

Idaho Department of Correction 	Standard Operating Procedure Department- Wide General Administration	Control Number: 146.00.01.001	Version: 1.4	Page Number: 1 of 9
		Title: ILETS: Idaho Public Safety and Security Information System		Adopted: 12-22-2010 Reviewed: 12-22-2010 Next Review: 12-22-2012

This document was approved by Brent Reinke, director of the Idaho Department of Correction, on 12/22/10 (signatures on file).

BOARD OF CORRECTION IDAPA RULE NUMBER

[None](#)

POLICY STATEMENT NUMBER 146

[ILETS: Idaho Public Safety and Security Information System](#)

POLICY DOCUMENT NUMBER 146

[ILETS: Idaho Public Safety and Security Information System](#)

DEFINITIONS

[Standardized Definitions List](#)

Idaho Public Safety and Security Information System (ILETS): A dedicated data communications network that links local, state, and federal criminal justice agencies to state records and files and to the National Crime Information Center (NCIC) system. (The Idaho Public Safety and Security Information System was previously known as the Idaho Law Enforcement Teletypewriter System.)

ILETS Operator: An Idaho Department of Correction (IDOC) staff member certified by a terminal agency contact (TAC) to use and access the Idaho Public Safety and Security Information System (ILETS).

Interstate Identification Index (III) File: An automated index of persons (1) maintained in the National Crime Information Center (NCIC) system, and (2) that includes names and personal identification relating to most individuals who have been arrested or indicted for a serious criminal offense anywhere in the country.

Manager: An employee appointed to manage, direct, and control a designated work unit. Managers include division chiefs, deputy division chiefs, facility heads, deputy wardens (or second-in-commands), district managers, designated lieutenants, program managers, or any appointed unit manager.

National Crime Information Center (NCIC) System: A nationwide criminal justice information system (1) owned and maintained by the Federal Bureau of Investigation (FBI) that is dedicated to serving and supporting local, state, and federal criminal justice agencies, and (2) capable of providing users information from various types of records and files that includes, but is not limited to, enhanced name and fingerprint searches, mug shots, records of subjects under the supervised release of probation and parole, convicted sex offender

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 2 of 9
---	------------------------	---	-------------------------------

and violent sexual predator registries, interstate identification index (III) information, information linking, and online manuals and resources.

Terminal Agency Contact (TAC): An Idaho Department of Correction (IDOC) staff member responsible for training and certifying Idaho Public Safety and Security Information System (ILETS) operators.

PURPOSE

The purpose of this standard operating procedure (SOP) is to establish standardized guidelines and procedures for authorized Idaho Department of Correction (IDOC) staff use of the Idaho Public Safety and Security Information System (ILETS).

SCOPE

This SOP applies to any staff member trained and authorized to use the ILETS in the performance of his duties.

RESPONSIBILITY

Director of the IDOC

The director of the IDOC (or designee) is responsible for:

- Entering into a direct access agreement with the Idaho State Police (ISP) for authorizing designated IDOC staff the use of the ILETS; and
- Ensuring annual ILETS audits are conducted at Central Office on director’s office staff members who are authorized ILETS users.

Division Chiefs

Division chiefs (or designees) are responsible for ensuring annual ILETS audits are conducted at all IDOC locations where their staff members are authorized ILETS users.

Managers and Facility Heads

Managers and facility heads (or designees) are responsible for:

- Implementing this SOP and ensuring staff adhere to the guidelines provided herein;
- Selecting and ensuring the training of one (1) or more terminal agency contact (TAC);
- Developing (where needed) an institutional field memorandum to help implement this SOP; and
- Ensuring institutional field memorandums (when developed) do not replicate, duplicate, or supersede the guidance provided herein.

Table of Contents

General Requirements3
1. Introduction3

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 3 of 9
---	------------------------	---	-------------------------------

2. ILETS Use and Management.....	4
Uses	4
Management	4
3. TAC Duties and Responsibilities.....	5
4. Criminal Background Investigations (CBI)	5
Reasons for Conducting a CBI.....	5
Documentation of a CBI	5
5. Warrants.....	6
Entering Warrants on Parole Absconders and Escapees	6
Responding to Hit Confirmation Requests	6
Documenting the Warrant Files and NCIC Warrant Roster.....	7
6. ILETS Operator: Approval, Initial Training, Written Exam, and Recertification	7
7. Security	8
Computer Terminal Security.....	8
Information Security	8
8. Audits	8
Quarterly Internal Audits.....	8
External Audits	9
References.....	9

GENERAL REQUIREMENTS

1. Introduction

The ILETS is provided by the ISP, Bureau of Criminal Investigation (BCI), and is comprised of hardware, software, electronic switches, peripheral gear, microwave links, and circuitry needed to operate and use the system. The ILETS provides identification and information services such as criminal history information, sex offender information, wanted and missing person information, stolen property information, and motor vehicle and driver's license information to criminal justice agencies throughout the State of Idaho.

In addition to local and State of Idaho information, the ILETS also access information from other systems, such as the National Crime Information Center (NCIC) system, the International Justice and Public Safety Network (NLETS), and the Idaho Record Management System. (NLETS was previously known as the National Law Enforcement Telecommunications System.)

The IDOC contracts with the ISP and uses the ILETS as described in [section 2](#).

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 4 of 9
---	------------------------	---	-------------------------------

2. ILETS Use and Management

Uses

The IDOC uses the ILETS for the following:

- **Criminal Background Investigations (CBI)** – CBI (see [section 4](#)) are performed on all offenders, existing and new employees (to include rehires), reinstated employees, contract staff, visitors, volunteers, and contractors. CBIs for new employees are performed in accordance with policy [211, Hiring and Probation](#). ILET operators enter the ILETS and retrieve criminal information on persons on a case-by-case basis.
- **Warrants** – Arrest warrants are entered for parole absconders and escapees as described in [section 5](#). Warrant checks are also conducted on offenders who are about to be released from IDOC custody.
- **Other Secure Law Enforcement Communications** – ILET operators may use ILETS for other secure law enforcement communications such as running various criminal histories, vehicle registration queries, **or** sending administrative messages to other agencies.

Note: The ILETS requires high security (see [section 7](#)) and therefore, its use is restricted to approved ILET operators.

Management

Standards

Information entered into **or** received from the ILETS may be critical to the apprehension and arrest of fugitives, and as a result, it is vital that data entry, inquiries, and responses meet certain standards of timeliness, accuracy, and completeness.

- **Timeliness** – Warrants must be entered immediately when the information is received from the Commission of Pardons and Parole. CBIs (see [section 4](#)) should be performed as soon as possible after receiving the individual's information.
- **Accuracy** – The accuracy of ILETS data entry must be double-checked by a second party. This occurs after a warrant is entered into the ILETS by an ILET operator. The ILET operator then verifies the warrant file.
- **Completeness** – ILETS data entry must contain all information that was available at the time it was given. If additional information is obtained afterwards, it must be added to the system in a timely manner.

Misuse

Both State of Idaho and federal law addresses the proper use of information obtained through the ILETS. (Federal law does not address the ILETS but addresses the information that can be obtained from other federally maintained systems linked to the ILETS.) Misuse of information obtained through the ILETS is a misdemeanor, **and** the misuse of that information for financial gain is a felony. (For more information, see appendix A, *Statement of Criminal History Record Information [CHRI] Confidentiality*.)

Additionally, misuse of the ILETS may result in corrective or disciplinary action in accordance with SOP [205.07.01.001, Corrective and Disciplinary Action](#).

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 5 of 9
---	------------------------	---	-------------------------------

3. TAC Duties and Responsibilities

Managers and facility heads (or designees) may appoint one (1) or more TACs at Central Office (as required by director's office or division assigned duties) **and** at each correctional facility **or** probation and parole district office. TACs will be responsible for the following:

- Collecting and maintaining an *ILETS Operator Approval Form* (appendix B) on all ILETS operators for their Central Office, correctional facility, or probation and parole district office location;
- Maintaining and updating a current roster of ILETS operators for their Central Office, correctional facility, or probation and parole district office location;
- Forwarding (upon request) a copy of the current roster of ILETS operators to the Central Office TAC;
- Training – ILETS operators must receive training in accordance with [section 6](#);
- Maintaining ILET training and certification records on all ILETS operators;
- Communicating with ISP, BCI staff on all ILETS matters and facilitating BCIs external audit (see [section 8](#));
- The timely monthly validation of records requested by the ISP, BCI staff; and
- Performing internal ILETS audits **and** ensuring that their Central Office, correctional facility, or probation and parole district office location is prepared for an external audit. (See [section 8](#).)

4. Criminal Background Investigations (CBI)

A CBI is an investigation conducted using the ILETS to access (a) motor vehicle records, (b) criminal history records in Idaho and other states, **and** (c) interstate identification index (III) files to determine if an individual has any criminal background.

Reasons for Conducting a CBI

- If required by SOP [510.02.01.001](#), *Facility Access*.
- For all employees and contract staff hired by the IDOC. (See policy [211](#), *Hiring and Probation*.)

Documentation of a CBI

- All CBIs will be documented (logged) by the ILETS operator performing the CBI.
- Each Central Office, correctional facility, and probation and parole district office location will maintain appendix C, [Criminal Background Investigation Log](#), and document information on each CBI completed. (It is not a requirement to document each ILETS query made. For example, an investigator may run a dozen or more queries to prepare a single presentence report but will only be required to log that particular investigation once.) The CBI Log will be used to document the following information:
 - ◆ IDOC location (e.g., Idaho State Correctional Institute [ISCI]);
 - ◆ Date the CBI was conducted;

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 6 of 9
---	------------------------	---	-------------------------------

- ◆ Name of the individual the CBI was conducted on;
 - ◆ Purpose of the CBI (e.g., new employee, public volunteer, visiting);
 - ◆ ILETS operator's name and employee number;
 - ◆ Results of the CBI (C = clear or NC = not clear); and
 - ◆ Whether CBI information was distributed and to whom it was distributed to.
- In order to accurately track CBIs, in all ILETS screens that require an operator's name, operators will enter their Novell client 'username' **and** then a letter code identifying the reason for the request. The letter codes are:
 - C – Contractor
 - H – Offender criminal history
 - N – New employee
 - O – Other (record the specific reason for the request)
 - P – Public volunteer
 - R – Reception/Diagnostic Unit (RDU) offender
 - T – Training
 - V – Visiting
 - W – Warrant research

Note: For example, if Sally Moose was conducting a CBI for a visiting applicant, the operator's name might be entered as such: SMoose - V.

5. Warrants

The IDOC will enter, maintain, and clear warrants in the ILETS for parole absconders, as well as, entering temporary warrants for escapees, if needed.

Note: For consistency in entry and reporting, all warrants will be managed by Idaho State Correctional Institution (ISCI) ILETS operators, unless conditions prevent it.

Entering Warrants on Parole Absconders and Escapees

- Parole absconders – After the Commission of Pardons and Parole has signed a warrant for the arrest of the absconder, the designated ILETS operator will enter the warrant into the ILETS.
- Escapees – When an offender escapes, an ILETS operator may enter a temporary warrant into the ILETS in accordance with SOP [507.02.01.002](#), *Escape/Walk-away Response*.

Responding to Hit Confirmation Requests

When a Hit Confirmation Request is received from another law enforcement agency, an ILETS operator will respond within the following time frame:

- Urgent priority – 10 minutes; and

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 7 of 9
---	------------------------	---	-------------------------------

- Routine priority – One (1) hour.

Documenting the Warrant Files and NCIC Warrant Roster

Warrant Files

All active warrants will have a physical warrant file that contains the information used to enter the warrant. The warrant file will include the following, at a minimum:

- A copy of the written warrant signed by the Commission of Pardons and Parole;
- The request to enter the warrant into the ILETS; and
- Printouts of all information gained in the CBI.

NCIC Warrant Roster

All warrants entered into the ILETS will be documented using appendix D, [NCIC Warrant Roster](#). The [NCIC Warrant Roster](#) will be used to document the following information:

- IDOC location (e.g., ISCI);
- Offender's name;
- Offender's IDOC number;
- NCIC file number;
- Warrant date;
- Date of entry;
- Locating ORI (originating agency identifier);
- Date of clear; and
- Clearing ILET operator's name and employee number.

6. ILETS Operator: Approval, Initial Training, Written Exam, and Recertification

It is important that all ILETS operators be approved by a manager, appropriately trained on the proper use of the ILETS, **and** understands the importance of confidentiality.

- **Approval** – Managers shall designate employees to become ILETS operators by submitting appendix B, *ILETS Operator Approval Form*, to their respective TAC.
- **Initial training** – Initial training will consist of a block of instruction from the TAC (or designee). ILETS operators must receive this initial training before they are given access to the ILETS. (Also see the note box below.) ILETS operators must:
 - ◆ Be trained on the importance of adhering to both ISP **and** NCIC system standards and policies when accessing the ILETS **and** NCIC system data;
 - ◆ Receive the appropriate level of training (e.g., inquiry, entry, or TAC) from ISP for their assigned duties and responsibilities.
- **Written exam** – All ILETS operators must pass a written exam within the first six (6) months of gaining ILETS access. The written exam is provided by the ISP, BCI.
- **Recertification** -- All ILETS operators must be recertified every two (2) years.

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 8 of 9
---	------------------------	---	-------------------------------

Note: Before gaining access to the ILETS, all ILETS operators are required to sign (a) appendix A, *Statement of Criminal History Record Information [CHRI] Confidentiality*, and (b) an *Idaho Public Safety and Security Information System, Security Awareness Training* document. Once signed, a copy of both documents will be retained by the TAC, and the originals forwarded to Human Resource Services (located at Central Office) for placement in the ILETS operator's personnel file.

Note: The Security Awareness Training document lives in the ILETS secure website and can be provided by the TAC or a certified ILETS operator.

7. Security

The data stored in the ILETS, the NCIC system, and other criminal justice information systems such as NLETS and the Idaho Record Management System is documented criminal justice information. Information retrieved from these systems must be protected to ensure its integrity and its correct, legal and efficient storage, dissemination, and use.

Computer Terminal Security

The computer terminal that accesses the ILETS must have adequate physical security (e.g., logon ID and password) to protect against any unauthorized viewing or access. Before walking away from the computer terminal (regardless of the amount of time), ILET operators shall ensure that the terminal is locked **or** that they log off. A locked terminal is one that when locked, screen data cannot be viewed and no keyboard entries can be made.

Note: All ILETS operators shall be approved and trained as provided in [section 6](#).

Information Security

All information retrieved via the ILETS is highly confidential. To prevent the misuse of information retrieved via the ILETS, any information that is printed must be retained in a secure area **or** immediately destroyed after its intended use.

Note: Printed ILETS information shall be destroyed by shredding. Paper shredding service providers such as Cintas and Shred-it shall not be allowed to shred printed ILETS information. Printed ILETS information must be shredded in IDOC-owned shredders by the ILETS operator.

8. Audits

Quarterly Internal Audits

Designated TACs at each Central Office, correctional facility, or probation and parole district office location will conduct a quarterly audit of CBIs and warrant entries, to verify that (a) the ILETS is being properly used and secured (see [section 7](#)), (b) all ILETS data entry is timely, accurate, and complete, **and** (c) all other requirements described in this SOP are being met.

To accomplish the above, TACs will spot check their Central Office, correctional facility, or probation and parole district office *Criminal Background Investigation Log* entries against Forsee/Com Web log queries. (All ILETS operators that have had ILETS access removed since the last audit should be included in the spot checked.) TACs shall be

Control Number: 146.00.01.001	Version: 1.4	Title: ILETS: Idaho Public Safety and Security Information System	Page Number: 9 of 9
---	------------------------	---	-------------------------------

responsible for reporting any misuse to the ILETS operator's manager and supervisor (also see [section 2](#), subsection titled "Misuse").

Note: Forse/Com Web is a computer application that is designed for use on the ILETS and other law enforcement communication networks.

External Audits

The ISP, BCI may randomly select specific IDOC locations (i.e., Central Office, a specific correctional facility, or a specific probation and parole district office) for an audit every three (3) years. BCIs audit will include a policy compliance review, a data quality review, and a risk analysis.

REFERENCES

Appendix A, *Statement of Criminal History Record Information (CHRI) Confidentiality*

Appendix B, *ILETS Operator Approval Form*

Appendix C, *Criminal Background Investigation Log*

- [Appendix C \(Fill-in version\)](#)

Appendix D, *NCIC Warrant Roster*

- [Appendix D \(Fill-in version\)](#)

Code of Federal Regulation, Title 28, Chapter I, Part 20, Subpart A, Section 20.3, *Definitions*

Department Policy [211](#), *Hiring and Probation*

Federal Bureau of Investigation (FBI), National Crime Information Center (NCIC), *NCIC 2000 Code Manual*

Federal Bureau of Investigation (FBI), National Crime Information Center (NCIC), *NCIC 2000 Operating Manual*

Idaho Code, Title 67, Chapter 30, Section 67-3009, *Criminal Penalties*

Idaho State Police (ISP), Bureau of Criminal Investigation (BCI), *Idaho Public Safety and Security Information System (ILETS) Manual, February 2006*

IDAPA 11.10.01, *Rules Governing Idaho Public Safety and Security Information System*

Standard Operating Procedure [205.07.01.001](#), *Corrective and Disciplinary Action*

Standard Operating Procedure [507.02.01.002](#), *Escape/Walk-away Response*

Standard Operating Procedure [510.02.01.001](#), *Facility Access*

Tailored Solutions Corporation (www.forse.com)

United States Code, Title 5, Part I, Chapter 5, Subchapter II, Section 552a, *Records Maintained on Individuals*

United States Code, Title 18, Part I, Chapter 47, Section 1030, *Fraud and Related Activity in Connection with Computers*

United States Code, Title 28, Part II, Chapter 33, Section 534, *Acquisition, Preservation, and Exchange of Identification Records and Information; Appointment of Officials*

IDAHO DEPARTMENT OF CORRECTION
Statement of Criminal History Record Information (CHRI) Confidentiality

Authorized Usage and Dissemination of Criminal History Record Information (CHRI) Obtained through the National Crime Information Center (NICI) System

Idaho Code, Section 67-3009 states " It is unlawful for a person for personal gain to request, obtain, or attempt to obtain criminal history records under false pretenses or willfully communicate or attempt to communicate criminal history records to any agency or person not authorized to receive the information by law. "

The United State Department of Justice and federal courts have interpreted Title 28, United States Code (USC), Section 534 (the basic and fundamental authorization for the collection, acquisition, exchange and dissemination of CHRI) to restrict access to Federal Bureau of Investigation (FBI) CHRI to criminal justice agencies for criminal justice purposes and to federal agencies authorized to receive it pursuant to a federal statute or executive order.

Title 28, Code of Federal Regulations (CFR), Section 20.3(g), defines "criminal justice agency" as "(1) courts; and (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice." 28 USC 20.3(b) defines the term "administration of criminal justice" by stating that "the administration of criminal justice means performance of any of the following activities; detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders."

The Privacy Act of 1974 (5 USC 552a) and the Computer Fraud and Abuse Act of 1986 (18 USC 1030) are two federal statutes affording criminal and civil liability for violations of privacy and security provisions relating to the use of CHRI. Additionally, 28 USC 534 contains provisions calling for the cancellation of access rights by criminal justice agencies if the dissemination of CHRI is made outside the receiving department or a related agency. Furthermore most (if not all) states have laws which criminalize or provide civil liability for misuse/unauthorized dissemination of their CHRI.

CHRI recipients are again reminded that, with the exception of federally approved uses, the Interstate Identification Index (III) file may only be accessed and used by criminal justice agencies for criminal justice purposes. Users are also reminded that III may be used for a criminal justice employment background, but that such inquiry should be followed up with fingerprint submission.

I have read and understand the above information. By affixing my name to this document, I agree to abide by all of the laws, rules and regulations cited within this document.

Signature

Date

**IDAHO DEPARTMENT OF CORRECTION
ILETS Operator Approval Form**

This form must be completed by a manager (see the SOP for a definition of manager) and submitted to their Central Office, correctional facility, or probation and parole district office TAC.

Employee's Name (First, MI, Last): _____

Location: _____

Employee's Status: Temp Permanent

Supervisor's Name: _____

Date ILETS Access Needed By: _____

Reason for ILETS Access and Use

Based on the duties and responsibilities associated with this employee's position, ILETS access and use is needed for the following reason(s). (More than one reason may be selected as appropriate.)

- To conduct background investigations
- To enter arrest warrants
- To run various criminal histories
- To run vehicle registration queries
- To send administrative messages to other law enforcement agencies
- For other reasons not listed above. (Provide details below as appropriate.)

In addition to this request to allow the employee access and use of the ILETS, I agree that upon termination of this employee's position with the IDOC, or for any reason that no longer requires this employee's access or use of the ILETS, I will inform my Central Office, correctional facility, or probation and parole district office TAC as soon as reasonably possible.

Manager's Signature: _____

Date: _____



TAC Use Only

This employee was provided access to ILETS on: _____

This employee's access to ILETS was removed on: _____

(Note: After ILETS access is removed, maintain this form until the next quarterly internal audit and then destroy.)