Global Intelligence Working Group
Information/Intelligence Sharing System Survey

Background

In spring 2003, the Global Intelligence Working Group conducted a preliminary survey of several multistate or interstate information sharing systems/initiatives that are in place or being developed at the local, state, federal, and regional levels.

Overview

Information was reported on 22 systems/initiatives:

- Nine interstate systems
- Six state systems
- Three city or county regional systems
- Four reported but did not fit the electronic system criteria

General observations:

- Numerous systems seem to be designing their system architecture for purposes of expansion beyond initial stages to connect or interface with other systems.
- Several systems cover significant population areas, even though they are not national systems.
- Around half of the systems do not currently contain intelligence information.
- Some of the systems are messaging systems but have the possibility for electronic intelligence sharing.
- Riss.net is connecting to several of the other systems: CISAnet, HIDTA, LEIU, LEO, MATRIX, and NLETS.
- Information was obtained on most, but not all, major systems of interest (missing: JRIES [CATIC] and Joint Terrorism Task Force Information Sharing Initiative [Gateway]).

Systems/Initiatives

CDU-Houston:	Community Defense Unit − Houston, Texas, Police Department
CISAnet:	Criminal Information Sharing Alliance Network (Southwest Border States Anti-Drug Information System)
CLEAR-Chicago:	Citizen Law Enforcement Analysis and Reporting − Chicago, Illinois, area

COPLINK:	COPLINK
CriMNet-MN:	CriMNet Minnesota
EFSIAC:	Emergency Fire Services Information and Analysis Center
EPIC:	El Paso Intelligence Center
ERN-Dallas:	Emergency Response Network − Dallas, Texas, FBI
HIDTA:	High Intensity Drug Trafficking Areas
JNET-PA:	Pennsylvania Justice Network
LEIU:	Law Enforcement Intelligence Unit
LEO:	Law Enforcement Online
LETS-AL:	Law Enforcement Tactical System − Alabama
MATRIX:	Multistate Anti-Terrorism Information Exchange
NLETS:	National Law Enforcement Telecommunication System
Project North Star:	Project North Star
RAID:	Real-time Analytical Intelligence Database
riss.net:	Regional Information Sharing Systems secure intranet
SIN-OK:	State Intelligence Network − Oklahoma
SPIN-CT:	Statewide Police Intelligence Network − Connecticut
TEW Group-Los Angeles	Terrorism Early Warning Group − Los Angeles, California, area
ThreatNet-FL:	ThreatNet Florida

Summary Results

- Of the 22 systems, 14 were governed/controlled by host agencies and 12 by policy boards (there was some overlap). Policy board governance is especially popular among the larger systems.

- Sixteen of the 22 systems receive federal grants or appropriations as a source of funding for their system/initiative.

- Of the 22 systems, 8 were national in geographic service coverage, 7 regional, and 7 state/local.

- Of the 22 systems, 15 have federal agency members, 17 state members, 18 local members, and 13 other agency members.

- Seven of the 22 systems/initiatives indicated their scope of geographic access as intrastate, 12 interstate, and 3 international.

- Twelve systems have law enforcement-only agency access, and 10 law enforcement-plus access.

- Thirteen systems contain general criminal data, 11 terrorism data, 11 drug data, and 9 gang data.

- Eight systems store system data at a central location, and 14 at decentralized locations.

- Nine systems own the data in the system, and 13 report that data contributors own the data.

- Eleven systems contain intelligence data and are compliant with 28 CFR Part 23.

- Means of connectivity include the following applications: VPN, intranet, extranet secure environment, firewall, Web-based, routers, and IP encrypted. Media used for connectivity include fiber, satellite, T-1, T-3, dial-up, and fractional (T-1).

- Nearly every system described itself as a limited access system (an invited community).

- Membership vetting methods include an application process, verification, screening, background checks, user certification training requirements, sponsorship, board approval, and member agency approval.

- User authentication methods include passwords, PKI, Smartcards, tokens, key fobs, and digital certificates.