Global Intelligence Working Group
Meeting Summary

Arlington, Virginia
April 2-3, 2003

The Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) met in Arlington, Virginia, on April 3, 2003. The GIWG is one of four working groups of the Global Advisory Committee (GAC).

Chairman Melvin Carraway requested a meeting with the Committee chairpersons and staff. Attendees at the meeting included Mr. Peter Modafferi, Standards Chair; Mr. Miles Matthews, Connectivity/Systems Chair; Mr. Tom O'Connor, Training Chair; Mr. Russ Porter, Privacy Chair; Mr. Richard Stanek, Policy Chair designee; Mr. Bruce Edwards, Bureau of Justice Assistance (BJA); Mr. Don Johnson, Institute for Intergovernmental Research (IIR); Mr. Bob Cummings, IIR; Mr. Joe Peters, IIR; Mr. Doug Bodrero, IIR; Mr. Bruce Buckley, IIR; Mr. John Terry, IIR; and Ms. Diane Ragans, IIR.

Chairman Carraway provided an overview of the day's activities and outlined his expectations for the Committees. Chairman Carraway also provided information on upcoming presentations/panel discussions in which GIWG Committee members would be participating, including the Law Enforcement Intelligence Unit (LEIU) Conference in Seattle, Washington, on June 2, 2003, and the International Association of Chiefs of Police (IACP) Annual Conference in Philadelphia, Pennsylvania, on October 22, 2003.

Breakout meetings occurred for the following GIWG Committees: Connectivity/Systems, Privacy, Policy, Standards, Training, and Outreach. The Training and Outreach Committees were combined due to the unavailability of several Outreach Committee members. The Connectivity/Systems, Training, and Privacy Committees convened brief meetings on the afternoon of April 2. Documentation from those afternoon meetings is combined with the attached individual Committee meeting notes.

In an effort to forge a working relationship with local law enforcement, several U.S. Department of Homeland Security (DHS) representatives met with members and staff of the GIWG. Attendees at the meeting included Mr. Paul Redmond, Information Analysis and Infrastructure Protection (IA&IP) Assistant Secretary, DHS; Ms. Karen Morr, DHS; Mr. Neal Riddle, Fusion Branch Director, DHS; Mr. Jim Savage, U.S. Secret Service, detailed to DHS; Mr. Gregory Stieber, U.S. Secret Service, detailed to DHS; Chairman Carraway; Mr. Richard Ward, Deputy Director, Office of Justice Programs (OJP), BJA; and Mr. Bodrero, Mr. Cummings, and Mr. Terry, IIR.

Chairman Carraway provided a briefing on Global and the GIWG efforts. Mr. Redmond inquired about the feasibility of a pilot project that would interface DHS with state and local law enforcement agencies. Mr. Redmond indicated the connection should provide DHS the ability to communicate, on a nationwide level, information relating to critical infrastructures (nuclear power plants, chemical storage facilities, seaports, water treatment plants). A suggestion was made to utilize the secure Regional Information Sharing Systems (RISS) secure intranet (riss.net) as the communication network for the proposed DHS pilot project, and Mr. Redmond requested a proof of concept for this proposal. Mr. Ward agreed to work with IIR in developing a proof of concept to provide to DHS for their review and approval.

The Plenary Session occurred after the breakout committee meetings. The notes from the Plenary Session will follow the committees' meeting summaries provided below.

Standards Committee

Chairman Peter Modafferi opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Standards Committee meeting on April 3, 2003, and welcomed the members and guests. The following individuals were present:

Mr. Bob Cummings (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Peter Modafferi (Chair)
Rockland County District Attorney's Office
New City, New York

Ms. Marilynn Nolan
U.S. Drug Enforcement Administration
Arlington, Virginia

Mr. Daniel Oates
Ann Arbor Police Department
Ann Arbor, Michigan

Ms. Marilyn Peterson
New Jersey Division of Criminal Justice
Trenton, New Jersey

Ms. Diane Ragans (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Steve Raubenolt
Ohio Highway Patrol
Columbus, Ohio

Mr. Gregory Stieber
U.S. Secret Service
U.S. Department of Homeland Security
Washington, DC

Mr. Cummings provided a brief overview of the project-to-date, as well as an explanation of the planned activities for the day. Mr. Modafferi had prepared a PowerPoint presentation that contained all the issue topics and discussion points that had been prepared for the Committee's use. The recommendations and further actions required were entered into the PowerPoint as they were finalized, and Mr. Modafferi provided the presentation to the Global Intelligence Working Group (GIWG) members during the afternoon Plenary Session.

The Committee had five issues on the agenda to resolve, and Mr. Modafferi requested that the discussion begin with Issue 2.

Issue 2: *Utilizing best practices from already established standards, develop model standards for all levels of the intelligence process. Differentiate between classified and unclassified information if applicable. Areas to include are: Collection, Evaluation, Collation, Analysis, Storage/Retention, and Dissemination.*

Discussion ensued regarding the proposed changes to 28 Code of Federal Regulations (CFR) Part 23. Mr. Oates indicated he was excited about the proposed changes to 28 CFR Part 23, specifically the area dealing with changing the reasonable suspicion collection criteria to reasonable indication. If the rule is passed, officers on the street can gather small bits of information that can be entered into an intelligence database. Under the old standard, this could not be done.

As a result of the discussion that followed concerning the proposed 28 CFR Part 23 revisions, the Committee made several recommendations pertaining to Issue 2.

Recommendations:

- 28 CFR Part 23 should be the minimum standard, regardless of whether or not a system is federally funded.

- In addition to 28 CFR Part 23, the GIWG recommends that law enforcement agencies utilize the Law Enforcement Intelligence Unit's (LEIU) Criminal File Guidelines as an additional model for intelligence file maintenance.

- The GIWG must officially communicate their support and any recommended changes to 28 CFR Part 23 to the U.S. Department of Justice (DOJ) within the prescribed comment period as noted in the Federal Register.

- Additionally, the GIWG should directly communicate their support of the revised 28 CFR Part 23 to Attorney Alan Fisher, General Counsel's Office, DOJ.

Continuing the discussion, Mr. Modafferi suggested utilizing the International Association of Chiefs of Police (IACP) Criminal Intelligence Model Policy as the foundation for the National Criminal Intelligence Sharing Plan standards. It was decided the group would review the policy and suggest modifications/additions as needed. Mr. Modafferi contacted IACP to obtain their input on the GIWG utilizing the document and providing suggested changes as needed. The IACP staff indicated the document had not been updated since 9/11, and any suggested changes proposed by the GIWG could be reviewed at the upcoming National Law Enforcement Policy Center Board meeting scheduled for June 9, 2003. Subsequently, the Committee made an additional recommendation for Issue 2.

Recommendation:

- The IACP's Criminal Intelligence Model Policy, with appropriate changes included, will be the model standards for the National Criminal Intelligence Sharing Plan.

The Committee members proceeded to review the IACP Criminal Intelligence Model Policy provided by Mr. Modafferi. It was agreed that the Committee would concentrate on the policy and not the discussion papers attached to the policy document. During the Committee discussion of proposed changes to the policy, Ms. Peterson related that she thought it important that analysis be emphasized in the IACP Criminal Intelligence Model Policy. The Committee agreed, and Mr. Modafferi requested that Ms. Peterson and Ms. Nolan work independently to develop analysis standards. In addition to the recommended analysis standards, the following modifications and enhancements to the document were suggested to the following sections:

Under Section II of the Policy standard, change sentence to:

It is the policy of this agency to gather information directed toward specific individuals or organizations where there is a reasonable indication (as defined in 28 CFR Part 23, Section 23.3c) that said individuals or organizations may be planning or engaging in criminal activity.

New language added:

It is also the policy of this agency to adopt the standards of the Commission on Accreditation for Law Enforcement Agencies (CALEA) for intelligence gathering. Specifically, if an agency performs an intelligence function, procedures must be established to ensure the legality and integrity of its operations, to include:

- Procedures for ensuring information collected are limited to criminal conduct and relates to activities that prevent a threat to the community.

- Descriptions of the types or quality of information that may be included in the system.

- Methods for purging out-of-date or incorrect information.

- Procedures for the utilization of intelligence personnel and techniques.

The policy contained herein is intended to remain at all times consistent with the current language of 28 CFR Part 23, as amended.

Under Section III of the Definitions standard, add definition:

Threshold for criminal intelligence: the threshold for collecting information and producing criminal intelligence shall be the "reasonable indication" standard in 28 CFR Part 23, Section 23.3c, which reads: "reasonable indication means that an objective, factual basis for initiating an investigation exists. The standard of reasonable indication is substantially lower than probable cause. In determining if there is reasonable indication of criminal activity, a law enforcement officer may take into account any facts or circumstances that a prudent investigator would consider. The standard, however, requires specific facts or circumstances indicating a past, current, or future violation; a mere hunch is insufficient."

Under Section IV, part A, of the Procedures standard, change sentence to:

It is the mission of the intelligence function to gather information from all sources in a manner consistent with the law and to analyze that information to provide tactical and/or strategic intelligence on the existence, identities, and capabilities of criminal suspects and enterprises, generally, and, in particular, to further crime prevention and enforcement objectives/priorities identified by this agency.

Under Section IV, part C, of the Professional standard, change sentences to:

1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable indication (as defined in 28 CFR Part 23, Section 23.3c) that specific individuals or organizations may be planning or engaging in criminal activity.

2. Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

Add proposed new section:

Section I. Analysis

1. Where possible, agencies involved in the intelligence function should establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value.

2. Where possible, the above-described process should be accomplished by professional, trained analysts.

Move this clause from Section IV and amend:

3. Analytic material (i.e., intelligence) shall be compiled and provided to authorize recipients as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals emerge.

<u>Issue 3</u>: *Develop a set of standards for management of an intelligence unit.*

The IACP *Criminal Intelligence Sharing Report* specifically recommends that local and state law enforcement chief executives should adopt standards for managing an intelligence unit and, more basically, intelligence data. The Committee discussed standards for management of an intelligence unit and made several recommendations for the GIWG to adopt for the Plan.

Recommendations:

- The chief executive officer of an agency should implement a mission statement for the intelligence process within the agency.

- An agency with an intelligence unit should define management and supervision of the intelligence function.

- The management of an intelligence function should implement a policies and procedures manual.

- The management of an intelligence unit should select qualified personnel for assignment to the unit.

- The management of an intelligence operations program should ensure appropriate training for all personnel assigned to or impacted by the intelligence process.

- Agency chief executive officers and management of intelligence units should promote sharing and coordination of criminal information between law enforcement agencies at all levels of government.

- The management of an intelligence unit should implement an appropriate audit or review process to ensure compliance with policies and standards.

- The agency chief executive officer should ensure standards are developed concerning backgrounds of staff/system users, ensuring security (of the system, facilities, etc.) and access to the system/network.

Issue 4: *Identify recommended core data elements to include in participating systems.*

Recommendation: Refer this topic to the Connectivity/Systems Committee for further discussion.

Issue 5: *Review the list of definitions and identify additional terms to be defined.*

The Committee approved the list of definitions, as presented, and recommended the addition of a single term.

Recommendation: Add the term "reasonable indication" to the glossary and use the definition provided in 28 CFR Part 23.

Issue 1: *Develop a policy regarding the institutionalization of standards in the intelligence community. This policy should address why this is important and how it relates to the officer on the street, as well as all other levels of law enforcement affected by this plan.*

As indicated in the IACP *Criminal Intelligence Sharing Report*, local, state, and tribal law enforcement agencies must move aggressively toward implementation of intelligence-led policing. Committee discussions centered on the importance of this policy, as well as how to ensure consistent implementation. Several recommendations were suggested as a result.

Recommendations:

- Chief executives should adopt standards for managing intelligence data.

- Chief executives of larger departments should designate a member to function as the chief/manager of the intelligence function.

- Chief executives of smaller agencies should ensure all appropriate staff are cross-trained in the intelligence mission.

- Chief executives should seek ways to share intelligence resources.

- Proposed policy: All criminal justice agencies should develop and share intelligence in order to prevent crime and enhance homeland security. To accomplish this, they should embrace the philosophy of intelligence-led policing and implement the National Intelligence Plan,[1] using all available resources.

- Once the GIWG establishes model standards, policies, and procedures, the GIWG should evolve into a "National Intelligence Council" as contemplated in the IACP *Criminal Intelligence Sharing Report*. The GIWG should serve as a true advisory council to the Attorney General, the Secretary of the U.S. Department of Homeland Security (DHS) and state governors, and provide a critical voice for local, state, and federal law enforcement. Its mandate should be to review standards, policies, training, and technology, to make recommendations to the Attorney General, the Secretary of DHS, and state governors, and to provide incentives to criminal justice agencies that support the National Intelligence Plan.

- Membership in the National Intelligence Council shall be composed of:

  - Sworn state and local law enforcement executives;

  - Executives of federal law enforcement agencies with criminal investigative authority; and

  - Executives of government agencies with policymaking responsibility or law enforcement program oversight.

- The National Intelligence Council must be funded by the federal government and have appropriate administrative support.

- It shall be a high priority of the National Intelligence Council to address the problem of access to classified information when its disclosure is essential for local law enforcement to ensure homeland security.

[1] During the closing remarks of the Plenary Session, the GIWG recommended that the Plan's title be changed to the National *Criminal* Intelligence *Sharing* Plan.

Mr. Modafferi thanked the attendees for their active participation and adjourned the meeting.

Connectivity/Systems Committee

Chairman Miles Matthews opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Connectivity/Systems Committee meetings on April 2-3, 2003 and welcomed the attendees.

The following individuals were present on April 2, 2003:

Mr. Bob Cummings (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Ms. Patty Dobbs (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Michael Duffy
Justice Management Division
Washington, DC

Mr. George March
Regional Information Sharing Systems
Office of Information Technology
Thorndale, Pennsylvania

Mr. Miles Matthews (Chair)
Counterdrug Intelligence Executive Secretariat
Washington, DC

Mr. Kent Mawyer
Texas Department of Public Safety
Austin, Texas

Mr. Joe Peters
Institute for Intergovernmental Research
Tallahassee, Florida

Ms. Diane Ragans
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Philip Ramer
Florida Department of Law Enforcement
Tallahassee, Florida

Mr. David Walchak
Federal Bureau of Investigation
Clarksburg, West Virginia

The following individuals were present on April 3, 2003:

Ms. Patty Dobbs (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Steven Hooks
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. William Luechkenhoff
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. Allyn Lynd
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. George March
Regional Information Sharing Systems
Office of Information Technology
Thorndale, Pennsylvania

Mr. Steve McCraw
Federal Bureau of Investigation
Washington, DC

Mr. Kent Mawyer
Texas Department of Public Safety
Austin, Texas

Mr. Joe Peters (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Philip Ramer
Florida Department of Law Enforcement
Tallahassee, Florida

Ms. Lynn Starling
Federal Bureau of Investigation
Washington, DC

Mr. David Walchak
Federal Bureau of Investigation
Clarksburg, West Virginia

Chairman Matthews began the meeting by asking participants if they had seen the Memorandum of Understanding signed by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) to the U.S. Department of Homeland Security (DHS), which provides a framework and guidance governing the sharing, use, and handling of information between the above agencies. The document is attached as *Appendix A*.

Mr. Cummings stated that Mr. Bill Casey of the Boston Police Department had told him about a new system originated in Chicago, known as Citizen Law Enforcement Analysis and Reporting (CLEAR). The system seeks to connect eight major cities to share information. Mr. Cummings suggested official contact be made with the system, so both groups could become more aware of their efforts.

Mr. Ramer and Mr. Mawyer stated that they had been approached to take part in a briefing on an effort out of the California Attorney General's Office, Bureau of Law Enforcement; New York Police Department; and the Defense Intelligence Agency (DIA). A pilot project is underway between the two jurisdictions and DIA to access armed forces information.

Chairman Matthews proceeded to move through the issues on the agenda and asked if the group was in agreement that the survey recap report should be appended to the final report. The group agreed to Issue 2, *Review further information obtained from the survey of existing intelligence systems/initiatives.*

<u>Issue 1</u>: *Describe the recommended network for the National Intelligence Sharing Plan. Develop a recommendation for how the national network should be structured.*

Chairman Matthews stated that he believed RISS/LEO was the defacto standard for connectivity. Mr. Duffy stated that there should be a minimum security standard. There was a general discussion regarding the differences between riss.net and the Criminal Information Sharing Alliance (CISA), formerly known as the Southwest Border States Anti-Drug Information System. Mr. March and Mr. Mawyer stated that the end repository establishes their access requirements and that the intranet can carry all sorts of information. The basic differences are in the type of security, individual v. group authentication, and how e-mail is encrypted. Mr. March suggested a key box concept as a way for existing systems to share information now. A user would come into their system and be authenticated. If they wanted to move to another system, they would go into a key box, which would be able to recognize the user systems' authentication and then allow or not allow them to enter the new system. Mr. March stated that this solution is feasible now and not cost prohibited. Mr. Mawyer was supportive of the idea provided the keys were mutually acceptable. Mr. Matthews asked Mr. March to submit a paragraph describing the concept. The key box concept does not address additional information/services that might be available from a resource or difference in the type of e-mail encryption, only the inquiry process.

On the topic paper titled Connect issue 1, provided as a working document for the Committee, the last sentence should be modified to read: Riss.net and LEO would serve as the nationwide network, and the LEO system would serve as the federal connection for information flowing to the states and locals. The following paragraph from Mr. March should also be added: Resources should be dedicated to establishing a means of recognizing and accepting various access control and individual authentication methods as being acceptable methods of access to the national network, as well as the information resources accessible on the network, and that of the various participating systems. For instance, system administrators must be able to choose from an 'approved' set of network and system access control methods in order to meet their all-inclusive needs, and all control methods chosen from the approved set must be capable of recognizing another and providing access throughout the national network, as if a single access method has been required.

Recommendation: Existing systems should be used to leverage information sharing. Riss.net and LEO are the core backbone. The standard should be a Web-enabled and an Internet-based system, which authenticate to individual users. There should be a control and access cross-certification process. A minimum encryption level should be established, and encrypted e-mail should be available. A key box compatibility of different authentication methods should be developed.

Issue 3: *Develop proposed policies for all appropriate areas relating to systems, security, networks, and their connections.*

Mr. March suggested using the same adoption method that Global has already used for security measures as a way to issue a standard on control and access. Mr. Duffy stated that control and access policies should be set at a minimum. He also suggested that policies be vetted prior to adoption.

Mr. Walchak then referred to Issue 6 on the agenda, regarding the proposed "trusted committee." He suggested using the Criminal Justice Information Services (CJIS) model where the board advises and the director makes the decision. Mr. Matthews voiced some concern over the use of the 'governing body' and suggested it be a technology standards definition board. Mr. Duffy suggested the Federal Bridge Authority as a model. The authority is made up of key players from the field and those certified to build bridges. Each is considered a voting member of the authority. New members, once they are voted in, are given a seat on the authority. The authority has a basic set of standards. Any proposed new standard must receive a two-thirds vote of the authority.

Issue 4: *Develop recommended standards for all appropriate areas relating to connectivity/systems.*

The Committee felt that this issue was subsumed into Issues 1 and 3.

Issue 5: *Develop a recommendation on the types/levels of background to conduct on system/network users.*

Mr. Matthews opened up the discussion by asking what the vetting process should be for user access. Mr. Ramer stated that a background check should include a name and fingerprint-based criminal record check, but should not include field interviews. He suggested including credit checks on those persons requesting access to terrorism information. He also stated that the background check should have to be updated. Mr. March stated that RISS required the agency to pass muster (a rumor test) and present their request for access on agency letterhead. The identified access officer would have to be in good standing with the agency. Mr. Walchak stated that the LEO vetting process was also at the agency level with telephone verification. Mr. Cummings suggested that the agency should be the trusted environment. Mr. Mawyer stated that CISA vetting is done through a first-line supervisor certifying the individual user is acceptable to be in the system. Texas, for example, does have a state law requiring background investigations at the time of hiring. The task forces in Texas run a print check on members. Mr. Mawyer stated that the requested access/dissemination levels play into the mix. Mr. March stated that the problem is defining all scenarios; it is not just access to network, but also access to resources. Mr. Matthews stated that the Open Source Information System (OSIS) has indicated that if you are a RISS or LEO member, then you are clear to access OSIS.

The discussion moved on to what happens to a user when they have a criminal history record. Mr. Cummings asked if a standard needed to be set for what type of record was acceptable, or whether or not it went back to the agency. Mr. March asked if setting such a standard raised any legal issues or set up a need for an appeal process. Mr. Walchak stated that the FBI would not pass any individual for their hiring process who had any felonies or repeat misdemeanors.

Recommendation: For law enforcement system users, a sworn officer, agent, or civilian analyst, a minimum standard for access should be the same as the sworn law enforcement officer requirements set by the state, so long as, at a minimum, it requires FBI and state fingerprint-based records check. Further, the records check must have been completed within the previous three years (this last portion was added on April 3, 2003, when the Committee was discussing their chapter outline).

Mr. Matthews adjourned the Committee meeting.

April 3, 2003

Mr. Matthews welcomed the Committee members and guests. He requested Mr. Ramer to give a brief overview of the Multistate Anti-Terrorism Information Exchange (MATRIX) project. Following Mr. Ramer's briefing, Mr. Matthews introduced Mr. Steven Hooks of the FBI CJIS unit, to brief the Committee on a new project.

Mr. Hooks explained that CJIS had been working to automate the Uniform Crime Report (UCR) program towards a national indices program to include data mining and research. He introduced Mr. Lueckenhoff, the new program manager for this effort. The CJIS unit is launching a new System of Services (SOS), described as an information sharing concept. Mr. Lueckenhoff described it as a fusion of all the services that CJIS offers. Basically, the system would be capable of looking for interrelationships between incidents at the local, state, and federal levels. The system would create national indices using local and state incident reports and federal case openings. The system would be able to reach into a variety of existing databases to look for connections with the inquiry. The CJIS unit is currently managing an incident reporting database (local, state, and federal); the Interstate Identification Index that houses criminal history record files; the National Crime Information Center (NCIC) that contains numerous files such as wanted persons, deported felons, stolen vehicles, Violent Gang and Terrorist Organizations File (many of these searches are currently done off-line on a request basis); CJIS Wide Area Network (WAN), which provides connections to NCIC, the Integrated Automated Fingerprint Identification System, the Combined DNA Index System (CODIS), and Ballistics; and the National Instant Check System (NICS) Index that contains persons denied gun permits. In addition, CJIS envisions being able to access the Joint Agency Booking System (federal bookings); National Drug Pointer Index; Joint Terrorism Task Forces; and sensitive but unclassified information from the Terrorist Threat Integration Center. The SOS does not store any of the information in a single database. Rather, it reaches out to existing sources and looks for a match/trend/string of data elements on the inquiry. It seeks to correlate and link information together. The search would be done on near or real-time basis and provide a point back to where the structured data is located. Fifty-three National Incident Based Reporting System (NIBRS) elements are currently being piloted. The PowerPoint presentation provided by CJIS is attached as *Appendix B*.

Mr. McCraw stated that the classified data should be stripped of method and source so the names and numbers could be mined for local and state crimes. He stated that he did not see this SOS as duplicative of other efforts. Mr. Matthews asked how this SOS would integrate with existing pointer systems. Mr. Reid stated that CJIS WAN is already utilizing RISS/LEO/National Law Enforcement Telecommunication System (NLETS). Mr. Reid stated that a contract had been made with Lockheed Martin to do the detailed system design. Mr. McCraw stated that he could see that the SOS would be seen as competitive with other systems. Mr. Ramer expressed his concern that state and local law enforcement really need to be given more access to classified and unclassified data, and that any such system needs to include access to Bureau of Citizenship and Immigration Services information. Mr. Matthews thanked the CJIS unit for their presentation and input and continued with the issues on the agenda.

<u>Issue 6</u>: *Discuss recommended activities for the proposed "trusted committee" that will govern the national network.*

Mr. Matthews stated that there had been some discussion about using a Federal Advisory Committee Act (FACA) compliant committee to oversee the RISS/LEO efforts. Mr. March stated that misuse of the network and information had to be an issue addressed by this Committee. Mr. Matthews stated that General Counterdrug Intelligence Plan would be a forum for receiving issues. Mr. March suggested that the national intelligence plan is in itself a minimum standard. Mr. Mawyer stated that the Committee needed to make an assumption that there will be a group that serves as this "trusted committee." Mr. Ramer reminded the committee that the IACP Summit Report calls for a coordinating body. Mr. Matthews stated that it should be a consensus body that advised policy and resolves disputes, and part of that effort would be to vet memberships and technology issues. It would be appointed under the auspice of Global to develop standards and policies.

Recommendation: The Global Advisory Committee (GAC) should appoint an advisory board that provides coordination and consensus on intelligence and information sharing policies and procedures. The advisory board should incorporate Global's Security Working Group report and recommendations. The board should recommend system connectivity standards as technology evolves.

Issue 7: *Identify and describe the types of analytical products available. Determine how to maintain a current listing.*

Mr. Mawyer stated that individual products should not be listed but, rather, what the products should support. Mr. Matthews stated that there were categories of products—open source, crime information, trend analysis, data visualization, Extensible Markup Language (XML) standards, link analysis, Geographic Information System mapping. Mr. Ramer stated that a standard set of tools should be identified in order to be able to connect to the sources and use the data. Mr. March stated that this should be created as a resource of what others are using and what is out there. Mr. Matthews stated that one possibility might be to share tools among a group, offered by the resource that has the data.

Recommendation: The Committee recommended identifying categories of analytical products: criminal information/intelligence, open sources, pointer information, finished intelligence/products, and visualization/analytical tools. A standard "tool set" would need to be defined.

Issue 8: *Recommend a Committee position regarding classified data.*

Mr. Matthews stated that background investigations for access to classified data are necessary, but they ought to be expedited and prioritized for state and local law enforcement so clearances can be completed in a timely manner. Mr. March stated that the issue with classified information is the method and source of the information, not the information itself. Mr. Mawyer stated that it is how the information is pushed out into the field that is of concern. Mr. Ramer stated that the entity performing the backgrounds should be encouraged to complete them in a timely manner, as the Attorney General said in his remarks to the GAC earlier that day. Mr. March stated that the resources to conduct the full background investigations required are not there but need to be. Mr. Ramer asked if the DOJ and the U.S. Department of Defense (DOD) recognized each other's clearances. He related that Florida has experienced problems with their National Guard counterparts and sharing information with those law enforcement personnel who do have DOJ clearances, but not DOD clearances. Mr. Ramer also asked that the report include a table of what the clearances are and what they mean, to help others determine a classification matrix.

Recommendation: The Committee recommended that the clearances for state and local law enforcement be expedited and the necessary resources be provided.

Issue 9: *Identify recommended core data elements.*

Mr. Mawyer suggested organizations, groups, and businesses should be the core data elements. Mr. Hooks and Mr. Reid informed that their new CJIS SOS has 53 data elements available. Mr. Matthews stated that there needed to be enough elements to differentiate between individuals. Mr. Hooks said they were using elements such as, race, use of gun, weather conditions, and proximity to other locations. Mr. March stated that the reconciled XML standards should be considered. He also stated that there was a difference between the minimum needed to search and standard data elements. RISS only needs the name, while Florida needs name, sex, race, and date of birth.

The Committee did not make a specific recommendation other than they would like to review elements from RISS, Florida, and Texas.

Issue 10: *Review definitions and identify additional terms to be defined.*

Mr. Matthews asked the Committee to review the list and provide any additional suggestions before the next meeting. He subsequently adjourned the meeting.

Training Committee

Chairman Thomas O'Connor opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Training Committee meeting on April 3, 2003, and welcomed the Committee members and observers. The following individuals were in attendance:

Mr. Donald J. Brackman
National White Collar Crime Center
Richmond, Virginia

Ms. June Hill (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Ritchie A. Martinez
Arizona Department of Public Safety/ HIDTA
Tucson, Arizona

Mr. Jerry Marynik
California Department of Justice
Sacramento, California

Mr. Thomas O'Connor (Chair)
Maryland Heights Police Department
Maryland Heights, Missouri

Ms. Marilyn B. Peterson
New Jersey Division of Criminal Justice
Trenton, New Jersey

Mr. John Terry (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

The following observers were in attendance:

Mr. William Berger
North Miami Beach Police Department
North Miami Beach, Florida

Ms. Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia

Mr. Richard Randall
Kendall County Sheriff's Office
Yorkville, Illinois

Ms. Pat Thackston
Institute for Intergovernmental Research
Tallahassee, Florida

Chairman O'Connor briefly reviewed the work accomplished by the Training Committee to date, including a draft report titled *Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies* that addresses items that the Committee was tasked with resolving.

Chairman O'Connor outlined the primary tasks to be accomplished during this meeting: finalizing the draft report and preparing a plan that contains specifics regarding how the training plan will be implemented and institutionalized. Items to be considered for the implementation plan include funding sources, specific delivery mechanisms, and a timeline for delivery. Due to time constraints, it was agreed that the Committee would focus primarily on the development of a training model with proposed minimum training standards for all levels of personnel affected by the intelligence sharing plan.

Chairman O'Connor explained that a portion of the meeting time would be allocated for discussion with the Outreach Committee and other agenda items would be discussed, if time permits.

There was a brief discussion regarding training standards versus training policies, and the accreditation of law enforcement training courses by the Commission on Accreditation for Law Enforcement Agencies (CALEA).

The Committee discussed the title of the *Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies*, and Mr. Martinez suggested that it should be titled *"Criminal Intelligence Training Standards….."* in order to make it clear that the intelligence being shared is specific to criminal activity. Chairman O'Connor advised that this matter was discussed at a meeting held the previous evening. It was agreed that the title should be consistent with the Global Justice Information Sharing Initiative (Global) and should have a marketable appeal. Mr. Martinez will address this matter at the Plenary Session.

The Committee proceeded to develop the training models for five levels of law enforcement personnel: law enforcement officer, executives, managers, intelligence officers, and analysts. It was agreed that each model should identify course objectives and outcomes, course curriculum, and recommended hours. The models must be a seamless product that connects to the whole National Intelligence Plan.[2]

Training Models

Level 1 - Law Enforcement (LE) Officers, Two-Hour Course

Four objectives were identified as necessary components for the LE Officer training model.

I. LE will understand the criminal intelligence process and its ability to enhance their contributions to the criminal justice system.

Discussion:

- LE officers are being asked to be involved; therefore, they must understand they are part of the process, that the intelligence sharing system exists, and know how to use it.

- When teaching a model, basic concepts are enough; it is not necessary to introduce specifics of the Regional Information Sharing Systems (RISS).

- Officers should have an introduction to all of the intelligence sharing/systems that are going to be available.

- Intelligence sharing should be seen as a job enhancement, not an interference or additional job responsibility.

[2] During the closing remarks of the Plenary Session, the GIWG recommended that the Plan's title be changed to the National *Criminal* Intelligence *Sharing* Plan.

- Training should teach officers to recognize information that should be collected and passed on to others; they must heighten their awareness; they should see themselves as the collectors and disseminators of intelligence information.

- It is possible that, if an officer sees a person acting unusual, he or she may not even know the appropriate LE to contact.

- The whole concept of justice information sharing is being enlarged and promoted.

II. LE will be provided with information on available data systems, networks, and resources.

Discussion:

- Variety of handouts should be distributed.

- The GIWG needs to know what information exists and develop a comprehensive list to share (including Internet Web sites).

III. LE will be able to identify key signs of criminal activity and procedures for collecting data on and reporting such activity.

Discussion:

- Teach LE to identify various types of indicators of criminal activity and information that could be used and passed on to different levels of LE. They may have additional information that seems inconsequential to their case, but that may be valuable in identifying other criminal activity.

- Teach the collection of certain types of information.

- Officers must recognize that criminal intelligence gathering is a long-term process.

IV. LE will gain an understanding of the legal and ethical limitations placed on the collection of criminal intelligence information.

Discussion:

- The model must have an ethical component that passes the integrity test.

- Examples of profiling should be included.

- Officers must be made aware of and learn to recognize privacy issues in regard to criminal intelligence gathering/sharing.

Level 2 – Executives, Four-Hour Course

Four objectives were identified as necessary components for the Executive Law Enforcement training model.

I. Executives will understand the criminal intelligence process and the role it plays in enhancing public safety.

Discussion:

- Must answer several questions for the Executive: why it is necessary to do criminal intelligence policing, what will LE get out of it, what value does it has, and what requirements are expected of LE.

- Address the executive mindset and philosophy that flows down through the organization and is used as the framework in policing-led environments.

- Include a component that assists in understanding the different systems that help do the job.

- Share information through all LE levels.

- The National Intelligence Plan brochure could be used as a teaching guideline/tool.

II. Executives will understand the philosophy of intelligence-led policing and their role in the National Intelligence Plan.

Discussion:

- Executives play a key role in assuring that other levels of LE will actively participate in criminal intelligence gathering/sharing by promoting the concept.

- The training model and National Intelligence Plan must capture the interest of the executive; it must broaden the executive's perspective of intelligence gathering/sharing.

- Executives must adopt a philosophy that moves LE away from the traditional process that has occurred, understand the value of intelligence-led policing, and through their leadership skills; enlist LE at other levels to do the same. Other levels will not embrace this plan unless the executives embrace it.

- Executives will want to know what they need to do, and how to do business using this plan.

III. Executives will understand the legal framework of criminal intelligence.

IV. Executives will be provided with information on existing criminal information sharing networks and resources available in support of their agencies.

Level 3 – Managers, Three-Day Course

Seven areas were identified as necessary components for the Manager Law Enforcement training model:

I. Managers will understand the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety.

II. Managers will be provided with information on training, evaluating, and assessing an effective criminal intelligence function.

III. Managers will understand the unique issues of a criminal intelligence unit, including personnel selection, ethics, developing policies and procedures, and marketing intelligence products.

IV. Managers will understand the principles and practices of handling sensitive information, informant policies, and corruption prevention and recognition.

V. Managers will understand the legal issues surrounding the criminal intelligence environment.

VI. Managers will understand the processes necessary to produce tactical and strategic intelligence products.

VII. Managers will be provided with information on criminal information sharing systems, networks, and resources available to their agencies.

Level 4 – Intelligence Officers, One-Week Course

Seven areas were identified as necessary components for the Intelligence Officer (IO) Law Enforcement training model:

I. IO will understand the criminal intelligence process and their critical role in the process.

II. IO will understand the legal issues surrounding criminal intelligence and their liability as intelligence information collectors.

III. IO will be provided with information about the Internet, information sharing systems, networks, and other sources of information.

IV. IO will gain an understanding of the proper handling of criminal intelligence information including file management and information evaluation.

V. IO will understand the processes of developing tactical and strategic products, and experience the development of some products.

VI. IO will experience the development of criminal intelligence from information through the critical thinking/inference development process.

VII. IO will understand the tasks of building and implementing collection plans.

Level 5 – Analyst, One-Week Course

Due to time constraints, discussion of this level was postponed until the next meeting of the Training Committee.

Funding and Implementation

The Committee addressed the issue of funding sources for providing training to law enforcement agencies. General and necessary expenses relating to course materials and training were discussed. It was agreed that if there is a national standard for the training, there should be standard materials available for the courses. It was suggested that staff might develop cost estimates for the national training course after more course specifics and material needs are identified. The need for a train-the-trainer component in order to increase the numbers of law enforcement personnel that can be trained was discussed, as well as a way to deliver the train-the-trainer training. Various types of training venues (i.e., state and national conferences, local and regional LE workshops) were suggested.

The Committee agreed that grant monies were the most appropriate and accessible form of funding. Possible sources identified: U.S. Department of Defense, U.S. Department of Homeland Security (training funds are going to states for training, mostly for first responders, but law enforcement is included), and the U.S. Department of Justice through the Bureau of Justice Assistance. An estimated $10 million to $15 million could be requested to fund the training program and then distributed through the grant process to law enforcement agencies and/or trainers. For the purpose of funding, a priority order ranking of trainees was developed: Train-the-Trainers, Executives, Managers (including Supervisors and Commanders), Officers (patrol), Intelligence Officers, and Analysts.

Draft Plan

Chairman O'Connor advised that work would continue on the draft plan that will contain specifics regarding how the training plan will be implemented and institutionalized.

Conclusion

Prior to adjourning the meeting, Chairman O’Connor thanked participants for their time and efforts in completing a large portion of the tasks assigned to the Committee. Recommendations from the Training Committee will be presented at the Plenary Session, and each member will receive a summary of the Training Committee meeting.

Policy Committee

Mr. Richard Stanek opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Policy Committee meeting on April 3, 2003, and welcomed the attendees. Chairman Frazier joined the meeting mid-morning. Mr. Stanek agreed to chair the Committee meeting until Mr. Frazier's arrival. The following individuals were present for the meeting:

Ms. Viola Bodrero (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Max Fratoddi
Federal Bureau of Investigation
Washington, DC

Mr. Thomas Frazier (Chair)
Major Cities Chiefs Association
Baltimore, Maryland

Mr. Dennis Garrett
Arizona Department of Public Safety
Phoenix, Arizona

Mr. Don Johnson (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Edward Reina
Yavapai-Prescott Tribal Police Department
Prescott, Arizona

Mr. Richard Stanek
Minnesota Department of Public Safety
Minneapolis, Minnesota

The group discussed the issues/topics as identified on the Committee agenda. The Committee members suggested these issues, recommendations, and action items be provided to all Committee members, including those who did not attend. They recommended a conference call with all members after each has had an opportunity to review the minutes.

Issue 1: *Propose a policy addressing the utilization of existing, proven systems and networks for intelligence sharing. Access to the network should be done electronically, using Extensible Markup Language (XML) standards if possible.*

Recommendations:

- Utilization of Regional Information Sharing Systems (RISS)/Law Enforcement Online (LEO)
- Use of XML
- Nationally agreed upon definition of intelligence vs. information sharing:
    - Intelligence is information that is analyzed; national intelligence model involves all criminal program information, not just terrorism (from International Association of Chiefs of Police [IACP] Summit Report 2002).

- All participating agencies conform to 28 Code of Federal Regulations (CFR) Part 23

Action Items:

- Create financial incentive to allow local, state, and tribal agencies to hook into system.
- U.S. Department of Homeland Security (DHS) and/or the U.S. Department of Justice (DOJ) channel money to make this happen.
- DHS requires update from states on their intelligence sharing as part of the states' emergency preparedness plans.

Discussion:

Mr. Garrett stated the RISS/LEO system should be the backbone of intelligence sharing. He also noted system compatibility is an issue and where systems are not compatible, XML should be used to ensure communications. He noted a recent Multistate Anti-Terrorism Information Exchange (MATRIX) demonstration as a significant source of information.

Mr. Reina stated that some tribal law enforcement agencies have small systems; however, the information is not shared. He also noted that tribal agencies do not have access to National Criminal Information Center (NCIC). Mr. Johnson stated that some tribal agencies have access to NCIC, but not all. The fee imposed to access NCIC is a drawback for some tribal agencies with very limited funds. Mr. Reina also stated that approximately five states do not recognize tribal law enforcement agencies, and as a result, will not share information with the tribal agencies.

The meeting participants agreed that a positive carrot-stick approach should be taken to provide incentives for agencies to participate. Mr. Stanek noted that Minnesota, and possibly other states, may have laws prohibiting intelligence sharing. Mr. Johnson added that as state governors and legislators understand the capabilities of MATRIX, they should be willing to participate.

Issue 2: *Identify barriers to intelligence sharing, as well as recommendations for resolving them.*

Recommendations:

- Adopt a policy statement that all agencies participate; the state is the hub, following the NCIC set up.
- Utilize a subcommittee to identify and study barriers and to forward the results and suggestions back to the Policy Committee to identify legal changes.
- Utilize RISS/LEO to disseminate information.

- Draft model legislation for states to adopt to share intelligence information which would create a state statutory requirement to comply with 28 CFR Part 23.

- Include tribal law enforcement agencies; "tribal" should be added to language of 28 CFR Part 23.

- Resources should be provided to agencies without equipment to connect to RISS/LEO.

Action Items:

- Address communication, information sharing, technology, intelligence standards, policies, analysis, relationships, etc.

- Identify issues of tribal law enforcement agencies ability to access and disseminate.

Discussion:

A suggestion was made to ask staff to draft model legislation to establish information sharing among states. Another comment suggested utilizing the National Conference of State Legislators to identify what states' needs are on this issue.

The group members discussed the current lack of a centralized unit. They noted the state police agency is generally the hub for cities and counties. The tribal law enforcement issues (noted in Issue 1) were again discussed. Mr. Reina noted that where tribal officers are not recognized, the county law enforcement agency provides services.

A comment was made that not only should all agencies participate in the national model, but in a state system as well.

Issue 3: *Develop policies covering the following areas:*

- *Collection of information – prior Committee discussion centered on preventing collection abuse*

- *Use of information – to ensure accountability*

- *Dissemination of information – prior Committee discussion centered on release to the public*

- *Quality of data*

- *Ownership of data*

Recommendations:

- Information collected conforms to 28 CFR Part 23
- Pointer System
- Data Warehouse
- Analytics
- Create a national model for public sharing information and intelligence sharing

Action Items:

- Determine that update on 28 CFR Part 23 allows for the sharing of information between local, state, tribal, and federal interests.
- Define the differences for disseminating criminal justice information vs. criminal intelligence information – right-to-know; need-to-know.

Discussion:

A comment was made that ownership of data entered onto a shared system should be owned by the agency that entered it and the maintenance of the data should be performed by the owner agency. Also noted was that RISS utilizes a pointer system for information that an analyst does not want everyone to see. Such pointer systems are generally for officer safety information, but the quality of information may be an issue. Another participant stated that if the information is input into a general index it may be okay; however, the future use of that information is a concern.

Mr. Garrett stated that the difference between criminal justice information and criminal investigation information should be the subject of discussion. He noted that a policy should be written to allow sharing of criminal investigative information and should be for general use, not just terrorism.

Issue 4: *Recommend methods to validate that policies and standards are being met (in order to ensure accountability and reduce liability). Possible mechanisms to utilize:*

- *Compliance audits*
- *Surveys/Questionnaires*
- *System/network/facility security tests*
- *Accreditation standards*

Recommendations:

- Establish a policies and standards oversight entity with staff support and funding; utilize a local, state, tribal, or federal chair.
- Policy/Trust Committee reports to include the best practices and systemic issues and/or problems.
- Create national plan, not federal plan.

Action Item(s):

(None identified)

Discussion:

The meeting participants suggested forming a permanent board formed under Global, consisting of directors of major intelligence networks with representatives of major agencies involved in intelligence (e.g., IACP, DHS, and the Federal Bureau of Investigation [FBI]). Additionally, they discussed the concept of a "trusted committee" that would report to the permanent board. The purpose for the board and committee would be to coordinate and continue implementation of the Global Initiative.

Issue 5: *Recommend guidelines/standards for participation in the proposed "trusted committee."*

Recommendations:

- Create a policy/trusted committee that reviews technology, identifies additional standards, provides incentives to comply with standards; policy body creates a Policy and Standards Entity.
- Follow IACP recommendation for local, state, or tribal chair of group.

Action Items:

- Acts as governing body for the national network.
- Review of new systems/initiatives requesting connection to the national network in order to determine adherence to established guidelines/standards reference security, connections, data elements, or user backgrounds.
- Review of Memorandums of Understanding.
- Review of proposed systems/initiatives for avoidance of duplicity with other established systems.

- Review allegations of misuse of intelligence information and recommend sanctions

Discussion:

The meeting participants suggested the "trusted committee" *(see Issue 4)* not be a self-policing body. A suggestion was made that an advisory board may also be identified to obtain input from time to time. Such input may come from organizations such as the American Civil Liberties Union. A comment was made that such a board was used on the implementation of the Brady gun laws.

Issue 6: *In addition to training, identify the framework for implementing and ensuring the longevity of the standards-based intelligence plan. Propose mechanisms for this effort (e.g., national/state accreditation, endorsement by professional organizations, creation of a permanent committee, etc.).*

Recommendations:

- Policy/Trust Committee to lead an effort to identify a framework for implementing and ensuring the longevity of the standards-based intelligence plan.

- Supported by staff, funded by the Bureau of Justice Assistance (BJA) or DHS.

- All user groups represented.

- GIWG to recommend structure for Policy/Trust Committee to oversee subcommittees.

Action Item:

- Identify how money flows to state and local agencies to implement this plan.

Discussion:

A comment was made that members of the permanent board have equal votes and that alternating chairmanship may ensure cooperation among agencies.

Issue 7: *Review the list of definitions and identify additional terms to be defined. This list will be included in the BJA report as an appendix/glossary.*

Recommendations:

- Include the definition of "intelligence" (from IACP Summit Report 2002) in the glossary.

- Adopt the glossary of terms.

Action Item:

- Security and Privacy Committees: Define “security,” “privacy,” “right-to-know,” and “need-to-know.”

Privacy Committee

Chairman Russell Porter opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Privacy Committee ("Committee") meeting on April 3, 2003, and welcomed the Committee members. The following individuals were in attendance:

Mr. Bruce Buckley (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Alan Carlson
The Justice Management Institute
Kensington, California

Mr. David Clopton
System Planning Corporation
Arlington, Virginia

Mr. Bruce Edwards
Bureau of Justice Assistance
Washington, DC

Ms. Beth Gammie (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Russell Porter (Chair)
Iowa Department of Public Safety
Des Moines, Iowa

Mr. Michael Schrunk
Multnomah County District Attorney's Office
Portland, Oregon

Chairman Porter asked the members to introduce themselves and to tell about their background and interest in intelligence and intelligence sharing.

Committee's Agenda and Scope

Chairman Porter began by discussing the Committee's goals for the meeting. It was agreed that the Committee would address the agenda issues with the goal in mind of drafting the Privacy Committee's chapter for the GIWG report on intelligence sharing. The Committee's first draft of its chapter will be completed by May 15, 2003, and the final draft will be completed by October 2003.

The Committee also discussed the scope of its work by exploring what is meant by the term "privacy." Mr. Carlson said that technically and legally, privacy is a small piece of what often is included in the concerns people have about information sharing systems. The whole of the privacy concerns include First Amendment rights of free speech, free association, and religious freedoms; Fourteenth Amendment protections against racial discrimination (applicable in profiling and watch lists); and Fourth Amendment-based regulation of searches and seizures.

Mr. Clopton echoed this sentiment by saying that the public's perception of what is private is as important as what is included in the legal definition of privacy. An agency can create uproar if it proposes or takes action that does not violate a legal privacy right, yet infringes on their perception of what is or should be protected. He also noted there are generational differences in public perception of privacy.

The Committee's discussion reflected a consensus that privacy is a term that encompasses more than the technical legal concept of privacy, including the constitutional rights discussed above, and taking into account public perceptions of privacy. There was some discussion of changing the name of the Committee to reflect this matter, but no decision was made.

Privacy Policy—General Considerations

The main task for the Privacy Committee is to make recommendations on a model privacy policy for intelligence sharing systems. Building on the previous discussion, the Committee agreed that what is legal in terms of intelligence systems and processes is the bare minimum, or the "floor" of what is required. The Committee's privacy policy will go above this floor and recommend a privacy policy that is *wise,* as well as legal.

The Committee agreed that it must be very clear in defining the scope of its proposed policy by stating what is and is not covered.

Committee members also discussed the role of 28 Code of Federal Regulations (CFR) Part 23 that describes the privacy rules and regulations for intelligence systems utilizing federal funds. Mr. Edwards pointed out that, again, 28 CFR Part 23 is the floor of what a privacy policy should include, but the Committee may go beyond this and make additional recommendations. There are intelligence units and operations that are not required to adhere to 28 CFR Part 23 because they do not use federal funds in their intelligence systems.

Chairman Porter described a framework the Committee may find useful in analyzing the intelligence process and developing a privacy policy.[3] Chairman Porter stated that under this framework, the intelligence process can be viewed as simply a series of discretionary decisions. Order, effectiveness, and accountability can be brought to the intelligence process by examining these discretionary decisions:

1) Eliminate unnecessary discretion.

2) Structure necessary discretion.

3) Conduct and build in checks to bring accountability to the process.

The Committee found this framework helpful and decided to employ it.

Post-9/11 Era

Committee members discussed the impact of the increased focus on preventing terrorism. Mr. Edwards noted that terrorism makes up only a small percentage of the crime in the United States. The privacy policy should make clear that recent legislation

[3] Chairman Porter credited Mr. Kenneth Culp Davis for developing this framework and Mr. Sam Walker with applying it to criminal intelligence work.

making exceptions for terrorism investigations and intelligence should not be abused in the course of investigating traditional crime. Discussion on this point suggested structuring the decision making process to prevent abuses when exercising any homeland security exceptions.

Accountability

Committee members agreed that in order to ensure that privacy is safeguarded and a privacy policy is adhered to, it is vital that accountability is built into the system. Accountability mechanisms, such as audit trails and periodic checks, are essential in order to discover when and where there are problems, and to build awareness in personnel that adhering to privacy procedures is important and monitored.

Chairman Porter stated that accountability must come from within an intelligence unit. He felt it important for the Committee's report to acknowledge the secret, sensitive, and confidential nature of intelligence work, and the automatic, understandable skepticism/wariness the public has about such secrecy. Outside auditing of an intelligence unit can render that unit ineffective. Other criminal intelligence units will not share information based on their concerns about keeping intelligence confidential.

Public concerns about the secrecy involved in the intelligence process may be offset by openness about its processes. While not revealing specific intelligence or information, an agency can be open about the process itself, including what privacy safeguards are built into the system and how the agency has built in accountability. Mr. Edwards added that it would be helpful to reiterate in the Committee's policy that the basic function of government is to protect public safety—and that, in order to discharge that duty, it must engage in activities that proactively protect its citizens to the highest extent possible. An agency can be open about the intelligence process to assure the public that it is important, useful, and being performed appropriately.

Intelligence Process

In order to identify the series of discretionary decisions that make up the intelligence process, the Committee needed to have a common understanding. Chairman Porter described a model of the intelligence process with five basic steps or stages:

1. Planning and Direction

2. Collecting Information

3. Processing and Collation of Information

4. Analysis and Production of Intelligence

5. Dissemination

Planning and Direction

Planning and direction involves actively choosing the focus of the intelligence process, rather than letting it unfold haphazardly. Some units, for example, focus their intelligence process on a list of specific crimes; or on organized crime, anti-terrorism, or other threats. This step is most often omitted, resulting in an intelligence process without direction, and creating a situation more prone to abuses and violations.

Collecting Information

Information comes to an intelligence unit or officer through a variety of sources, both solicited and unsolicited. For example, tips may be received in which officers may notice specific activity and seek more information. Committee members had vigorous discussion on how information is received and collected, and how it may implicate privacy concerns. Members then discussed whether the Committee's policy should even apply to the *collection* of information. The Committee agreed that its policy should be clear on what it does and does not cover.

Processing/Analysis/Dissemination

The meeting adjourned before the Committee was able to have similar discussions of these stages.

"Working Files"

The Committee agreed that its proposed policy should address the issue of "working files"—those temporary files containing information that cannot be dismissed out-of-hand, but do not rise to the level required to become part of an intelligence file and entered into an intelligence system. They require further investigation before a decision can be made. Most, if not all intelligence policies, including 28 CFR Part 23, are silent on the issue and their provisions do not apply.

Outreach

The Committee briefly discussed outreach in terms of educating the public about the privacy protections GIWG advocates (to allay fears of abuses and violations), and about the value and wisdom with law enforcement adopting sound privacy policies.

Action Items

In order to prepare the first draft of its proposed policy, Committee members and staff agreed to complete the following action items:

April 14 Committee members will review and critique existing intelligence policies and return their comments to Ms. Gammie.

- Proposed changes to 28 CFR Part 23

- Denver Police Department Intelligence Policy

Committee members agree to submit their proposed accountability mechanisms to Ms. Gammie.

Committee members (primarily Chairman Porter) will compile a list of improper intelligence practices or abuses and problems—not to cast blame, but to motivate and guide the intended audience of the model policy.

Committee members will determine terms to be defined in the Committee's chapter and/or the report's glossary.

Ms. Gammie will circulate a proposed outline of the Committee's chapter to Committee members.

April 18 Committee will conduct a conference call to discuss the first draft of their chapter.

April 22 First draft will be circulated to Committee members and submitted for the Bureau of Justice Assistance Interim Report.

Conclusion

Chairman Porter thanked the members for their participation and adjourned the meeting.

Outreach Committee

Chairman William Berger opened the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Outreach Committee ("Committee") meeting on April 3, 2003, and welcomed the Committee members and observers. The following individuals were in attendance:

Mr. William Berger (Chair)
North Miami Beach Police Department
North Miami Beach, Florida

Ms. Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia

Ms. June Hill (Note taker)
Institute for Intergovernmental Research
Tallahassee, Florida

Mr. Ritchie A. Martinez
Arizona Department of Public Safety/HIDTA
Tucson, Arizona

Mr. Richard Randall
Kendall County Sheriff's Office
Yorkville, Illinois

Mr. John Terry (Facilitator)
Institute for Intergovernmental Research
Tallahassee, Florida

Ms. Pat Thackston
Institute for Intergovernmental Research
Tallahassee, Florida

The following members of the GIWG Training Committee were in attendance:

Mr. Donald J. Brackman
National White Collar Crime Center
Richmond, Virginia

Mr. Jerry Marynik
California Department of Justice
Sacramento, California

Mr. Thomas O'Connor
Maryland Heights Police Department
Maryland Heights, Missouri

Ms. Marilyn B. Peterson
New Jersey Division of Criminal Justice
Trenton, New Jersey

Chairman Berger invited the members of the GIWG Training Committee, as well as others present, to offer input and suggestions during the discussions. The Outreach Committee had nine issues on the agenda to resolve. The following is a summary of discussions and recommendations/action items.

Issue 1: *Develop a proposed policy promoting the involvement of all relevant parties (local, state, and tribal law enforcement; emergency management and corrections personnel; emergency responders; etc.) in the National Intelligence Plan.*[4]

Chairman Berger reviewed the language recommended as a result of the IACP Summit for a proposed policy statement that promotes the involvement of relevant parties in the National Intelligence Plan. There was discussion regarding the need for all

[4] During the closing remarks of the Plenary Session, the GIWG recommended that the Plan's title be changed to the National *Criminal* Intelligence *Sharing* Plan.

relevant groups to have access to criminal intelligence information, and it was agreed that some should be based upon the "need-to-know, right-to-know" concept. Examples cited was that emergency responders/management should share information, but not necessarily receive or have access to intelligence, unless it is relevant to their scope of work. Mr. Randall mentioned that there is some intelligence information going out to them from the Regional Information Sharing Systems (RISS) that is tailored to their needs, so they have limited access to a portion of intelligence information. After further discussion, the Committee recommended the following language for the proposed policy:

Recommendations/Actions: Proposed policy statement: All relevant parties utilizing the communications capability recommended by the Plan, with a goal of promoting public safety, include but are not limited to: local, state, and tribal law enforcement personnel; emergency responders; emergency management staff; corrections personnel; and probation officers that shall contribute to and share intelligence information.

Discussion continued on how this policy would be implemented and what steps could be taken to institutionalize this effort. Suggestions and comments included: all law enforcement (LE) must have access to the National Intelligence Plan; the capacity to participate is not equal among all LE because of funding—some do not have the computer/network systems needed; local, state, and federal LE, and other relevant groups must become stakeholders or buy-in to the concept and plan; and some individual agencies have not agreed to participate, even through it has been endorsed through the office of the U.S. Attorney General. The Committee outlined an additional recommendation for this issue.

Recommendations/Actions: A National Signing Day should be held where leaders of LE and other relevant groups come together for a symbolic "sign-on" to the National Intelligence Plan. Participants should include a wide range of representatives—from the highest level of government, to the local LE level. Education regarding the plan for all LE levels is imperative prior to the National Signing Day. Beginning at the federal level, the education process should include national LE organizations (i.e., Fraternal Order of Police, Sheriff's Association, state and local LE association/organizations, and entities of federal, state, local, and campus LE). Specific groups should be targeted for presentations at national conferences. Press conferences about the Plan should be held for the public.

Issue 2: *How is endorsement of the Plan by federal officials and key contacts ensured? Identify points to be discussed with the Federal Bureau of Investigation (FBI)/ U.S. Department of Homeland Security (DHS)/U.S. Drug Enforcement Administration (DEA)/other major federal agencies.*

Chairman Berger acknowledged that obtaining federal agencies "buy-in" of the National Intelligence Plan is a major challenge for the GIWG. He suggested that consideration should be given to developing a step-by-step plan detailing how this effort should occur. The following forums/mechanisms could be utilized to deliver appropriate information: federal academies, personal one-on-one contacts, and letters. Consideration should also be given to developing a "ready-to-use" package that would contain information and materials suitable for outreach and marketing efforts (could contain language such as, "in the spirit of the Patriot Act"). The federal agencies should be approached first, followed by other levels of LE. It is imperative that high-level federal leadership implements the Plan. It was noted that the GIWG Committee is a Federal Advisory Committee, and does not have direct access to Congress. However, recommendations can be made by Global that could result in Congressional action.

Recommendations/Actions: Develop a one or two-page overview or at-a-glance for the National Intelligence Plan to highlight the most important points. Identify and hold one-on-one meetings with federal leadership/agencies to obtain consensus and endorsement. Recognize there are political aspects and prepare a plan—what we propose, what we anticipate, what results will be. Pitch the plan as the best system developed to help all LE. The end result should be a declaration of cooperation, documented by signature.

<u>Issue 3</u>: *Recommend a plan of action for working with state Police Officer Standards and Training (POST) directors to encourage/require intelligence training for all appropriate levels of personnel.*

Chairman Berger began the discussion by stating that the International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Report outlined a mandate for the coordinating council (GIWG) to work with local, state, tribal, and federal training academies and other training providers to make curriculum changes in support of the new intelligence sharing goals. A plan should be developed that identifies the various types of academies and facilities that provide training and would be affected by this mandate, and should include actions needed to effect curriculum changes.

The group discussed training specifications for various states, how they are mandated (by the state or locally), and whether or not the intelligence training could be incorporated through those channels. This might require a legislative package for states or governors (to be delivered by an outreach team), and should include a funding component. The benefit of partnering with associations/organizations with training functions was discussed.

Recommendations/Actions: Partner with state POST directors and other associations and membership organizations that represent training functions for endorsement of intelligence training curriculum for all appropriate levels of personnel. Request their input to determine the various types of academies and facilities that provide training. Develop an in-service curriculum at the academy level that will provide basics of the National Intelligence Plan—what, when, and where type of information, as well as software application training for entering, importing, and extracting data.

<u>Issue 4</u>: *Identify organizations/agencies/audiences to outreach/market the plan to. This should include not only executives but also all other levels of affected personnel.*

A timetable and calendar for marketing of the National Intelligence Plan was discussed, as well as centralized calendar maintenance. Venues for public relations/marketing opportunities were identified, and it was suggested that a major conference of associations/organizations should be considered for the specific purpose of disseminating information about the plan. It was noted that Mr. Randall has already presented an overview of the Plan to the directors of 50 states and will make additional presentations as often as possible to various groups. A presentation is currently being developed for marketing purposes to groups such as the National Sheriff's Association, IACP, and others. Additionally, print materials will be developed for association and organization magazine articles that could be used for advanced marketing, perhaps with cover stories occurring in the same month. Chairman Berger added that all members of the GIWG are encouraged to take responsibility for outreach, wherever and whenever they can.

Recommendations/Actions: Access a major association or organization conference during the summer for the purpose of disseminating information and marketing the National Intelligence Plan. In October, or upon completion of the initial marketing product, the first public display of the Plan should be released. The marketing/outreach timetable should begin at that point, and may take as long as three years. Marketing should be presented to agencies, associations, and organizations as follows: year one, national and federal; year two, state; and year three, local.

Issue 5: *Identify the methods of outreach available, and determine which is appropriate for each type of audience.*

The Committee discussed the mechanisms available to publicize and market the Plan. Methods of outreach were discussed and include Web sites, publications, speaking engagements, conferences, etc. It was agreed that documentation of the outreach performed should be maintained in order to monitor the results of the efforts.

Recommendations/Actions: The National Signing Day will be the catalyst for the marketing/outreach efforts. Press conferences will be used to publicize what the National Intelligence Plan is, how it works, and how agencies can work together. Through Global, a Web site should be developed and linked to all levels of LE agencies, associations, and organizations. A logo should be designed for the National Intelligence Plan so groups can use it as a "We support the National Intelligence Plan" on their own Web sites.

Issue 6: *Identify information to disseminate for each type of audience, which may be different based on a recipient's perspective, level, or type of agency (e.g., tribal agencies).*

The Committee discussed the development of an outreach/marketing plan that can be geared towards specific audiences. It was suggested that a train-the-trainer application could be developed to train several individuals, who will in turn train others to make marketing/outreach presentations at all levels of LE. Identification of what should be contained in the "package" for each audience should be determined.

Recommendations/Actions: A train-the-trainer application should be developed to increase the number of presenters available to make marketing/outreach presentations at all levels of LE, including but not limited to: chief executives, emergency responders, street officers, and tribal officers. The Plan should be developed for each audience, as appropriate. The marketing/outreach plan for federal agencies and national associations/organizations should include information appropriate for each level of LE. Two to three types of plans must be developed, as well as an overview plan for CEOs and participants.

Issue 7: *Determine how to monitor the success of outreach efforts. Should feedback mechanisms (surveys, questionnaires) be employed?*

Chairman Berger began the discussion by asking that the Committee consider methods for assessment of the marketing/outreach efforts. Items to consider monitoring might include community knowledge of the Plan, training efforts, agency adoption of policies and standards, and systems participating in the communications capability recommended by the Plan. Types of surveys and other monitoring and reporting mechanisms were discussed. To determine if the Plan is working, doing what was expected, or is useful, it was agreed that the first group surveyed should be the participants. Types of questions to include were suggested.

Recommendations/Actions: Follow-up with Plan participants should occur by a time interval series of surveys (i.e., six months, one year, two year, and completed towards the end of the third year). The surveys should be developed appropriate to various LE levels and clear definitions of what is being measured should be defined (beginning with the implementation of the Plan, through use and benefits of the Plan). These surveys may not necessarily be written; they could be available by an 800-telephone number, conducted by staff, placed on the Global Web site, or mailed. It was suggested that staff should work on the development of the measurement tools/surveys.

Issue 8: *Identify publications to disseminate the article prepared at the request of the Committee.*

The Committee identified several sources, publications, and Web sites that can be utilized for education and promotion of the National Intelligence Plan. There was discussion regarding the need to define the scope of what we are selling: national security; a system that will do a better job for information sharing; prevention of criminal activity; helping to prevent bad things from happing to this nation; a national standard for information gathering/sharing; or concepts so LE can be more knowledgeable.

Recommendations/Actions: Develop and publish a master list of publications and Web sites to be utilized for promotion of the National Intelligence Plan. Produce information and overview articles for publication, as articles to be published during the various stages of implementation of the Plan, available training for LE, emergency responders, etc. Develop and produce a Web site accessible to appropriate LE personnel.

Issue 9: *Review the list of definitions and identify additional terms to be defined.*

The Committee reviewed the list of definitions defined in the draft report that might significantly affect policy choices. Chairman Berger advised that additional terminology and definitions would be received from other committees of the GIWG during the coming weeks.

Recommendations/Actions: This item is postponed until additional terminology and definitions are received; at that time, the Committee will consider and discuss possible terms for inclusion.

Chairman Berger thanked participants for their input, as well as Mr. O’Connor, Chairman of the Training Committee.

Plenary Session

Chairman Carraway convened the Plenary Session and welcomed the guests and attendees. The following individuals were in attendance:

Mr. Donald J. Brackman
National White Collar Crime Center
Richmond, Virginia

Ms. Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia

Mr. Doug Bodrero
Institute for Intergovernmental
Research
Tallahassee, Florida

Mr. Bruce Buckley
Institute for Intergovernmental
Research
Tallahassee, Florida

Mr. Alan Carlson
The Justice Management Institute
Kensington, California

Mr. Melvin Carraway
Indiana State Police
Indianapolis, Indiana

Mr. David Clopton
System Planning Corporation
Arlington, Virginia

Mr. Carlo Cudio
Monterey Police Department
Monterey, California

Mr. Bob Cummings
Institute for Intergovernmental
Research
Tallahassee, Florida

Ms. Patty Dobbs
Institute for Intergovernmental
Research
Tallahassee, Florida

Mr. Bruce Edwards
Bureau of Justice Assistance
Washington, DC

Mr. Max Fratoddi
Federal Bureau of Investigation
Washington, DC

Mr. Tom Frazier
Major City Chiefs Association
Baltimore, Maryland

Mr. Dennis Garrett
Arizona Department of Public
Safety
Phoenix, Arizona

Mr. Don Johnson
Institute for Intergovernmental
Research
Tallahassee, Florida

Mr. Phil Keith
Knoxville Police Department
Knoxville, Tennessee

Mr. Patrick McCreary
Bureau of Justice Assistance
Washington, DC

Mr. George March
Regional Information Sharing Systems
Office of Information Technology
Thorndale, Pennsylvania

Mr. Ritchie Martinez
Arizona Department of Public
Safety/HIDTA
Tucson, Arizona

Mr. Jerry Marynik
California Department of Justice
Sacramento, California

Mr. Miles Matthews
Counterdrug Intelligence Executive
Secretariat
Washington, DC

Mr. Kent Mawyer
Criminal Information Sharing Alliance
Austin, Texas

Mr. Steve McCraw
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. Peter Modafferi
Rockland County District
Attorney's Office
New City, New York

Ms. Karen Morr
U.S. Department of Homeland Security
Washington, DC

Ms. Marilynn Nolan
U.S. Drug Enforcement Administration
Arlington, Virginia

Mr. Dan Oates
Ann Arbor Police Department
Ann Arbor, Michigan

Mr. Thomas O'Connor
Maryland Heights Police Department
Maryland Heights, Missouri

Mr. Joe Peters
Institute for Intergovernmental
Research
Tallahassee, Florida

Ms. Marilyn Peterson
New Jersey Department of Law
and Public Safety
Trenton, New Jersey

Mr. Henry Pino
Ak-Chin Tribal Police Department
Maricopa, Arizona

Mr. Russell Porter
Iowa Department of Public Safety
Des Moines, Iowa

Mr. Louis Quijas
Federal Bureau of Investigation
Washington, DC

Ms. Diane Ragans
Institute for Intergovernmental
Research
Tallahassee, Florida

Mr. Philip Ramer
Florida Department of Law Enforcement
Tallahassee, Florida

Mr. Richard Randall
Kendall County Sheriff's Office
Yorkville, Illinois

Mr. Steve Raubenolt
Ohio Highway Patrol
Columbus, Ohio

Mr. Paul Redmond
U.S. Department of Homeland Security
Washington, DC

Mr. Edward Reina
Yavapai-Prescott Tribal Police
Department
Prescott, Arizona

Mr. Neal Riddle
U.S. Department of Homeland Security
Washington, DC

Mr. Jim Savage
Federal Bureau of Investigation
Washington, DC

Mr. Michael Schrunk
Multnoma County District Attorney's
Office
Portland, Oregon

Mr. Michael Seelman
Office of Community Oriented
Policing Services
Washington, DC

Mr. Gregory Stieber
U.S. Secret Service
U.S. Department of Homeland Security
Washington, DC

Mr. John Terry
Institute for Intergovernmental
Research
Tallahassee, Florida

Ms. Pat Thackston
Institute for Intergovernmental
Research
Tallahassee, Florida

Ms. Kathy Timmons
Federal Bureau of Investigation
Washington, DC

Mr. Dave Walchak
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. Richard Ward
Bureau of Justice Assistance
Washington, DC

Committee Reports

Standards Committee

Chairman Modafferi delivered a PowerPoint presentation that contained the recommendations and items requiring further action for the issues/topics that the Committee was tasked with resolving. *(Attachment C)*

Connectivity/Systems Committee

Chairman Matthews prepared a PowerPoint presentation, which contained the Committee's recommendations for their ten assigned issues/topics. *(Attachment D)*

When discussing the Committee's recommendation for fingerprint-based checks on those users desiring access to the national network, Mr. Dick Ward questioned how the requirement would affect state and local law enforcement agencies. Mr. Matthews indicated the recommendation was controversial, but he explained the Committee members thought it was a necessity in order to elevate the trust of the system users.

While presenting the Committee's recommendations for suggested analytical tools, Ms. Peterson inquired as to whether the Committee was recommending that all agencies obtain Geographic Information System capabilities, as this could be very expensive. Mr. Matthews advised that the Committee members suggest utilizing some sort of mechanism that would allow numerous agencies to access a "tool box" and share the analytical tools contained within it.

Training Committee

Chairman O'Connor provided a brief overview of the Committee's discussions, indicating that the members focused their attention on the specific goal of fine-tuning the proposed training plan. Chairman O'Connor related that the Committee believes that the Plan will not be accepted nationally unless participants understand "what's in it for them."

Chairman O'Connor spoke briefly about funding for training efforts. GIWG Chairman Carraway responded by indicating that funding should be attached to the entire process, which would include training as a portion of that process.

Chairman O'Connor related that the Committee prioritized the levels that should receive the recommended training, with number one having the highest priority: 1) Train-the-Trainers, 2) Executives, 3) Managers − including Supervisors and Commanders, 4) Patrol Officers, 5) Intelligence Officers, and 6) Analysts.

Policy Committee

Mr. Garrett, speaking on behalf of Chairman Frazier, delivered a PowerPoint presentation that contained the recommendations and action items for the issues that the Policy Committee was tasked with resolving during their meeting. *(Attachment E)* In addition to the action items identified in the PowerPoint, Mr. Garrett indicated that when drafting the letter to the U.S. Department of Justice (DOJ) regarding 28 Code of Federal Regulations (CFR) Part 23, the Committee requested that the word “tribal” be added to the language of the regulation.

Privacy Committee

Mr. Porter provided a PowerPoint presentation that summarized the Committee’s discussions, and included action items that the Committee is tasked with resolving. *(Attachment F)* At the end of the presentation, Mr. Porter emphasized that privacy and civil rights should be highlighted and prioritized within the National Criminal Intelligence Sharing Plan so that all readers and recipients of the Plan know how important privacy issues are to the GIWG.

Outreach Committee

Mr. Randall provided the Committee report for Chairman Berger, who departed the meeting for a previous appointment. Mr. Randall summarized the Committee’s recommendations for outreach activities and tasks as follows:

- A National Signing Day should be held where law enforcement leaders and other relevant groups come together for a symbolic “sign-on” to the National Criminal Intelligence Sharing Plan.

- Develop a step-by-step plan for obtaining “buy-in” of the Plan by all levels of law enforcement.

- Partner with state Peace Officers Standards and Training directors and other associations and membership organizations that represent training functions for endorsement of intelligence training curriculum for all appropriate levels of law enforcement.

- Access a major association or organization conference during the summer months for the purpose of marketing and disseminating information on the Plan.

- Develop a Web site and logo for the Plan.

- Develop a train-the-trainer application in order to increase the number of presenters available to conduct marketing/outreach efforts.

- Surveys should be utilized to monitor the success of the Plan.

- Develop a master list of publications and Web sites to be utilized for promotion of the Plan.

Closing Remarks

Chairman Carraway thanked the members for their efforts in their individual Committees. He indicated that members of the GIWG have a large window of opportunity between now and October 2003 (when the final report is due), to perform outreach to further the efforts of the working group. Chairman Carraway advised that this is a grassroots effort—it is not just a local, state, or federal initiative—it is a *national* effort that takes a partnership between all involved parties to do the right thing.

Mr. Martinez asked if the GIWG was going to recommend that the word *criminal* be inserted into the Plan's title, e.g., The National *Criminal* Intelligence Sharing Plan. Chairman Carraway responded that was not problematic and he recommend that the word be added.

Chairman Carraway requested that all Committee work products be provided to staff by April 18 in order to be included in the interim report due to BJA on May 15, 2003. Mr. Matthews requested clarification regarding when the vetting process, outside of the GIWG, begins on the report. Mr. Cummings responded that the process would begin after the interim report is submitted to BJA. He indicated several opportunities exist in the near future to promote the Plan, including the upcoming Law Enforcement Intelligence Unit Conference in Seattle, Washington. Mr. Cummings also advised planning discussions must occur for the presentation on the Plan at the upcoming International Association of Chiefs of Police Annual Conference in October 2003.

Chairman Carraway advised the membership that the next meetings were planned for June 16-17, 2003, in Boca Raton, Florida, and on September 9-10, 2003, in Arlington, Virginia. The meeting was then adjourned.

Attachment A

Memorandum of Understanding
Between the

Federal of Bureau of Investigation
Central Intelligence Agency
U.S. Department of Homeland Security

Attachment B

CJIS PowerPoint Presentation

Attachment C

Standards Committee
PowerPoint Presentation

Attachment D

Connectivity/Systems Committee PowerPoint Presentation

Attachment E

Policy Committee
PowerPoint Presentation

Attachment F

Privacy Committee
PowerPoint Presentation