

*Global Intelligence Working Group*  
**Connectivity/Systems Committee**  
**Meeting Summary**  
San Antonio, Texas  
January 28, 2003

## **Introduction**

A Connectivity/Systems Committee daylong meeting was held to begin the process of developing recommendations for systems databases, and applications for the collection, collation, storage, analysis, evaluation, and dissemination of classified and unclassified law enforcement information, as charged by the Intelligence Working Group. Mr. Miles Matthews serves as Chairman of the committee. The following committee members were in attendance:

Mr. Miles Matthews  
*Committee Chairman*  
*Counterdrug Intelligence Executive*  
*Secretariat*

Mr. Mike Duffy  
*U.S. Department of Justice*  
*Office of the CIO*

Mr. Bill Eubanks  
*Federal Bureau of Investigation*  
*(FBI)*

Mr. Gerard Lynch  
*MAGLOCLEN*

Mr. George P. March  
*RISS Office of Information*  
*Technology*

Mr. Phil Ramer  
*Florida Department of Law*  
*Enforcement (FDLE)*

Mr. Bob Cummings and Mr. Kurt Bonhamer from the Institute for Intergovernmental Research (IIR) were also in attendance. Due to scheduling conflicts, committee members Mr. Ronald Brooks and Mr. Richard Stanek were unable to attend the meeting.

## **Discussion and Decisions**

The committee discussed the following objectives:

- Identify existing networks, systems, and applications.
- Achieve appropriate connection standards, including the following factors:

- Accessibility
  - Connectivity
  - Authentication
  - Vetting process
- Once standards are set, develop a marketing strategy to encourage existing and newly developed systems to adapt to the connectivity standards.
  - Encourage information sharing from classified systems to appropriately-cleared law enforcement members, and the “tearline” redaction (removing identification of and information on the capabilities of sources and methods) to permit sensitive but unclassified (SBU) sharing of such information.

The meeting began with Mr. Bob Cummings providing a status report of the Global Intelligence Working Group (GIWG) and details of the meeting to be held in February 2003 in San Francisco, California. The timeline for the GIWG National Intelligence Plan was also discussed. The objectives for this meeting include the identification of networks; databases at the federal, state, and local levels; collaboration tools that include e-mail, chat, and Special Interest Groups; and data visualization tools which include data mining, link analysis, and geospatial information systems.

The committee discussed various intelligence networks, systems, and applications that exist to aid criminal justice agencies. Among those mentioned were the Regional Information Sharing Systems (RISS); FBI Law Enforcement Online (LEO); National Law Enforcement Telecommunication System (NLETS); Defense Information Systems Agency Anti-Drug Network–Unclassified (ADNET-U); Department of the Treasury Financial Crimes Enforcement Network (FinCen); Drug Enforcement Administration (DEA) El Paso Intelligence Center (EPIC); Intelligence Community Open Source Information System (OSIS); the State Department’s OpenNET, including the Bureau of Consular Affairs visa database; COBIJA; the Multistate Anti-Terrorism Information Exchange (MATRIX); and various state networks. The committee members agree that RISS/LEO interconnection, its connection with OSIS/OpenNET, and its plans to connect to other SBU networks, databases, and applications are positive steps toward achieving a wider network that will be available to criminal justice agencies. The survey of existing intelligence systems that IIR is currently conducting for the GIWG and an upcoming meeting, hosted by the FBI and FDLE, were mentioned as sources for discovering what additional intelligence tools exist that may not be known by committee members. The committee expressed an interest in utilizing and leveraging existing intelligence systems and networks, in lieu of creating new networks and systems, viewing the currently interconnected systems and networks as proof that building on and improving existing capabilities can most rapidly expand collaboration and information sharing among law enforcement.

Mr. Tom Hayden and Mr. Rocky Stone gave an executive briefing of COBIJA. COBIJA (a Spanish word for “blanket”) started as a means for federal, state, and local law enforcement agencies to plan and coordinate southwest border interdiction activities with Mexico. The initiative has grown to include additional states, with statistically proven arrest and seizure results. Multijurisdictional operations are planned, with the aid of GIS-depicted seizure reports, for COBIJA operational periods.

Mr. Phil Ramer presented the MATRIX project to members of the committee. He briefed the members on the goals of MATRIX and methods being used to achieve them. The presentation included a demonstration of the data-mining capabilities currently used within the FDLE.

Following the two briefings, the meeting participants discussed classified federal information with law enforcement at all levels. Ultimately, the committee agreed that access would expand among law enforcement and other state and local government elements, but within the currently defined system of national security personnel clearances and physical and systems information. There may be a capability within RISS/LEO/OSIS that might provide a useful means of communicating law enforcement information interests from state and local perspectives to the intelligence community personnel and systems. An “EPIC model” was described where federal, state, and local agencies would access electronically, through RISS or LEO, an intelligence community site on OSIS to submit their request for particular information. A response desk established at the national level would review the request, indicate its receipt to the sender, check the intelligence community information holdings, and forward to the appropriate agency. A determination would be made on what response would be sent back to the requester. It could be in the form of an SBU response and include, as necessary, the intelligence community agency’s preparation of a “tearline” report; or, it could be in the form of a tip or lead passed through a federal enforcement agency, thereby protecting the sources and methods of classified information collection. Mr. Matthews and Mr. Eubanks agreed to speak to appropriate federal agencies to provide information on the current means by which access to classified systems is obtained and will report back to the committee.

Prior to the next committee meeting in San Francisco, the members agreed to review collaboration and data visualization tools that can be used by the interconnected systems and contact Mr. Matthews with additional tools that they believe can be employed.

Mr. Matthews indicated that he wanted to prepare a draft of the network and system aspects agreed to in the meeting and forward them to the GIWG in advance of the meeting in San Francisco. At the San Francisco meeting in February 2003, the committee is to prepare an outline of the Connectivity/Systems chapter of the National Intelligence Plan for presentation to the GIWG on the following day.