IDAHO STATE POLICE PROCEDURE

11.01 ILETS ACCESS REQUIREMENTS

A. General

The Idaho Public Safety and Security Information System (ILETS) is a network of computer systems built around an information broker, also known as a switch, which provides criminal justice and other authorized agencies the capability of obtaining Criminal Justice Information (CJI) from state, federal, and international criminal justice agencies. In addition, the system provides secure and efficient point to point delivery of messages between agencies and users. Pursuant to Idaho Code §19-5202, the Idaho State Police (ISP) provides administrative and technical support for the ILETS network.

ILETS is the gateway for its direct access agencies to the National Crime Information Center (NCIC), managed by the FBI and to the International Public Safety and Security Information System (Nlets); managed by the states. ISP is the NCIC CJIS System Agency (CSA) and is responsible for the security and integrity of communication between ILETS, NCIC, Nlets, and other interfaced systems.

B. Definitions

"Criminal History Record Information" (CHRI) is a subset of CJI and is also known as "restricted data." Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI.

"Criminal Justice Information" (CJI) refers to all FBI CJI provided data necessary for law enforcement and civil agencies to perform their missions, including biometric, identity history, biographic, property, license plate reader data, and case/incident history data.

"Direct Access" means any electronic device, including a computer, workstation, or mobile data device loaded with software or other connection, which accesses ILETS.

"Idaho Hot Files" include the State's Concealed Weapons License file, certain No-Contact Order files that do not qualify for entry into NCIC, and Idaho civil warrants.

"ILETS Intranet" can only be accessed using a computer / terminal programmed for ILETS access. This internal website contains news updates, BCI Audit & Training (BAT) Team class schedules and contact information, ILETS library, ILETS Conference Information, a TAC page containing forms and agreements, and a specific page for each subject matter area in the BAT Team.

"ILETS user" means any person who, through an ILETS terminal, may launch inquiries and/or make entries, or perform associated transactions.

"Indirect Access" means access to CJI derived information from ILETS, but no direct terminal access to perform inquiries of make record entries.

"NCIC Non-Restricted Files" are records that may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities. These files include Wanted File, Stolen Property File, Active Protection Order File, No Contact Order File, and Missing and Unidentified Persons Files.

"NCIC Restricted Files" shall be protected as CHRI and includes Gang Files, Known or Appropriately Suspected Terrorist Files, Supervised Release Files, National Sex Offender Registry Files, Historical Protection Order Files, Identity Theft Files, Protective Interest Files, Person with Information (PWI) data in the Missing Person Files, Violent Person File, and the National Instant Criminal Background Check System (NICS) Denied Transaction File.

"Terminal Agency Coordinator" (TAC) means the person assigned by an agency or work unit to serve as a liaison between the agency or work unit and the ILETS support staff. The ILETS Operating Manual lists the duties of a TAC and is located in the library on the ILETS Intranet.

C. Management Responsibilities

1. Each ISP Captain/Manager of a district or work unit with direct access to ILETS, or indirect access to CJI derived from ILETS, is responsible for:
    a. Compliance with:
        i. Title 28, Part 20 Code of Federal Regulations (CFR) for regulatory guidance for dissemination of Criminal History Record Information (CHRI);
        ii. Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy requirements, including creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI;
        iii. Idaho Statute Title 19 Chapter 52 – Public Safety and Security Information System, and Title 67 Chapter 30 – Criminal History Records and Crime Information; and
        iv. Idaho Administrative Code 11.10.01 – Rules Governing ILETS.
    b. Proper access, use, and dissemination of NCIC Restricted and Non-Restricted Files, Nlets Files, Idaho Hot Files, Idaho Criminal History Database, and Idaho Department of Motor Vehicle information.
    c. Proper protection of Personally Identifiable Information (PII) derived from CJI.
    d. Submission of all TAC and Assistant TAC (ATAC) appointment forms to ilets@isp.idaho.gov.
    e. Maintaining updated ILETS Access Agreement Forms.
    f. Maintaining user profiles and records of all:
        i. CJIS Security Awareness training, testing, initial and annual recertifications; and

ii. ILETS direct-access users' training, testing, and biennial recertifications at the level to which they have access for their job responsibilities.

g. Maintaining an EHF 11 01-01 Statement of Confidentiality for all ILETS users and for any employee handling CJI derived from ILETS.
h. Complete a triennial audit with the BCI ILETS Audit & Training Specialists. The pre-audit questionnaire must be completed prior to your audit and will be assigned using the CJIS Audit website.
i. Participate in triennial audit(s) with the FBI if selected to do so.

2. The duties stated in this section may be assigned to the appointed TAC or ATAC. It is highly recommended that the TAC/ATAC attend annual TAC training provided by the BCI ILETS Audit & Training Team.

D. User Training and Certification

1. The BCI Auditing and Training Team distributes schedules of ILETS training via:
   a. posting in nexTEST under Class Management;
   b. sending an ILETS Administrative Message (APB);
   c. sending all TACS an e-mail;
   d. posting on the ILETS Intranet; and
   e. inclusion in the biennial IDARAP newsletter.

2. Upon initial hire, and prior to receiving ILETS access, the end-user must complete the appropriate level of CJIS Security Awareness Training on CJIS Online.

3. Annually, all persons with unescorted access to a physically secure location must complete their assigned level of CJIS Security Awareness Training by using the CJIS Online website.

4. Within 3 months of receiving ILETS access, the user must pass the ILETS certification test consistent with assigned duties on the NexTEST website. It is highly recommended that the ILETS user also attend the appropriate ILETS class(es) consistent with assigned duties.

5. Biennially, each ILETS user must recertify ILETS proficiency by completing the test consistent with current certification and usage of the system by using the nexTEST website. It is highly recommended that each user attend an in-person or virtual refresher class consistent with their current certification, or complete Computer-Based Training (CBT) modules consistent with current certification and usage of the system on the CJIS Launch Pad website: CJIS Launch Pad (cjisapps.com).

E. ILETS Certifications Security Roles

1. The Restricted Inquiry certification allows users to run driver and vehicle

registration information from the Idaho Department of Transportation (ITD), Wanted File, Hazardous Materials File, Boat File, and Snowmobile File. ISP Mobile Data Computers/Terminals (MDCs/MDTs) are typically configured for these capabilities along with access to the Idaho Hot Files.

2. The Limited Inquiry certification provides users with all Restricted Inquiry file access, in addition to NCIC property files (e.g., Stolen/Lost Gun File, Article File, Securities File, etc.). Persons assigned this security role do not need to complete the Restricted Inquiry certification test.

3. The Full Inquiry Certification provides users with all Restricted and Limited Inquiry File access, in addition to access to all available query message keys, CHRI, Interpol, and Canadian Files. In addition, users can send administrative messages. Persons assigned this security role do not need to complete the Restricted or Limited Inquiry certification test.

4. The Entry Certification is required of users who enter records into NCIC and/or the Idaho Hot Files and complete monthly validations. Persons assigned this security role must complete the Full Inquiry and Entry certification test.

H. System Misuse and Security Incidents

1. System misuse occurs any time the system is used for any purpose not expressly authorized by State and federal regulations.

2. Misuse of the ILETS system can be prosecuted under Idaho Code § 67-3009 as a misdemeanor or felony offense. The privacy ACT of 1974 and the Computer and Abuse Act of 1986 are two federal statutes affording criminal and civil liability for violations of privacy and security provisions relating to the use of CHRI. All suspected cases of misuse must be reported Immediately to the Bureau of Criminal Identification (BCI) Audit & Training Team Supervisor.

3. Security-related incidents that impact ILETS data or communications circuits shall be reported to the BCI ILETS Information Security Officer (ISO) by completing a security incident form located at https://isp.idaho.gov/bci/incident-response/.

4. If an ILETS user is unsure about the legitimacy of any ILETS transaction, the user can request guidance by contacting the BCI Auditing and Training Team at (208) 884-7130 or email: Ilets@isp.idaho.gov.