Gulf Coast HIDTA SAFETNet Policy

Mission Statement

The mission of SAFETNet is to provide a secure and electronic solution to those participating law enforcement agencies across the country for event and target deconfliction. The system allows participating federal, state, local, and tribal agencies to deconflict events and targets for all categories of crime. The system enhances officer safety by alerting agencies of simultaneous operations in relation to time and place, while allowing participating agencies the capability to share information.

SAFETNet Defined

SAFETNet is an internet based system created for the purpose of providing participating agencies the capability to facilitate and share active investigative target pointer information. Designed to be a true pointer system, rather than an intelligence system, SAFETNet serves as a vehicle for timely notification of active investigative conflicts.

The Office of Justice Programs has determined SAFETNet to be a true pointer index system and 28 CFR Part 23 (Operating Criminal Intelligence Systems) does not apply. SAFETNet is in compliance with all applicable federal regulations.

The design of the system allows and facilitates information sharing among and between all participating HIDTA SAFETNet instances. The SAFETNet system will also connect and by default send information to the National Virtual Pointer System (NVPS). All participating agencies must adhere to this policy to maintain the integrity of the deconfliction process and system.

Goals

The goals of SAFETNet are to:

- Improve officer safety,
- Improve information sharing between law enforcement agencies,
- Facilitate and improve communication between participating agencies,
- Facilitate and improve coordination and cooperation between participating agencies.

System Access

There are two ways to access the SAFETNet system for participating agencies:

1. Watch Center via telephone service
2. Remote access via secure internet connection

Required information for deconfliction through SAFETNet

*****Entries must be associated with an active and ongoing criminal investigation*****

Events – Any law enforcement action that is scheduled to occur at a certain time or span of time and location. Events can be associated with your subjects but are time specific. Length of time is determined by the user not to exceed a period of two weeks. All events have a default radius set by the system administrator.

- Address – minimum required fields
  - Agency case number
  - Event type – i.e. Search Warrant, Knock and Talk
  - Start date
  - Start time
  - End date
  - End time
  - Location of event
  - City
  - State

Targets – Any element of an active criminal investigation including persons, places and things. Targets will remain active in the system for up to 180 days, unless extended thereafter.

- Persons – minimum required fields
  - Agency case number
  - First and Last Name
  - Gender
  - Date of Birth

- Businesses – minimum required fields
  - Agency case number
  - Business name

- Vehicles – minimum required fields
  - Agency case number
  - License Plate Number
  - License Plate State of Origin

- Weapons – minimum required fields
  - Agency case number
  - Caliber

- Internet – minimum required fields
  - Agency case number
  - Either screen name or email address

- Accounts – minimum required fields
  - Agency case number
  - Financial Institution
  - Account number

- Telephones – minimum required fields
  - Agency case number
  - Telephone number of targets only (no batch loading)

Notification and Resolution of Conflicts

1. Users with conflicts are notified immediately via email, text or on screen and are provided with users contact information ONLY.
2. In order to ensure resolution of conflicts follow up will be made via telephone in a timely manner to all users involved in the conflict.
3. Participating agencies have a responsibility to ensure their users are responding to conflict notifications.

Participating Agency

Participating Agency is any agency of local, county, state, federal or tribal government which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through a regional intelligence system.

Participating agencies must identify an administrative point of contact(s) that is authorized to act on behalf of the agency.

Agency Point of Contact(s)

1. Participating agencies must submit a completed User Agreement Form (attached) providing a point of contact for their agency. The administrative point of contact shall ensure that SAFETNet operating policies are followed.
2. The point of contact will be the focal point for all communication between the agency and the respective HIDTA.

3. The point of contact will notify the HIDTA immediately of changes to user's authorizations, new users, relocations or terminations.

Participating Agency Users

1. Each agency point of contact shall certify by the User Agreement Form (attached) or by other comparable means that users are employees or sworn officers of the agency and have agency authorization to access SAFETNet.
2. A current list of authorized agency users shall be maintained by the HIDTA and every six months this list will be provided to the agency point of contact. The participating agency point of contact will audit the list and notify the HIDTA of updates as necessary.

System Training

The Gulf Coast HIDTA will provide training to all users approved for access to the system and will provide periodic training updates as needed to all current users as part of their ongoing outreach programs.

System Audit Requirements

An audit trail is a tool for each HIDTA to protect against unauthorized access to information, intentional or unintentional, contained within the SAFETNet system. It is also a monitoring tool for the staff of each HIDTA to use to ensure that the operating policies and procedures of the SAFETNet system are followed.

The system audit trail is based on the who, what, and when premise. The Gulf Coast HIDTA must be able to determine *who* has accessed the SAFETNet system, *what* information was gained from the system, and *when* the access occurred.

1. Audits will be performed at the supervisory or managerial level.
2. Audits shall be conducted every six months or more frequently as deemed appropriate.
3. Each agency point of contact shall, upon the completion of the audit, certify in writing or by email to the Gulf Coast HIDTA that each user is a current employee with authorization to access SAFETNet and all user information is current and correct.
4. Agency users email address shall be that of the participating agency's email domain or other secure email system sponsored by a law enforcement agency. Commercial email domains such as Yahoo! Mail, Google Gmail, Hotmail or other internet providers that are not law enforcement related are not acceptable.

Non-Compliance

Violations of this policy can result in sanctions ranging from a verbal/written notification of policy violation up to barring access to the system.

System Security

It is the policy of the SAFETNet Deconfliction System Administrators to ensure Law Enforcement Sensitive information is only transmitted to trusted parties on trusted systems.

Trusted systems must be Federal Information Security Management Act (FISMA) certified in order to store or process Law Enforcement Sensitive data.

Definitions

Agency User - Is any member of a participating agency that has been vetted via User Agreement Forms or other comparable means and approved by the HIDTA.

Conflict - A conflict occurs when data submitted to a deconfliction system by one law enforcement party matches the same data submitted by one or more law enforcement parties.

Match - See conflict. These terms are used interchangeably.

Nationwide Deconfliction Pointer Solution (NDPS) - A target, investigative data, and event deconfliction pointer system that interfaces with existing event, target and investigative data systems to determine whether any participating agency has an interest in the same event, or investigative target and investigative data. When a match occurs, NDPS provides select information to the agents and officers who own the information that caused the match. The NDPS is composed of two parts:

I. ***Partner Deconfliction Interface (PDI)*** - The technology that enables the interface of three nationally recognized event deconfliction systems: Case Explorer, RISSafe, and SAFETNet. This technology supports:

   a. ***Event deconfliction*** - The process of determining when law enforcement personnel are conducting an event in close proximity to one another at the same time. Events include law enforcement actions such as raids, undercover operations, surveillance, or executing search warrants. When certain elements (e.g., time, date, and location) are matched between two or more events, a conflict results. Immediate notification is then made to the affected agencies or personnel regarding the identified conflict.

2. ***Target/Investigative Data Deconfliction Platform*** - The technology hosted and managed by EPIC, with participation from partner systems enables the interface of target and investigative data systems used for determining when law enforcement personnel are conducting an investigation focused on the same target or have an interest in the same investigative data. When a conflict occurs, immediate notification is then made to the affected agencies or personnel regarding the identified conflict. This technology supports:

a. ***Active/Open Investigative Target Deconfliction*** - For purposes of deconfliction, an active/open target will meet the following criteria: the agency is actively investigating the target; there is reasonable suspicion that criminal activity has occurred or is occurring; the agency has assigned a case number; and the agency anticipates an arrest and prosecution or is submitting criminal intelligence in support of an active investigation.

b. ***Investigative Data Deconfliction*** - The process of determining when law enforcement personnel are conducting an investigation that involves the same investigative data. When investigative elements match, immediate notification is then made to the affected agencies or personnel regarding the identified conflict.

SAFETNet
(User Agreement Form)

NAME: _____
LAST FIRST

EMPLOYING AGENCY:_____Agency ORI: _____

AGENCY DIVISION or HIDTA GROUP(TASK FORCE): _____

OFFICE ADDRESS: _____
STREET CITY STATE ZIP

WORK PHONE:_____CELL PHONE: _____

CELL PHONE PROVIDER:_____SSN: ### - ## - _____
(AT&T, Verizon, Sprint, etc.) (Last 4 digits only)

DEP'T. EMAIL ADDRESS:_____

I understand that the utilization of this application is for my safety and security, as well as the safety and security of other users. I agree to protect the security and integrity of the system. Any illegal use of this system will be grounds for immediate termination of privileges.

AGENT'S SIGNATURE:_____DATE:_/_/____

PRINT SUPERVISOR'S NAME: _____

SUPERVISOR'S SIGNATURE:_____DATE:____/____/____

RETURN TO: Gulf Coast HIDTA
3838 N. Causeway Blvd., Suite 1900
Metairie, Louisiana 70002
(571) 362-4869 - Main
(571) 362-4915 - Fax

CONTACTS:

Ronnie Hoefeld	(571) 362-4881	hoefeldr@gchidta.org
Royce Pardue	(571) 362-4878	parduer@gchidta.org

FOR GC-HIDTA USE ONLY

LOGIN NAME: _____ PASSWORD: _____

AGENCY: _____

ACCESS LEVEL: User ☐ Agency User ☐ Watch Center ☐ Agency Admin ☐

Revised: 2017