

U.S. Attorney General Ashcroft Supports Global's *National Criminal Intelligence Sharing Plan*

On May 14, 2004, in the Great Hall of Justice, U.S. Attorney General John Ashcroft launched the *National Criminal Intelligence Sharing Plan* (NCISP or "Plan").



The Plan describes a nationwide communications capability linking all levels of law enforcement personnel—including officers on the street, intelligence analysts, unit commanders, and law enforcement executives—for the purpose of sharing critical data to prevent terrorism and crime. The NCISP includes 28 recommendations and action items.

"The *National Criminal Intelligence Sharing Plan*

is the first of its kind in the nation, uniting law enforcement agencies of all sizes and geographic locations in a truly national effort to prevent terrorism and criminal activity," said Attorney General John Ashcroft. "By raising cooperation and communication among local, state, and federal partners to an unprecedented level, this groundbreaking effort will strengthen the abilities of the justice community to detect threats and protect American lives and liberties."

The NCISP is a direct result of recommendations made at the 2002 Intelligence Sharing Summit, hosted by the International Association of Chiefs of Police (IACP). Building on the IACP groundwork, the Global Justice Information Sharing Initiative (Global)—through its Intelligence Working Group—designed a plan to address security and intelligence needs not long after the tragic events of September 11, 2001.

Attorney General Ashcroft was joined in supporting the NCISP by a host of justice and law enforcement leaders, including Federal Bureau of Investigation Director

Upcoming Events

November 4-5, 2004

Global Infrastructure/Standards Working Group Meeting
Hyatt Regency Albuquerque, Albuquerque, NM

November 8-10, 2004

Global Justice XML Data Model Developer's Workshop
Marx Hotel, Syracuse, NY

November 10, 2004

Global Privacy and Information Quality Working Group
Meeting
Offices of the Illinois Criminal Justice Information
Authority, Chicago, IL

December 1, 2004

Global Security Architecture Committee Meeting
Marriott Crystal Gateway, Arlington, VA

December 2, 2004

Global Web Services Security Task Force Meeting
Marriott Crystal Gateway, Arlington, VA

December 7-8, 2004

Global Security Working Group Meeting
Denver, CO (meeting site to be determined)

For information on other training programs, conferences, and meetings that may be of interest, please visit the Event Calendar on the OJP IT Web site at www.it.ojp.gov.

Robert Mueller; Assistant Attorney General Deborah J. Daniels, Office of Justice Programs; General Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection, U.S. Department of Homeland Security; Chief Joseph Polisar, President, IACP; Director Carl Peed, Office of Community Oriented Policing Services; Special Agent in Charge Russ Porter, Iowa Department of Public Safety; and Superintendent Melvin Carraway, Indiana State Police and chair of the Global Advisory Committee.

The *National Criminal Intelligence Sharing Plan* and additional Global resources are available at www.it.ojp.gov/global.

Fall GAC Meeting a Big Success

The second biannual Global Advisory Committee (GAC or “Committee”) meeting of 2004—held September 28-29 in Arlington, Virginia—was a big success.

The Committee agenda was filled with important topics that have the potential to greatly impact the justice arena. The new meeting format, designed to provide members a greater opportunity to participate, resulted in productive discussions and some excellent recommendations.

Two panel discussions were held: *Perspectives on Privacy in the Justice Information Sharing Arena* and *Intelligence Sharing (What the 9/11 Commission Report Left Out)*.

The privacy panel featured James Dempsey, Center for Democracy and Technology; Lance Hoffman, Ph.D., George Washington University; and Peter Sand, U.S. Department of Homeland Security (DHS). The panelists discussed privacy issues from several angles. The point was made that privacy is generally the last issue addressed when creating new technology and is usually not addressed adequately, if at all. It is seen as a barrier to law enforcement and to information sharing.

Also discussed was the use of databases created primarily for prevention of terrorism, such as the systems designed to screen airline passengers. Several members of the GAC voiced opinions that these networks could, and should, be used for solving other major crimes.



CHAIRMAN'S CORNER

A word from GAC Chair Melvin Carraway

As those of you who attended the fall GAC meeting in Arlington can attest, the meeting was extremely productive—one of the best ever. The revised format led to unprecedented participation and group discussion that proved to be very beneficial to decision making. An overview of the major events that took place at the meeting is provided in this newsletter.

As evidenced during the meeting, Global members are key players in a wide array of high-profile projects. One such project involves members of the Global Intelligence Working Group and Criminal Intelligence Coordinating Council (CICC) working with other law enforcement professionals to develop standards for fusion centers. Several local and state agencies are developing fusion centers using funds received from the U.S. Department of Homeland Security. There are currently no standards in place to ensure that these centers are interoperable with other such centers and law enforcement and homeland security agencies. The Fusion Center Focus Group is working to develop basic elements of an intelligence fusion center, suggested steps to establish fusion centers, model policies, and other materials necessary to implement a fusion center concept.

The CICC was requested by the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security

(DHS) to coordinate the assignment of several full-time local and state representatives for a 60 to 90-day time period beginning in late October 2004 to assist with the implementation plan for Executive Order 13356. The individuals will serve as the focal point for coordination of all DHS/DOJ Tiger Team activities related to the provision of local and state law enforcement input into the implementation plan. Issues will be identified and shared with other members of the CICC.

The full-time representatives are Deputy Superintendent Willie Bradley, Boston, Massachusetts, Police Department; Sheriff Richard Randall, Kendall County, Illinois, Sheriff's Office; and Investigator Thomas Brozycki of the New York State Police, assigned to the Upstate New York Regional Intelligence Center (UNYRIC). Additionally, the following individuals will be assisting with the project on a part-time basis via video/teleconferencing and occasional meeting attendance: Kenneth Bouche, Peter Modafferi, Joseph Polisar, Russell Porter, Richard Stanek, and Kurt Schmid.

These are only two of the many projects to which Global members are currently lending their expertise. Global continues to shine because of the dedication and involvement of its outstanding members. Thanks to all of you for devoting your time and efforts to these important initiatives!

Continued from page 2



The Markle Foundation Task Force's report entitled *Creating A Trusted Information Network for Homeland Security* was also discussed at length. GAC members expressed concern to James Dempsey that the report, as well as the *9/11 Commission Report*, both failed to address the need and value of connectivity to state and local law enforcement. Mr. Dempsey advised that the task force did try to include the principle of information sharing at the state and local levels. He further advised that he felt the Markle Task Force would welcome at least one representative of local and state law enforcement, and he agreed to take the word back that Global should be involved in future discussions.

The intelligence panel was composed of experts in the field, including Russ Porter, Iowa Department of Public Safety; Richard Russell, DHS; Maureen Baginski, Federal Bureau of Investigation; William Berger, Palm Bay, Florida, Police Department; and Daniel Oates, Ann Arbor, Michigan, Police Department. These experts provided updates on major intelligence issues and the critical role of law enforcement at the local and state levels (an issue largely absent from the *9/11 Commission Report*). The panelists also discussed intelligence initiatives under way in their own organizations as well as in the Global Intelligence Working Group and Criminal Intelligence Coordinating Council.

GAC members were also briefed on the temporary assignment of several Global members to assist in the implementation of Presidential Executive Order 13356 (see details regarding this project under the Chairman's Corner).

Another key agenda item was the demonstration of the Counterterrorism Collaborative Interoperability Project (CCIP). Ken Cassine, Law Enforcement Online (LEO); Angelo Fiumara, Regional Information Sharing Systems® (RISS); Glen Gillum, Criminal Information Sharing Alliance network (CISAnet); and Chris Holmes, DHS Homeland Security Information Network (HSIN), showcased their respective systems and illustrated how the CCIP is working to promote interoperability among the participating networks. This groundbreaking technology was very well received by GAC members. (Additional details regarding this project can be found elsewhere in this newsletter.)

Several Global products were reviewed and approved by the GAC membership, including *Audit Checklist for the Criminal*



Intelligence Function (to be added to the Global resource library) *Law Enforcement Analytic Standards*, and *Core Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies* (produced by the Global Intelligence Working Group for mass distribution).

Also presented was the much-anticipated report by the Global Infrastructure/Standards Working Group. (Details of this report are provided elsewhere in this newsletter.) The subject of the document—Service-Oriented Architecture, and its potential for the justice arena—will impact all of Global's efforts and Working Groups; therefore, the Committee's unanimous approval of the following resolution is particularly newsworthy:

The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) adopts the report (as amended, per GAC response, to address privacy and information quality issues) of the Global Infrastructure/Standards Working Group (GISWG), titled *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*.

Continued from page 3

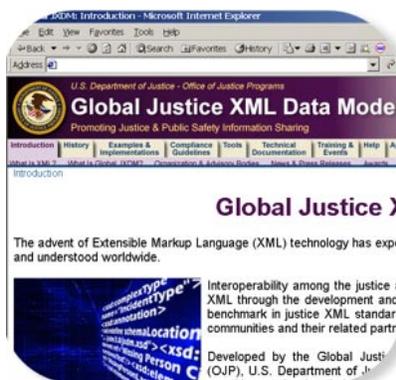
Global:

- Recognizes SOA as the recommended framework for development of justice information sharing systems.
- Adopts the report's action agenda for its activities to further the utility of SOA for the justice community.
- Urges the members of the justice community to take corollary steps in the development of their own systems.

As part of the Global Security Working Group update, Tom Coty, DHS, briefed the Committee on the DHS *Statement of Requirements* (SoR), a document outlining future technology requirements for public safety wireless communications and interoperability. The SoR, developed under the SAFECOM Program, marks the first time the 50,000 public safety agencies have a single document that defines future requirements for communicating and sharing information—as authorized, when and where needed, and in a manner that allows for the most effective use of that information. Members unanimously voted to recognize and support the SoR as a model for wireless information sharing and to contribute GAC expertise (through the participation of select members) on the SoR-related Steering, User Needs, and Architecture Committees.

Elections for GAC chair and vice chair—which occur every two years—were held on the afternoon of September 28. Superintendent Melvin Carraway, Indiana State Police, was reelected as chair; Gerry Wethington, Chief Information Officer for the state of Missouri, was reelected as vice chair.

The next GAC meeting is scheduled for April 27-28, 2005, at the Wyndham Washington, DC, hotel, located at 1400 M Street, NW. More details will be forthcoming as the meeting date draws closer.



Announcing the Newest Global JXDM Release, Version 3.0.2

The Office of Justice Programs (OJP), together with Global, has officially issued a new version of the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM)

to the justice community—version 3.0.2. This latest release of the Global JXDM, Version 3.0, series is enhanced to increase the ability of justice and public safety communities to share justice information at all levels, laying the foundation for local, state, and national justice interoperability.

The Global JXDM is a comprehensive product that includes a data model, a data dictionary, and an XML schema. The Global JXDM is sponsored by OJP, with development supported by the Global XML Structure Task Force (XSTF), which works closely with researchers at the Georgia Tech Research Institute. The XSTF is composed of government and industry-domain experts, technical managers, and engineers.

New releases are issued by the XSTF, which reviews and evaluates each version of the Global JXDM. The XSTF solicits feedback from technical experts and practitioners in both industry and government and authorizes Global JXDM changes based on this feedback. All approved additions, deletions, and modifications are applied to future releases, with a cumulative change log published along with each release. When a reasonable number of updates are approved by the XSTF, a new version is released.

Since its first prerelease in April 2003, the Global JXDM has continued to undergo intensive reviews, receive feedback-and-error reports online from the public, and provide a Global JXDM Listserv discussion forum for sharing expertise and support. Today, more than fifty law enforcement and justice-related projects have been implemented utilizing the Global JXDM, further demonstrating its flexibility and stability.

For more information on the Global JXDM, Version 3.0.2, and the resources and tools associated with the product, refer to the Global JXDM Web site at <http://it.ojp.gov/gjxdm>. To specifically access the Global JXDM, Version 3.0.2, refer to <http://it.ojp.gov/jxdm/>.

Service-Oriented Architecture

At their fall meeting, the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) unanimously adopted the report of the Global Infrastructure/Standards Working Group (GISWG) titled *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*.

Global recognizes Service-Oriented Architecture (SOA) as the recommended framework for development of justice information sharing systems, adopts the report's action agenda for its activities to further the utility of SOA for the justice community, and urges the members of the justice community to take corollary steps in the development of their own systems. Global's approval was based on the understanding that SOA is an approach that is most likely to result in an infrastructure that will support its vision of how information should be shared among the justice community.

Information sharing is a long-standing practice among justice agencies, particularly within the law enforcement community. As society becomes more mobile, the importance of sharing data to improve police effectiveness grows exponentially. The technology available has been critical to the ability to share. The kinds of information, the working partnerships, and the types of data exchanged have been transformed as we have moved from paper, telegraph, telephones, and teletype machines to computers and wireless communications. The arrival of the World Wide Web (the Web) and the technologies that support it have spawned a brave new world of information sharing that goes beyond exchanges among specific partners to embrace the whole of the justice community—law enforcement, prosecutors, defense counsel, courts, probation, corrections—and a host of corollary disciplines such as homeland security, fire, emergency services, health, education, transportation, and motor vehicle licensing.



SOA incorporates six fundamental principles for the sharing of information in the justice community:

- The architecture must recognize innumerable independent agencies and funding bodies from local, state, tribal, and federal governments.
- Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.
- The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.
- Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.
- Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.
- The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

This concept of design allows the original data owners to control their own data, both in terms of who is allowed to access it and in ensuring the integrity of the data. It allows agencies to retain the investment they have made in their existing systems, while at the same time gaining access to valuable information contained in other agency systems. It uses the technology of the Internet, which is user-friendly and readily understood by most users of today's computer systems.

Counterterrorism Collaborative Interoperability Project Pursues Groundbreaking Technology

The operators of the Homeland Security Information Network (HSIN), Law Enforcement Online (LEO), the Regional Information Sharing Systems (RISS), and the Criminal Information Sharing Alliance network (CISAnet) are working together to develop and implement a plan for interoperability among their systems. This plan, known as the Counterterrorism Collaborative Interoperability Project, combines the best features of each of the partner systems to form a new connectivity and information sharing environment that will provide for more effective communications and more efficient responses to better deter, detect, and prevent criminal and terrorist activities.

Since July 2004, several meetings have taken place between the U.S. Department of Homeland Security, the Federal Bureau of Investigation, the U.S. Department of Justice, RISS, and CISA to discuss how interoperability among the systems can be achieved. This initiative represents significant collaboration among several of the country's largest criminal justice information systems. Not all the information contained in each of the member systems will be accessible to every agent of the other organizations. Instead, each agency will determine what information it is willing to share, along with user vetting requirements and protocols.

Information shared will remain within the agency that has collected it; however, each organization will allow the other

participating member systems access to selected information that it has gathered and published. On September 20, 2004, HSIN, RISS, and CISAnet demonstrated the ability to post information in their individual databases and review/retrieve the information via the other systems. HSIN and LEO achieved connectivity by cross-posting information.

To accomplish this goal, the group formed a timeline that allows for systematic growth toward mid- and long-term interoperability. The first step in this process was to establish a clear understanding among all parties regarding technical requirements and other considerations. Once the requirements have been met, the next step calls for the participating members to develop the ability to share and publish information.

The vision for interoperability is system compatibility, which is defined in three stages:



- Near-term (60 days)—sharing and publishing appropriate finished products and documents; this was accomplished by September 20, 2004.
- Mid-term (3 to 6 months)—enabling individual users to collaborate among themselves.
- Long-term (12 to 18 months)—enabling federated search capabilities and sharing chat and whiteboard information, data integration, protocols, standards and, possibly, single sign-on features.

It is anticipated that this project, when complete, will have a tremendous impact on the ability of all levels of law enforcement to obtain and share information regarding criminal and terrorist activities.

Mark your calendars

The next GAC meeting is scheduled for April 27-28, 2005, at the Wyndham Washington DC.

This document was supported by Grant No. 2000-LD-BX-0003, awarded by the Office of Justice Programs. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the U.S. Department of Justice.