monitoring agency.

(B) When all communications relative to the particular operation have been completed, the FCC call sign must be announced. This identifies the licensee as required by the FCC Rules and also will indicate the end of the transmission.

EXAMPLE:

State Police 32-16, KA 2181

Lafayette Police Department Car 9

KB3624

Hamilton County Sheriff Car 23

KA6439

(State Police Department; Ch I, Sec II; filed Dec 20, 1978, 2:43 pm: 2 IR 142; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA)

Rule 5. Indiana Law Enforcement Emergency Network–System Violation Reports

240 IAC 5-5-1 Reporting system violations; form

Authority: IC 10-11-2-10

Affected: IC 10-11-2-10

Sec. 1. (A) Reporting. One of the major objectives of the ILEEN Committee is to maintain a high level of performance on the ILEEN System. ILEEN is a system for all Indiana police agencies and each person involved should be interested in its integrity. So it behooves any agency or officer observing or overhearing an infraction to report the incident when it occurs in order to protect the integrity of the system and eliminate continued violations.

To assist in this area, an "ILEEN System Violation Report Form" was developed and is to be completed as follows:

1. Violation Date–Include month, day, and year.

Time–List time a.m. or p.m., and time zone.

2. Agencies Involved–List agencies involved by full name.

3. Car Identifiers

Involved–List actual car numbers of all units that were involved.

4. Violation Details–Be specific and list all pertinent details as to what transpired or was said, word for word if known. Use back of sheet if more space is needed.

5. Signature; Agency,

Date–The form is to be signed by the reporting individual along with the agency name and date.

Once completed, the form is to be mailed to the following address:

Superintendent, Indiana State Police
Attn ILEEN Advisory Committee
Indiana State Police
100 North Senate Avenue
Indianapolis, IN 46204

(B) Rules, standard operating rules for the ILEEN are defined in Section II of the ILEEN Manual. If read, understood, and followed, obviously the form would not be necessary.

ILEEN SYSTEM VIOLATION REPORT FORM

VIOLATION DATE _____

TIME _____

_____

_____

AGENCIES INVOLVED _____

_____

CAR IDENTIFIERS INVOLVED _____

_____

_____

_____

VIOLATION DETAILS (BE AS SPECIFIC AS POSSIBLE) _____

_____

_____

_____

_____

_____

_____

FILLED OUT BY _____

(signature)

_____

(agency name)

_____

(date)

REQUEST FOR OPERATING AUTHORIZATION

Date _____

The _____

(Agency Name)

wishes to participate in the Indiana Law Enforcement Emergency Network (ILEEN) and as a condition for such authorization to participate submits the following information:

1. Agency Headquarters Location

_____

(Street) (City) (Zip)
Telephone: (Area Code) _____ (Number) _____
2. Communications Center Location
_____
(Street) (City) (Zip)
Telephone: (Area Code) _____ (Number) _____
3. FCC Call Sign (Base) _____ (Mobile) _____
4. If you do not have FCC license in your name, give name of department under whose authority you operate and who furnished base station service to your mobile(s).
Department Name _____ FCC Call Sign _____
5. Advise the number and type (police, ambulance, portable, etc) of vehicles operating under your authority for which participation authority is requested.

TYPE	NUMBER

6. Projected increase in next 12 months of Item #5 _____ .
7. A base station monitor on ILEEN frequency (155.475 MHz) will be installed by _____ .
(Date)
8. Frequency and modulation checks required by FCC will be performed by:
Name _____
Address _____
Telephone _____
Signed _____

STATE OF INDIANA
INDIANA STATE POLICE
INDIANA STATE OFFICE BUILDING
100 NORTH SENATE AVENUE
INDIANAPOLIS, INDIANA 46204

TO WHOM IT MAY CONCERN:
The Superintendent of the Indiana State Police, the licensee of 155.475 Mhz, hereinafter referred to as the Indiana Law Enforcement Emergency Network frequency, hereby concurs to share the ILEEN frequency for mobile use only with the _____ Department for the purpose of coordinating police activities.
By accepting the concurrence, the _____ Department agrees to operate and maintain the ILEEN frequency in strict compliance with all applicable FCC Rules and Regulations and all present and future rules, policies and decisions made by the ILEEN governing body.

_____
Superintendent
Indiana State Police

By placing my signature below, I understand that the Superintendent of the Indiana State Police reserves the right to withdraw this concurrence with due cause.

_____
Agency Head

STATE OF INDIANA
INDIANA STATE POLICE
INDIANA STATE OFFICE BUILDING
100 NORTH SENATE AVENUE
INDIANAPOLIS, INDIANA 46204

May 7, 1977

TO: All ILEEN Participants
FROM: Superintendent
Indiana State Police
SUBJECT: ILEEN

Enclosed is the "Concurrence Form" for your agency. This should accompany your application to the FCC for license modification.

All agencies both within and outside the Chicago jurisdiction area should apply to the Washington, D.C. office.

Agencies inside the Chicago area that do not presently have a license should complete Form #425.

Licensees with valid license records in the Chicago Regional Data Base need only complete an abbreviated form. This consists of the following blanks:

Section I–1, 2, 3, 4, 5, 7, 8, 9, 10, and the certification at the bottom of the page.
Section II–1, 2, 3, 4, and 8
Section III–1, 3, 33, 35, 36, 38, and 39

Both licensees and those not presently having licenses that are outside the Chicago area are to completed Form #400.

The Federal Communications Commission has advised that frequency coordination is required for all new license applications and for present license holders outside the Chicago Region that are requesting modifications.

Each agency having received State Police concurrence and a valid FCC license for the frequency 155.475 MHz may begin operating for emergency purposes only at that time.

Agencies operating under another agencies license need only to confirm that the license holder is in possession of a valid license which has been modified to cover their units before beginning operation.

Superintendent
Indiana State Police

VNH: rw

STATE OF INDIANA
INDIANA STATE POLICE
INDIANA STATE OFFICE BUILDING
100 NORTH SENATE AVENUE
INDIANAPOLIS, INDIANA 46204

May 6, 1977

TO: All Indiana Law Enforcement Agencies
FROM: Superintendent
Indiana State Police
SUBJECT: Invitation to Participate in ILEEN

Your agency is invited to participate in the Indiana Law Enforcement Emergency Network (ILEEN). The purpose of this new law enforcement communications system is to provide car-to-car communications between all Indiana law enforcement agencies at all levels; municipal, county, state, and federal. This will be accomplished on a separate dedicated radio frequency of 155.475 MHz. This frequency will be used only as required for coordination and cooperation between different police agencies during emergencies.

The enclosed forms must be completed and processed in accordance with the following instructions.

The form entitled "Request for Operating Authorization" will provide the ILEEN Advisory Policy Committee with the necessary eligibility information for your agency's participation in ILEEN.

Your agency's eligibility will be confirmed upon your receipt of the "Concurrence Form" signed by the Superintendent of the Indiana State Police.

If your agency desires to participate in ILEEN, fill out one "Request for Operating Authorization" and the two "Concurrence Forms" and forward them to the Chief Communications Engineer. After your eligibility has been confirmed, the State Police Superintendent will sign the "Concurrence Forms" and one copy will be returned to your agency.

Those agencies presently licensed and located within the Chicago jurisdiction should file a Form #425 with the FCC Washington, D.C. office requesting modification of their present license. Those agencies presently licensed but not located within the Chicago jurisdiction should file Form #400 with the Washington, D.C. office.

Agencies operating under another agency's license should contact that agency to affirm its inclusion in the provisions of the agency's license. This applies to Town Marshals operating on a Sheriff's license and all other such arrangements.

A copy of the signed "Concurrence Form" must be included with the FCC License Application Form. Also, a cover letter should be included stating operation will be in, by, and under the Indiana Law Enforcement Network (ILEEN) plan.

The Federal Communications Commission has advised that frequency coordination is required for all new license applications and for present license holders outside the Chicago Region that are requesting modification.

If you do not choose to participate or are not eligible, we would appreciate your indicating this on the forms and returning them. If this condition changes at a later date, contact the ILEEN Advisory Policy Committee for instructions.

ILEEN will be operated in compliance with Part 89 of the Rules of the Federal Communications Commission and the regulations of the ILEEN Governing Board.

Agencies having a base station operation must obtain and install a monitor receiver on the channel; however, the primary licensee, Indiana State Police, will be the only agency licensed for base station transmitters.

Every effort is being made to get this information to every Indiana police agency utilizing two-way mobile radios. If you know of any agency not receiving this letter, please advise them to contact the ILEEN Advisory Policy Committee for instructions.

It behooves each participant to monitor this channel and maintain strict system discipline so that this new law enforcement tool may be utilized effectively for the benefit of Indiana law enforcement.

Superintendent
Indiana State Police

JTS: rw
Enclosures

(State Police Department; Ch I, Sec III; filed Dec 20, 1978, 2:43 pm: 2 IR 143; readopted filed Oct 17, 2001, 10:05 a.m.: 25 IR 935; readopted filed Jul 2, 2007, 3:01 p.m.: 20070711-IR-240070255RFA)

*