Florida Intelligence Site

OPERATING GUIDELINES

2019

ACISS Version: 2.3.5.1205

Table of Contents

I.GOVERNING LAW AND STANDARDS

The InSite - Florida Intelligence Site Agency Agreement, User Agreement, and System Operating Guidelines are subject to and governed by Florida Statutes and the Code of Federal Regulations (28 CFR Part 23).

II. SYSTEM DESCRIPTION

The InSite - Florida Intelligence Site (hereinafter referred to as the System) is an application located on the Criminal Justice Network (CJNet), and serves law enforcement agencies (federal, state and local) by providing a secured computerized database of active criminal intelligence and active criminal investigative information to the legally authorized users across the state. The main goal of the System is to improve the effectiveness of criminal investigations on all levels and provide for the exchange of intelligence information between law enforcement agencies throughout the state. In addition, some members of the Criminal Justice Community may be provided access to the system on a case by case basis for those who have a need to know and a right to know the information contained within the system.

A) ADVISORY COMMITTEE

The Florida Department of Law Enforcement (hereinafter referred to as FDLE) shall establish the System Advisory Committee to oversee the operations of the system. This committee shall provide recommendations regarding security, privacy, management, and enhancements to the System. The committee members will consist of current InSite users which will be selected by the FDLE Regional Directors. The System administrator will maintain a current listing of committee members.

B) COMMITTEE MEETINGS

The committee will meet to discuss the operation, administration, and any identified issues of the System on an as needed basis, either in person, by telephone conference or via electronic communications, whichever the discussion topic necessitates. Committee meetings may be requested by any committee member and will be coordinated by the System administrator.

C) POLICIES

The System Advisory Committee shall work in concert with FDLE in the development of policies and procedures relating to the operation and use of the System.

III. RESPONSIBILITIES OF FDLE

A) ADMINISTRATION

FDLE shall administer, support and maintain the System. FDLE's Investigation and Forensic Science Program Office (hereinafter referred to as the IFS Program Office), will designate an individual to serve as the System Administrator for the System. This individual shall be the primary contact for participating agencies and individual users regarding requests for system assistance.

B) SECURITY

FDLE shall ensure that safeguards are in place, which will provide confidentiality for the information entered into any module of the System by Participating Agencies.

C) BACKGROUNDS

FDLE will conduct background investigations on all prospective users of the System in accordance with FDLE Policy. Upon receipt of an Individual User Agreement/Background Investigation Waiver form, FDLE will conduct a background investigation, which will include at minimum a search of the following: FCIC/NCIC, FDLE Automated Investigative Management System (AIM), and InSite. As well, Employment Verification will be obtained by way of the required supervisor signature on the individual User Agreement/Background check form which serves as acknowledgement of employment with the applicants identified agency. A user background will be conducted prior to the user receiving training or being given access to the System. Results of the background checks will be noted on the Individual User Agreement and handled as confidential. Original User Agreement/Background Investigation Waiver Forms will be retained by the respective FDLE Regional Operations Center for which training was received. A copy of the completed user agreement form will be sent to the IFS Program Office for filing and will be maintained by the System Administrator.

Individuals with an active Secret or Top Secret clearance are exempt from the above mentioned background, as Federal backgrounds are more comprehensive than the standard state level background completed for system access.

D) TRAINING

FDLE has designated trainers in each region that are responsible for training users in the proper use of the System.

E) USER ACCESS

Access will be granted to members of criminal justice agencies who have access to the CJNet. Access will be assigned upon completion of the required forms and training.

F) QUALITY CONTROL

FDLE is authorized to conduct quality control reviews of the System entries made by users of the participating agencies. These reviews shall help to ensure compliance with the System Operating Guidelines.

G) SUPPORT

FDLE, IFS Program Office, System Administrator (850-410-8795) can provide assistance to participating agencies regarding problems encountered with the System. If a participating agency is having problems with their connection to the CJNet, the FDLE Customer Support Center should be contacted at 800-292-3242.

IV. RESPONSIBILITIES OF PARTICIPATING AGENCY

A) COMPLIANCE WITH AGREEMENTS

The participating agency head must sign and submit a System Agency Agreement to FDLE prior to the Agency's users obtaining access to the System. The System Agency Agreement states that the participating agency head has read and agrees to follow all of the requirements set forth in the System Operating Guidelines. A change in the participating agency head shall cause a new System Agency Agreement to be executed within ninety days. It is the responsibility of the participating agency to initiate the execution of a New System Agency Agreement should a change in the agency leadership occur.

B) INDIVIDUAL USER ACCESS

The participating agency must ensure that all users who require access to the System have submitted all necessary documentation and are properly trained in the authorized use of the System. Additionally, the participating agency must ensure only authorized personnel are allowed to access the System and that users are not sharing their operator ID and password with others. The sharing of operator ID's and passwords is a serious breach of system security. Users who are found to have shared their operator ID and password may have their access to the System terminated and their agency notified.

Any misuse of the System or failure to comply with the operating guidelines can lead to an administrative investigation, internal investigation, or criminal investigation.

In order to reactivate a user's access, the participating agency head must submit a letter to the System Administrator requesting that the user's access be reactivated.

C) CHANGES IN PERSONNEL

The participating agency must notify the System Administrator when a user no longer requires or no longer is permitted access to the System or has separated from the agency. Should the identified former user have any System entries, the participating agency must identify a current System user to have these records transferred to in order for the participating agency to retain the records in the System. System entries cannot belong to an Inactive operator due to review and purge policies. If no other current System user exists or can be established, the participating agency agrees to have the records purged from the system.

D) SYSTEM MATERIALS

The participating agency must safeguard all materials, manuals, and handouts associated with the System. The agency must also ensure that distribution of these materials is limited to authorized personnel.

E) AUTHORIZED ENTRY AND QUERY

The participating agency shall determine which individuals within that agency will be authorized to access to the System.

F) RESPONSIBILITY FOR INFORMATION

All information collected, received, stored, accessed, used or disseminated from the System must be done in strict compliance with all existing criminal justice guidelines; including but not limited to: 28 Code of Federal Regulations (CFR), Part 23, Sections 119.011(3), 119.07(6)(b), and 119.072, Florida Statutes (2004), and the System Operating Guidelines.

The participating agency shall use its best efforts to insure the validity of all information entered into the System by the agency. Responsibility for the custody, timeliness, completeness, accuracy and reliability of any information accessible through the System remains with the agency originating and submitting the information to the System.

The participating agency must fully comply with all of the System quality control procedures, or risk removal of its information from the System, sanctions, and possible loss of access to the System.

G) SYSTEM ENTRY PROTOCOL

Agencies entering information into the System must maintain sufficient documentation within the contributing agency's own records management protocol to support each entry in the event of legal challenge. Each entering agency shall adhere to approved procedures and requirements to ensure the proper entry of data into the System. Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be entered into the System.

H) RESPONSIBILITY TO VERIFY INFORMATION

The System is not designed to provide users with information upon which official actions may be taken. The mere existence of records in the System should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. Only the facts, which led to the entry of the record into the System, can be used to establish probable cause in an affidavit. The agency that entered the information into the System should be contacted to obtain and verify the facts needed for any official action.

The participating agency will not allow the entry of any information regarding political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct and there is reasonable suspicion that the subject may be involved in the criminal conduct.

When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be entered in the System; however, it is the responsibility of the submitting agency to ascertain and clearly affirm the relationship to the key element of criminal activity.

I) DISSEMINATION PROTOCOL

Operators authorized to access the System may make information available to other members of their Agency for law enforcement purposes only, on a need to know and right to know basis. Dissemination is defined as the

sharing of information, either written or oral, to other members of the criminal justice community. All cases and reports contained in the System have one of the following dissemination levels:

1. **Check Before Disseminating:**
   This indicates that a user must obtain the permission of the entering agency prior to disseminating the agency's active criminal intelligence and investigative information to another law enforcement agency. If the originator declines to give permission for dissemination of information, the requestor will not disseminate the information contrary to the originator's permission. This is the default dissemination for all System entries.

2. **Do Not Disseminate:**
   This indicates that the user cannot disseminate the entering agency's criminal intelligence or investigative information to another law enforcement agency.

3. **Disseminate:**
   This indicates that the user can disseminate the agency's criminal intelligence or investigative information to another law enforcement agency.

J) DISSEMINATION TO OUTSIDE AGENCY "Third Agency Rule"

When searching the System, on behalf of another agency not having access to the system, the user MUST comply with all of the requirements of the "Third Agency Rule."

Third Agency Rule – a traditional implied understanding among criminal justice agencies that confidential criminal intelligence information, which is exempt from public review, will not be disseminated without the permission of the originator.

1. Users must first determine if the requestor is from a criminal justice agency and has a need and right to know about intelligence contained in the System.

2. If requested information is contained in the System, the user must verify the dissemination level of the information.

3. Each participating agency shall insure the dissemination of any information from the System is documented in a dissemination log, which shall be maintained for two years. The Individual User must document the actions taken to comply with this rule on the dissemination log.

4. The dissemination log must include: the subject of the query including identifiers (DOB, SSN, etc.), to whom the information was released, who released the information, the date of dissemination, and the purpose for which the information was released.

Only if the requirements identified above are met, due diligence of maintaining dissemination safeguards must be taken should any records from the System be disseminated to an outside agency. This includes not disseminating active intelligence information via any means that would subject it to public disclosure. Information should only be provided which provides the outside agency with a 'pointer' regarding the information they have a need to know/right to know, as well as the contact information provided in the records so that the outside agency can make direct contact with the originating agency contributing the intelligence.

K) LIABILITY FOR DISSEMINATION

The participating agency acknowledges that the records and information accessible through the System are subject to federal and state laws and regulations. Each agency shall assume liability for the acts, omissions, or conduct of its own employees as applicable in Florida Statutes, without waiving any immunity or defense to which it may be entitled.

L) AUDITS

The participating agency shall keep sufficient records necessary and will cooperate with FDLE to make their records available for the purpose of conducting periodic audits of compliance with the terms of the System Operating Guidelines.

M) SECURITY

The participating agency must provide a reasonably secure area for the placement of all computer terminals used to access the System and will restrict access to authorized personnel.

If the agency deems it necessary to use its own network to provide access to the System, appropriate security measures must be in place to limit access to authorized criminal justice personnel only. These security measures must be compliant with CJIS/CJNet Security Policies set forth by the FDLE.

N) INFORMATION ERRORS

Any agency that finds information errors contained in the System should immediately notify the FDLE system administrator, in writing or email.

FDLE has the ability to make corrections or remove any information found to be incorrect, misleading, obsolete or otherwise unreliable. Every effort will be made by FDLE to consult with the agencies having an interest in the record. FDLE will maintain a log of all such corrections or deletions.

O) DISCLAIMER OF RESPONSIBILITY FOR ACCURACY OF RECORDS

FDLE affirmatively states that the existence of the System Agency Agreement and the Operating Guidelines does not cause FDLE to assume responsibility for the timeliness, accuracy and reliability of any information accessible through the System.

V. SECONDARY AGREEMENTS

The participating agency is not permitted to enter into any secondary agency agreements. Every agency accessing the System must enter into a System agency Agreement directly with FDLE.

VI. AMENDMENTS

The System Agency Agreement and the System Operating Guidelines shall not be altered, changed, or amended without the explicit permission of FDLE and then only in writing and as appropriate through the execution of an agreement between the participating agency and FDLE.

VII. SEVERABILITY

The terms of the System agency agreement and the System Operating Guidelines are severable. In the event that any of the terms of the System agency agreement or the System Operating Guidelines are deemed to be void or otherwise unenforceable, the remainder of the System agency agreement and System Operating Guidelines shall remain in full effect.

VIII.SUSPENSION OF SERVICES

FDLE reserves the right to immediately and unilaterally suspend an agency's access to the System when any material term or requirement of the System Agency Agreement or the System Operating Guidelines is violated.

IX. TERMINATION OF AGREEMENT

The System Agency Agreement is subject to termination if the agency violates any of the terms or conditions listed in the agreement. FDLE shall send a notice to the agency head of the agency regarding the proposed date by which the agency's access will be terminated and a description of the alleged agreement violation(s). The termination date shall be at least twenty days after the date of the notice if corrective action is not taken by the agency; however, suspension of System access may occur immediately and without prior notice if conditions warrant. The agency may terminate the System agency agreement any time after providing ten days written notice to FDLE.

X. PRESS POLICY

The System contains active criminal intelligence and investigative information, which is exempt from disclosure under the Public Records Act, per Section 119.07(6) (b), Florida Statutes. The terms "criminal intelligence information," "criminal investigative information," and "active" are defined at Section 119.011(3), Florida Statutes. Any release of information from the System should be made in conformance with the exemptions from dissemination imposed by Florida law. Participating agencies will not release information generated by another agency without first consulting the originating agency to determine the current status of that information. Information which is exempt from disclosure by law may not be released without the permission of the originating agency.

Although each participating agency is governed by its particular local policies regarding contacts with the media, the agency must notify FDLE of any press contacts or inquiries that appear to involve or have an impact upon the System users or the system as a whole.

XI. LEGISLATION

FDLE will monitor legislation for any possible impact on the System, and make recommendations for modifications to the system when necessary to maintain compliance with criteria and requirements established by Florida Statutes. FDLE will review existing and proposed rules and regulations to ensure compliance with applicable federal and state rules, regulations and statutes.

XII. INTELLIGENCE CASES

Each intelligence case type is designed to provide federal, state and local law enforcement agencies in Florida with the ability to document and share criminal intelligence and investigative activity with other participating agencies and authorized users. The System consists of different case types. Each case type represents a law enforcement issue such as criminal street gangs, major drug crime, domestic security, violent crime and major economic crime. New case types may be added as needed with the approval of the System Advisory Committee. Users can conduct searches for entities (subjects, addresses, vehicles, or telephone numbers) in the system regardless of the case type.

A) USER ACCESS

As an authorized user of the System, the user has a right to know and need to know the intelligence contained within ALL Case, Case Report, and Tip/SAR information in the System, regardless of the case type. However, cases of a sensitive nature can be restricted to certain users, when warranted. Records can only be Hidden by the System Administrator and are completed by request on rare occurrences for which the intelligence documented in the System necessitates the need to be documented, yet secure to only specified authorized users. The System administrator can assist your agency with this request.

B) PURGE CRITERIA

Cases that are five years old and determined by the originating agency to be no longer active intelligence should be marked for 'Purge'. These records will be purged by the System administrator in accordance with approved records retention schedules, with only statistical information being kept (the 'shell' of the record). The time a criminal subject is incarcerated may be used to extend the purge time for the amount of time the defendant was in custody.

Tip/SAR information should be reviewed 90 days after entry to make a determination of its status (Open/Closed). Tips/SARs that are unsubstantiated within a two year period must be reviewed by the originating agency to determine if the records should be purged from the system. Tips/SARs that are determined to no longer be valid should be marked for 'Purge' to be purged from the system by the System administrator in

accordance with approved records retention schedules, with only statistical information being kept (the 'shell' of the record).

NOTE: In compliance with section IV, sub-section 4, of the System Operating Guidelines, the Review/Purge process should be completed by the responsible agency and must be completed every 2 years for Tips/SARs and 5 years for Cases for compliance. The record owner will be notified within the System when it is time for such reviews. At this time, the operator identifies the record for retention or purge. Any agency failing to complete the Review/Purge process within one calendar year from the time the Review is scheduled to occur, and from the time the responsible party is notified via the System, accepts that the records identified will be automatically purged by the System administrator manually. Once a record is Purged it cannot be retrieved as this is a permanent action. Please see the Review and Purge Document for instructions on how to complete the Review and Purge process.

C) SYSTEM COMPONENTS

The System contains two primary components, Tips/Tasks and Cases. Each component has different criteria for the entry of information, access to the information, and retention of the information in the system.

The Tips/Tasks component is used to capture Domestic Security related tips and suspicious activity reports (SAR) received by law enforcement agencies and must be initially reviewed, assigned, and closed. This component can also be used to document tasks generated from within a law enforcement agency or Domestic Security Task Force. Each Tip/Task/SAR must be reviewed within two years of submission (entry date) into the System by the record owner.

The Cases component may only be used to enter and maintain information documenting reasonable suspicion to believe that criminal activity has or will take place, which information is pertinent to the detection, prevention, and mitigation of or response to crimes. Subjects entered into the System must be clearly identified as a Criminal or Non-Criminal.

(a). Criminal Suspect – Subjects for whom reasonable suspicion of involvement in criminal conduct or activity exists may be identified as a "Criminal Suspect" provided the information submitted is relevant to criminal conduct or activity.

(b). Non-Criminal Suspect - Other subjects may be entered into the System as a possible suspect, witness, victim, or a non-criminal subject as long as there is a connection to a case or tip that meets the reasonable suspicion threshold. The submitting agency is responsible for adherence to this requirement.

D) TYPES OF CASES

1. Major Drug Crime

The goal of these cases is to improve the effectiveness of narcotics investigations, provide for the exchange of drug intelligence among

agencies and help document and reduce the amount of illegal drugs in the State of Florida.

2. Criminal Street Gang

The goal of these cases is to improve the effectiveness of gang investigations, provide for the timely exchange of gang intelligence among agencies and to help document and reduce the impact of gangs in the State of Florida. These cases are also used to document gang subjects that meet the statutorily defined criteria per Florida Statute. Additionally, a Gang Member Status File is automatically created in the Florida Crime Information Center (FCIC) for subjects meeting the statutory criteria for classification as a gang member.

(2.1) Entry Protocol

This case type consists of a primary component that sets it apart from the other case types. When a subject's relationship is selected as criminal suspect, gang person or victim, the below Florida Gang Criterion will appear in a menu to be completed by the user.

Criterion	Occurrences
Admits to Criminal Gang Membership	1
Adopts Style/Dress of Criminal Gang	1
Adopts use of Hand Sign of Criminal Gang	1
Associates with one or more known Gang Members	1
Authored any Communication (crime responsibility)	1
Corroboration of Untested Informant Information	1
Has a Tattoo identified as used by Criminal Gang	1
ID as Criminal Gang Member by Documented Informant	1
ID as Criminal Gang Member by Parent / Guardian	1
Observed in the company of 1 or more Gang Members	4
Physical Evidence	1

(2.2) Statutory Membership Status

Subjects may have one of three Statutory Membership Statuses: Pending Gang Associate, Gang Associate or Gang Member.

1. *Pending Gang Associate:* Some, but not enough "occurrences" have been recorded to document one "criterion". For example, the subject is observed in the company of 1 or more Gang Members less than three times.

2. *Gang Associate*: One criterion has been met.

3. *Gang Member:* Two criteria have been met.

(2.3) Interface with FCIC

When a subject entered into a Criminal Street Gang case meets the statutory criteria for classification as a gang member (from one or multiple cases), a Gang Member Status File is automatically created in the Florida Crime Information Center (FCIC). Subjects who are classified as "affiliates" or "pending" will not be sent to FCIC. The status

files are also modified or deleted automatically as changes are made to subject records in the case. The Gang Member Status File is a status record only and an arrest should not be made based on these records.

Additionally, pursuant to Florida Statutes 119.07(2)(c)1 – Active criminal intelligence information and active criminal Investigative information are exempt from s. 119.07(1) and Section 24(a), Article I of the State Constitution. Do not disclose the Existence of this intelligence record to non-law enforcement personnel.

The following fields will be sent to FCIC: NAM, SEX, RAC, DOB, DOW, INC, OCA, OFF, PIK, MNU, and REM. Gang Member status files are NOT uploaded to the National Crime Information Center (NCIC); they are state records only.

3. Domestic Security

The goal of these cases is to improve the effectiveness of domestic security investigations and provide for the timely exchange of domestic security intelligence among agencies.

Authority - A Statewide Florida Domestic Security and Counter-Terrorism Database, authorized by Section 943.0321, Florida Statutes, is used for gathering, documenting and sharing intelligence related to terrorism, extremist groups and extremist individuals, among law enforcement agencies throughout the state.

Regional Domestic Security Task Forces – Florida Statutes, Section 943.0312 created The Domestic Security Task Forces (RDSTF) in each of FDLE's seven Regions (Tallahassee, Jacksonville, Tampa Bay, Orlando, Miami, Fort Myers and Pensacola). The RDSTF's have the responsibility to coordinate the prevention and mitigation of, and the responses to terrorist incidents to ensure proper training for state and local personnel. They also have a responsibility to collect and disseminate terrorist intelligence in a manner that will provide accurate, timely, and meaningful intelligence information to law enforcement agencies statewide.

4. Major Economic Crime

The goal of these cases is to improve the effectiveness of economic crime investigations, provide for the exchange of economic crime intelligence among agencies and help document and reduce the amount of economic crime in the State of Florida.

5. Violent Crime

The goal of these cases is to improve the effectiveness of communication sharing in violent crime investigations, by providing for the exchange of intelligence among agencies and help document and reduce the amount of violent crime across the State of Florida.

XIII. SPECIAL FUNCTIONS

A) eGuardian Export (SARs)

Agencies that use the System to document Florida suspicious activity reports (SARs) may also request that this data be exported to the Federal Bureau of Investigation (FBI) eGuardian system via an interface within the System. These Florida SARs are reviewed by the Florida Fusion Center to determine if they qualify and meet federal guidelines for exporting to the national eGuardian platform.

B) National Virtual Pointer System (NVPS)

The System interfaces with the Drug Enforcement Administration's (DEA) National Virtual Pointer System (NVPS). NVPS is a fully-automated pointer system that provides law enforcement agencies with the ability to determine if a subject is currently under investigation by other law enforcement agencies through the automated exchange of information. The entry of a criminal suspect meeting the data elements required by NVPS for submission will automatically be crosschecked in NVPS. If a possible match is identified, NVPS will return a positive response to the user (via ACISS Mail), which contains contact information for the originator of the matching record.

XIV. ACISS FUSION

The ACISS Fusion Client provides the ability to seamlessly connect the agency client ACISS system to the InSite system. Users have the ability to forward copies of Cases, Reports and Tips/SARs to the InSite system automatically. When these records are forwarded to InSite, the user can identify which components to export to InSite, including core entities and attachments, which are duplicated in the InSite system without any additional data entry.

The participating agency and users of ACISS Fusion are under the same policies defined in the Operating Guidelines for the System.

XV. GENERAL DEFINITIONS

These general definitions have been included in the System Operating Guidelines to assist readers with some of the terminology used throughout this document.

A. **Agency Agreement** – An agreement between FDLE and each criminal justice agency that desires to participate in and use the System. Once this document is signed and on file with FDLE, the agency shall be classified as a Participating Agency.

B. **Criminal Justice Network (CJNet)** – A statewide Intranet system designed by FDLE to provide criminal justice agencies with secure access to sensitive criminal justice information.

C. **The InSite - Florida Intelligence System (the System)** - An application located on the CJNet designed by FDLE, IFS Program Office, to allow criminal justice agencies to enter and share criminal intelligence electronically.

D. **The System Advisory Committee** – A committee designated by FDLE, consisting of members of Participating Agencies across Florida. This committee will provide recommendations regarding policy, management and enhancements to the System.

E. **Individual User Agreement** – A form completed by each individual to request access to the System. This form is to be completed upon request for user access and must be accompanied by a Supplemental Background form. This documentation and successful completion of a background investigation is necessary prior to training.

F. **Participating Agency** – A criminal justice agency with a signed System Agency Agreement on file with FDLE, having authorized users with access to the System.

G. **Regional Trainers** – Individuals designated by FDLE, Regional Operations Centers, who are authorized to provide System training and assistance to the Participating Agencies in their respective region.

H. **Suspicious Activity Report –** an established, unified, standards based approach for all levels of government to gather, document, process, analyze, and share information about behavior-based suspicious activities that potentially have a nexus to terrorism while rigorously protecting privacy, civil rights, and civil liberties of all Americans.

I. **Supplemental Background** – Each Individual User form submitted requesting access to the System must submit an updated supplemental background form.

J. **System Administrator** – A member of FDLE, IFS Program Office, who will administer the System and serve as the primary contact for system users.

K. **Criminal Conduct** - Activities, which constitute a violation of the criminal laws of the state of Florida, the United States or any jurisdiction in the United States.