

**Global Justice Information Sharing Initiative (Global)
Global Privacy and Information Quality Working Group (GPIQWG) Meeting**

Salt Lake City, Utah
March 26–27, 2009

March 26, 2009—Meeting Summary

Background, Purpose, and Introductions

The U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), and the Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group (GPIQWG) convened a meeting on March 26, 2009, in Salt Lake City, Utah, at 8:30 a.m. The Honorable Anthony Capizzi (Judge Capizzi), Montgomery County, Ohio, Juvenile Court and GPIQWG Chair, led the meeting in furtherance of and alignment with the GPIQWG's *Vision and Mission Statements*.

Chair

The Honorable Anthony Capizzi
*Montgomery County, Ohio, Juvenile Court
National Council of Juvenile and
Family Court Judges*

Vice Chair

Mr. Phil Stevenson
Arizona Criminal Justice Commission

Mr. Francis (Paco) X. Aumand, III
Vermont Department of Public Safety

Ms. Cindy Southworth
National Network to End Domestic Violence

Ms. Ayn H. Crawley
*Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security*

Ms. Martha W. Steketee
Independent Consultant

Lieutenant Kathleen DeGrasse
Illinois State Police

Randall Wickline
*Criminal Justice Information Services Division
Federal Bureau of Investigation*

Mr. Eric Johnson
*SEARCH, The National Consortium for Justice
Information and Statistics*

Mr. Carl Wicklund, GAC Vice Chair
American Probation and Parole Association

Erin Kenneally, Esquire
eLCHEMY, Incorporated

Ms. Tammy Woodhams
National Criminal Justice Association

Mr. Dominic LaMar
*Space and Naval Warfare Systems Center
(SPAWAR), U.S. Navy*

Guest Observer
Mr. John Loverude
Advanced Technology Systems, Inc.

Mr. Thomas MacLellan
National Governors Association

Staff
Ms. Christina Abernathy
Institute for Intergovernmental Research

Mr. Michael McDonald
Delaware State Police

Ms. Terri Pate
Institute for Intergovernmental Research

Mr. Steve Siegel
Office of the Denver District Attorney

Judge Capizzi welcomed all the attendees and reviewed the meeting agenda (Appendix B) and goals. Judge Capizzi asked whether members had any changes to the December 16, 2008, GPIQWG meeting summary. No changes were suggested and the meeting summary was accepted and finalized.

Judge Capizzi discussed his efforts, upon appointment as GPIQWG chair, to make personal calls to each individual GPIQWG member to foster involvement and contributions to the GPIQWG endeavor. “I wanted to instill in everyone the feeling that each of you can and will be actively involved.” he said. “While members provide great effort at the meetings, we also need a broad-based level of input in between meetings. I am asking everyone to give the level of effort we need to ‘round third base’ and complete the two tools that are in final draft form.” Judge Capizzi stated that he would like for GPIQWG to meet its goal of completing the *Information Quality Program Guide* in 2009.

Judge Capizzi has been attending GAC meetings and has heard the concerns raised about the budget reductions. “As you know, we have had cost reductions across the board in Global. BJA has requested, when possible, to reduce working group meetings to two per year. Based on a discussion with BJA, however, GPIQWG has been approved to continue to hold three meetings, based on its justification that we are a ‘hub of the wheel’ of the GAC.” he said. By “‘hub of the wheel,” Judge Capizzi means that GPIQWG is in some ways the vetting group for some of Global’s products, in particular those that touch privacy and information-quality issues. Several federal partners look to GPIQWG for this role. This membership has done a lot of great work and is seen as the body with a lot of expertise that other agencies seek to tap into.

Judge Capizzi spoke about the Privacy Activities Coordination meeting, held on March 16, 2009, in Washington, DC, which was attended by GAC Chairman Bob Boehmer, GAC Vice Chair Carl Wicklund, GPIQWG Vice Chair Mr. Phil Stevenson, Judge Capizzi, Terri Pate, and Christina Abernathy. He described the purpose of the meeting, which was to bring together all of the privacy representatives, GAC, GPIQWG, the U.S. Department of Homeland Security (DHS), and DOJ to ensure that everyone was on the same page regarding privacy efforts, and to discuss collaboration and expectations of each program. An update was provided on the fusion center privacy policy development efforts, as well as GPIQWG priorities for 2009. The group was informed of the National Governors Association’s (NGA’s) new Privacy Policy Academy, which is currently in the planning stages and will fund five state agencies with \$20,000 to develop privacy policies. According to Mr. Thomas MacLellan, NGA, the request for proposal is nearly complete and ready for solicitation.

Global Updates

GAC Vice Chair Carl Wicklund gave an overview of Global Advisory Committee (GAC) activities. He stated that he had spoken with Ms. Laurie Robinson, Acting Assistant Attorney General, OJP, DOJ, about setting up a meeting with the U.S. Deputy Attorney General (DAG) and to extend an invitation to attend the April 2009 GAC meeting. Ms. Robinson helped with the letter being sent to the DAG, which will be copied to Mr. Vance E. Hitch, Chief Information Officer, Office of the Chief Information Officer, DOJ, and also to key people at DOJ.

The Global Outreach Working Group’s Transition Team has developed a briefing booklet to provide a summary of Global’s efforts and products for the new administration’s transition team. GAC also formalized a resolution in support of the Law Enforcement Information Sharing Program (LEISP), which is contained in the briefing booklet in the meeting folder.

It is believed that the new administration may be more open to funding requests if pilots and lessons learned are included as part of the success of Global products. Global is requesting an increase in dollars to help fund these pilot projects. Ms. Robinson is working very hard to establish Global in the DOJ budget as a line item, which would be helpful for future funding.

At the National Fusion Center Conference held on March 10–12, 2009, Ms. Janet Napolitano, Secretary of DHS, spoke to the attendees and spent a good deal of time taking questions from the audience. It was impressive. It was evident that she clearly understands fusion centers. She made it very clear that she sees fusion centers as one of her top two priorities. She made a point of stating that it all starts with the local, state, and tribal agencies. One of the primary points emphasized at the

conference was how important it is for fusion centers to have privacy policies, and each center was encouraged to establish a privacy officer role. Privacy policies are part of the *Baseline Capabilities for State and Major Urban Area Fusion Centers* guidance established for fusion centers. There were many messages at the conference on the importance of having privacy and civil liberties policies. Privacy advocates were also invited to present on topics such as the importance of protecting the privacy rights of citizens in fusion center processes. Information sharing is a top priority, but not at the liberty of privacy and civil rights. Judge Capizzi further emphasized how DOJ's partnerships have become more successful and cooperative, not only between DOJ departments but with other federal agencies as well. There is a growing movement of cooperation and collaboration with privacy and information sharing.

The next GESC meeting will be on April 22, 2009, and the next GAC meeting will be on April 23, 2009, in Washington, DC.

Global Working Group Updates

Chairman Capizzi provided an overview of the activities of the other four Global working groups and referred the attendees to the working group summaries included in the meeting folder. The following is a synopsis of each working group's activities.

Global Infrastructure/Standards Working Group (GISWG)

The Global Infrastructure/Standards Working Group (GISWG) is currently focusing on expanding the suite of JRA products with the following technical standards and guidelines documents in support of the Global Justice Reference Architecture (JRA).

- JRA Frequently Asked Questions (FAQs) for Executives
- JRA Specification Version 1.7
- Guidelines for Identifying and Designing Services
- Execution Context Guidelines
- WS SIP Version 1.2
- Service Specification Package
- Statement of Participation

The GISWG Services Task Team (STT) effort, which is an offshoot of the GISWG JRA effort that began in 2008, is producing reference service specifications for fusion centers, biometrics exchanges, and other future services to be determined. These specifications will further show alignment with national strategies and projects.

The associated Services Task Team will continue working with practitioners and industry to define new JRA reference services for justice agencies to use as starting points. Also, the JRA will be included in a Standard Global Package of products to be formally defined as an integrated and standardized collection of standards, guidelines, and best practices that vendors and justice agencies can use.

Criminal Intelligence Coordination Council (CICC)/Global Intelligence Working Group (GIWG)

Security and Access: Work collaboratively with the Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (DHS), and other federal partners to provide access to applicable databases for appropriate fusion center personnel.

Baseline Capabilities: Continue to vet appendices for the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, including the Fire Service appendix and a Public Health Sector appendix.

Tips and Leads: The GIWG Privacy Committee is finalizing the updated "Tips and Leads Issue Paper," which incorporates the Nationwide SAR Initiative and best practices from various states on addressing the handling of tips and leads information with law enforcement agencies.

Training and Technical Assistance: Continue to work with the DHS/DOJ Fusion Process Training and Technical Assistance Program and Services in reviewing new services and deliveries for fusion center personnel. Also, work collaboratively with the Law Enforcement Intelligence Unit (LEIU) and International Association of Law Enforcement Intelligence Analysts (IALEIA) in the review and advocacy of front-line officer training that focuses on criminal intelligence.

Outreach: Work collaboratively with the National Fusion Center Coordination Group (NFCCG) in the development of a strategy for fusion center outreach efforts to local, state, and tribal law enforcement and homeland security agencies.

Gang-Related: Continue support of the Gang Intelligence Strategy Committee and the development of its initiatives, including the development of recommendations for law enforcement agencies addressing border/drug crime gang-related activities.

Global Outreach Working Group (GOWG)

Communication and outreach is a standing concern for all organizations, and the Global Advisory Committee (and efforts of its Outreach Working Group) is not unique in this regard. With the advent of a new administration (and people who may be unfamiliar with Global's good work), it became evident that a concise, yet informative outreach deliverable needed to be created to meet the particular challenges and opportunities of a new audience, "fresh eyes," and the ongoing push for institutionalized funding for the Initiative. To that end, Global Outreach Working Group members have recently applied their talents toward creation of "transition" materials, such as the enclosed *Global Briefing Booklet* in the GPIQWG meeting folders. This resource contains an Initiative overview; a listing of GAC agency and representative membership, featured resources, and efforts; the *Global Resolution* (unanimously endorsed at the fall 2008 GAC meeting); and, in the introductory letter from GAC Chairman Boehmer, specific ways in which the Global Initiative is **already meeting top priorities of the new administration** (as outlined on www.change.gov, now closed since completion of the administration's transition). GPIQWG members are encouraged to read Chairman Boehmer's letter (pp. 2–3) as well as the Global overview on page 6; this revised "Global Card" text now includes a "Bottom Line" section listing four key bullets to help communicate the value of the Initiative in the proverbial "elevator" setting—a few minutes, the top points. The Briefing Booklet is posted on the Global and Office of Justice Programs (OJP) Information Technology (IT) Initiatives front Web pages (www.it.ojp.gov), and additional copies are available in hard copy from Global staff.

Because of the current lean funding, the Outreach Working Group is modifying its operating procedures toward a tiger team approach: assembling ad hoc groups from within the Outreach Working Group membership to tackle specific tasks as they arise. By agreement at the beginning-of-year GAC leadership meeting, limited funds are being prioritized for pilot and implementation projects, such as automation of privacy policies as specified in Global's *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework* (a specification resulting from joint expertise of GPIQWG and Global Security Working Group members; this resource is available on the Global Web site and is a key component of the Global Justice Reference Architecture).

Global Security Working Group (GSWG)

The Global Security Working Group (GSWG) is developing documentation for Global Federated Identity and Privilege Management (GFIPM) implementers. Current products include the GFIPM Operational Policies and Procedures Guidelines and the GFIPM Governance Guidelines. The GFIPM Delivery Team is integrating lessons learned from pilots and operational projects that are under way in Los Angeles County, Pennsylvania, Nebraska, Alabama, Kansas, and Wyoming. Participants include the FBI, DHS, JNET, RISS, and the CONNECT project.

GSWG plans to follow up on the Technical Privacy Policy Framework with pilot projects that will leverage the recommendations from the report *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework*. The GSWG is seeking practitioners who would like to pilot the framework within their organizations and who would like to be active participants on the team.

DOJ/DHS Privacy Partnership

Ms. Ayn Crawley, Director, Civil Liberties Institute, Office for Civil Rights and Civil Liberties, U.S. Department of Homeland Security (DHS), provided an overview of the DHS/DOJ/IIR collaboration effort to provide training and resources to fusion centers on privacy, civil rights, and civil liberties. These organizations have been working with state and local agencies to provide training on civil rights and civil liberties (CR/CL) to fusion centers. The DHS Civil Rights Office handles broader issues and deals with all of the components of the public, 508 compliance, etc. The DHS Privacy Office looks at a variety of policy pieces DHS puts out and advises the Secretary of DHS on a broad range of CR/CL issues. A few years ago, Congress amended the DHS directive to create a balance between CR/CL issues and security issues. We provide training to fusion centers, working with DOJ and IIR. One part of the training endeavor is the Privacy, Civil Rights, and Civil Liberties Web portal, www.it.ojp.gov/privacyliberty. Second is the actual training delivery to fusion centers. We are hoping to complete at least six to eight trainings for fusion centers this year. Our first will be in Maryland, a three-part effort in conjunction with BJA and IIR. Our final goal is to train the trainers so that every fusion center around the country can leverage the expertise of those who hold the privacy officer role in their centers and provide them with tools/training products to help them train their own staff/centers.

The Web portal, www.it.ojp.gov/privacyliberty, is anticipated to go live on Tuesday, March 31, 2009. It is housed on the OJP Information Technology (IT) Initiatives Web site, which will include a Privacy and Civil Liberties tab. This site will house topical information, news, state information, training resources, a training calendar, a film library for training films, authorities and guidance, and more. Where possible, it links to other resources. There are also statutes/general provisions, amendments, and commentary. There is a section on policy guidance and standards, including Global materials and those published by other agencies. One goal is to provide a clickable map to show which state fusion centers have privacy policies, with links to their privacy policies once finalized and approved for publishing on the Web. Finally, there will be a password-protected area for fusion centers and authorized users for sensitive information. The goal is a single point of access for fusion centers to support our training endeavor.

The following issues/questions were raised regarding the fusion center privacy policy development efforts:

- The Maryland Dashboard provides law enforcement officers with information provided by fusion centers. What privacy governs this type of sharing?
- Do fusion center products apply to tribal nation fusion centers? Ms. Crawley said that DHS is beginning to focus on this issue to uncover whether tribal centers are using these products and to determine what kind of assistance they may need. Chairman Capizzi stated that GPIQWG had requested BJA's assistance in selecting an appropriate tribal representative who would represent as many as possible, if not all, of the tribal nations. This has been the roadblock to appointing an individual. Not all technical assistance providers for tribal nations are viewed by all tribal nations as representing their tribes. Ms. Crawley was curious as to whether this group would consider exploring a product that might focus on specialized issues around working with tribes in the information sharing environment regarding privacy. Mr. Wicklund stated that there is a current solicitation from BJA on information sharing for tribal agencies. Mr. Randall Wickline stated that he believes there is tribal representation on the FBI Criminal Justice Information Services (CJIS) Advisory Board. Mr. MacLellan also said that he thinks there is tribal representation in NCJA. Ms. Tammy Woodhams said that she would talk with Mr. Cabell Cropper to find out who their representative is.

Ms. Crawley has asked the group to provide feedback on the future plans for the Web portal and to suggest additional topics.

Action Item: Ms. Crawley said that she will send out an e-mail to members containing a link to the site to request their feedback and suggestions for inclusion.

GPIQWG Success Stories

Vice Chairman Stevenson reminded the attendees of GPIQWG's goal to collect success stories. He referred the group to the fusion center privacy delivery synopsis, as well as to the fusion center suspicious activity reporting delivery synopsis, contained in the meeting folders for further information. The fusion centers are, to a certain degree, one of GPIQWG's success stories, since the template used by fusion centers to draft privacy policies was developed using the *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* (Privacy Guide) as its foundational source.

We need to continue to accumulate success stories and add to the white paper that we will eventually send to the Global Outreach Working Group for its distribution to constituents. Every working group has been tasked with collecting success stories by GOWG, which will create a summary to inform the new administration. GPIQWG's 2009 Business Plan also lists GPIQWG's development of a white paper on its product's successes.

Comments/suggestions were as follows:

- We have done a good job with fusion centers but not as well with other justice entities. Just as we are piloting the *Information Quality Self-Assessment Tool* (IQ Tool), should we also pilot the Privacy Guide?
- The National Criminal Justice Association could help by posting a request through the Justice Information Sharing Practitioners (JISP) group to identify local, state, or tribal-level agencies that may be interested.
- The Arizona Criminal Justice Commission (ACJC) reviewed the Privacy Guide, and though there was some pushback to the process, the real success was that it raised issues and the importance of privacy in the agency.

Mr. Stevenson stated, "What I am hearing around the table is that we do not readily know of other local or state agencies that have used the Privacy Guide." Mr. Wicklund expressed that it would be helpful to have a one-paragraph summary on the importance of developing privacy policies to send out in a mass e-mail. Chairman Capizzi emphasized that GPIQWG needs to continue its effort in collecting success stories.

Action Item: Ms. Woodhams will get with Ms. Erin Lee, NGA, to ensure that the listserv posting, which occurred this week, captures this group's request for awareness of the Privacy Guide, use of the Privacy Guide, and its feedback on its development of privacy policies using the Guide.

Action Item: Mr. Stevenson requested that the members provide a write-up on success stories and asked each member to think more broadly about what a success story is. Success stories will be sent to IIR by April 8, 2009.

Information Quality Self-Assessment Tool Pilots

Several conference calls were held among Chairman Capizzi; Ms. Erin Kenneally, eLCHEMY, Inc.; Mr. Stevenson; and IIR staff to discuss how best to vet this tool. One issue we addressed from a pilot agency was how best to limit the assessment to one particular justice event and how to focus the tool on that one event. This pilot agency narrowed the data choice down to arrest-based fingerprints in electronic format and indicated that it could not answer the tool's questions unless they were very narrowly based pieces of data. The agency found that the questions were most easily applied to a single data element.

Other feedback from the first two pilots include the following:

- A better explanation in the instructions on the difference between maintenance and use.
- Two-part questions should be avoided because the completed "Yes/No" answer choices could be different for the first and second questions.
- Need to include a standard "N/A" answer choice in addition to the "Yes/No" choices.
- Put a blank on the form to indicate what data is being assessed.

- The directions need to be clarified a little better since there was some confusion on how to use the tool.
- There was some difficulty in determining how to set the confidence levels. Once the agency was able to do this, it was better able to complete the assessment.
- There was concern on whether the results of the assessment tool would be Freedom of Information Action (FOIA) information. This was not completely resolved but may be an issue for other agencies/states. We need to research and pay attention to the FOIA issue because this may be a barrier to agencies interested in completing these assessments. We should deal with this in the instructions, raise the issue that other agencies need to research their specific state laws, and indicate that this may fall within an exemption since it is an internal assessment.

Mr. Wicklund emphasized the need for personal outreach to pilot this tool, stating, “This needs a personal presence to push this product.” He stated that he was able to secure a third pilot agency and that he, Ms. Pate, and Ms. Abernathy met with this agency, which had implemented a fairly sophisticated record management system with courts, probation, and detention facilities, as well as the Department of Human Services. The first thing the agency representative stated was, “I wish we had this when we first developed this system. We could have eliminated a lot of issues from the beginning.” In meeting with this agency, we learned the following:

- Having the *Information Quality Program Guide* along with the tool would help significantly in providing the agency with the information it needs to complete the tool, such as definitions, the selection of IQ dimensions, etc.
- The administrator was present at the meeting, as well as the deputy administrator. It helps to have personal relationships to get people interested in completing this task—having a high-level champion to raise the charge is pivotal.
- Knowing why an agency should use this tool is key.
- The agency looked at the different dimensions and the information life cycle description and thought it was a good framework. This tool gave agency staff a great deal of relief that they could choose one piece of data and complete an assessment.

Tomorrow, Ms. Steketee and Mr. Stevenson will be working on the Guide to see whether it is close enough to completion to present to the GAC. All of the pilot recommendations on the tool will be discussed further in the breakout session.

The meeting was adjourned for lunch at 12:15 p.m. and reconvened at 1:45 p.m.

Information Quality Program Guide

The latest draft of the *Information Quality Program Guide* was distributed to this group by e-mail. A drafting session had been held among Ms. Jeanette Plante, Office of Records Management Policy, Justice Management Division, DOJ; Ms. Steketee; and Ms. Abernathy on December 17, 2008, and the Guide has been revised further since that time. The purpose of this product is to educate readers on IQ dimensions, the IQ assessment, and the overall IQ program that an agency should implement within its organization. As this draft was completed, it was further simplified and annotated with footnotes.

Mr. Wicklund recommended that the Guide be completed as soon as possible. The GAC has been expecting this product for over a year. Mr. Aumand reiterated that this has been a complicated process and a difficult topic to approach. Judge Capizzi stated that we are very close to completion and that we will continue the conversation in a breakout at tomorrow’s meeting. Our goal has to be that by the end of tomorrow’s meeting, we have a product, barring proofreading, to recommend to the GESC on April 22, 2009, with the final publication ready for recommendation for GAC approval in October 2009.

National Academy of Sciences Report—*Strengthening Forensic Science in the United States: A Path Forward*

Mr. Steve Siegel, Office of the Denver District Attorney, provided an overview and a slide-show briefing on the background, work, and recommendations that came out of the National Academy of Sciences (NAS) report.

On November 22, 2005, the Science, State, Justice, Commerce, and Related Agencies Appropriations Act of 2006 became law. Under the terms of the statute, the U.S. Congress authorized NAS to conduct a study on forensic science. Over eight sessions, the committee heard expert testimony and deliberated over the information it heard and received. Between meetings, committee members reviewed numerous published materials, studies, and reports related to the forensic science disciplines, engaged in independent research on the subject, and worked on drafts of the final report. Experts who provided testimony included federal agency officials; academics and research scholars; private consultants; federal, state, and local law enforcement officials; scientists; medical examiners; a coroner; crime laboratory officials from the public and private sectors; independent investigators; defense attorneys; forensic science practitioners; and leadership of professional and standard-setting organizations. The testimonial and documentary evidence considered by the committee was detailed, complex, and sometimes controversial. Given this reality, the committee reached a consensus on the most important issues now facing the forensic science community and medical examiner system and issued the report *Strengthening Forensic Science in the United States: A Path Forward*, which asserted 13 recommendations to address these issues.

Mr. Siegel explained that this report was developed based on both old and new forensic science. The areas that were touched on included scientific information, the practical side of the justice system, ethical issues, and legal standards. As a group, we will need to determine where GPIQWG's biometric product exploration fits within these issues and recommendations.

The committee was charged with looking at present and future needs of the forensic community; making recommendations for premier utilization of forensic technologies and identifying potential advances; developing programs for forensic scientist accreditation; and designing and disseminating best practices. The committee had to address the interaction of the forensic community with the homeland security mission; the interoperability of the Automated Fingerprint Information Systems (AFIS); and any additional issues pertaining to forensic science as determined by the committee. Competing interests start to come into play regarding who is authorized/certified to serve in the courtroom and provide scientific evidence. Prequalification before trial is an issue so that there is a choice of court-approved subject-matter experts. This would be contrary to the judicial process as it currently exists.

Mr. Siegel summarized the main concerns of the committee and the concerns from the forensics community.

Main concerns of the committee were as follows:

- Certification of expert forensic professionals and the accreditation of forensic laboratories
- Lack of testing, expertise, creditability, and oversight parallelism in the various disciplines of forensic science
- Evidence interpretation and evaluation disparities
- Admissibility of evidence in court
- Funding for forensic science research—to improve best practices, techniques, bias analysis, ethics, and certification/accreditation

Concerns from the forensics community included the following:

- Fear that inadequate or unequal funding will skew this to one science or another
- Differing modus operandi
- Bureaucracy, responsiveness, and effectiveness from DOJ evaluations and reports
- Bias from pressure and the observer effect
- If the problem of wrongful conviction is dire, why not call for a moratorium?
- Political maneuvering

- Loss of independent thinking
- Very few cases are decided on forensic evidence alone
- Creation of independent labs
- Of the millions of nationwide cases in the last 30 years, how many wrongful convictions were the fault of forensic science?

Report on Biometric Webcasts

Mr. Stevenson spoke about some of the biometric-related Webcasts that have occurred since the December 16, 2008, GPIQWG meeting. It was an educational experience to sit through these Webcasts. Mr. Stevenson requested that those who attended each Webcast provide an overview of these events.

Mr. Siegel talked about the issues that were the focus of the *DNA Evidence and Property Crimes* Webcast. In solving property crimes with DNA, you have to train officers to work with evidence on these types of crime: how to collect evidence, how to get it to the labs, how to inform detectives on the proper questioning of a suspect when there is DNA evidence, etc. We answered these needs by providing training to five particular law enforcement agencies and were able to actually reduce property crimes.

Regarding potential issues around privacy and/or IQ:

- Familial searches are definitely an issue. For example, there are far more property crimes than violent crimes. If you use familial searches in property crimes versus violent crimes, it raises privacy issues.
- What do you do with the DNA samples that are collected from people who are not suspects—are they destroyed? For example, to rule out an individual in a household who is not the burglar/criminal, you have to collect DNA from everyone in the house. Arguably, you have to hold the DNA until the end of the statute of limitations. The question is, What do you do with the profile? Do you store it in a separate database? You need to keep the profile, but do you keep it in a suspect classification? Mr. Siegel stated that while Denver categorizes the information in the system separate from suspects, there really is no standard throughout the country.
- Frequently, juvenile offenders run in a group—one who steals the car and those who ride along. Car thefts leave a lot of biological evidence. Depending on DNA privacy policies (upon arrest or conviction), there is potential for a large database based only on auto thefts versus other crimes.

Mr. MacLellan spoke about the National Governors Association's (NGA's) sponsored Webcast, *The Future of DNA: Collecting DNA in High-Volume Crimes*. It was interesting to hear the debates about the NAS report, but one issue raised was about local law enforcement and local labs having their own private databases in response to the rules promulgated by the CODIS committee with the Federal Bureau of Investigation (FBI). Local law enforcement agencies decided to do it on their own and deal with their own private databases.

GPIQWG Member Biometric Status and Recommendations

Chairman Capizzi stated that, in preparation for our work on biometrics, he had asked several GPIQWG members to go back to their constituents and determine what is being done with biometrics in their jurisdictions. He asked them to bring back issues related to privacy and/or information quality, and recommendations for GPIQWG.

Delaware State Police

Mr. Michael McDonald gave a status on biometrics in the Delaware State Police. In Delaware, samples can be obtained from a person's mouth or blood. Samples are collected from a suspect to compare with samples from an unknown source. A sample is collected by search warrant or voluntary consent. If the known sample is collected by voluntary consent, then it can only be used for the specific crime for which the sample was given. It cannot be submitted to the CODIS database. It is then destroyed. All law enforcement officers in Delaware are trained in collecting DNA samples and have the necessary swab kits to collect DNA when appropriate. All DNA

analysis is conducted by the office of the chief medical examiner. In some instances, a DNA sample may be sent to a private lab for analysis, but usually only when the need is to expedite the results. This is one of the areas of concern—the cost of paying for analysis when it is done to expedite the results. Delaware participates in CODIS, which has strict policies and procedures for submitting samples. We flag a criminal history record if a sample is available in CODIS. Within the last few years, we solved two cold cases using DNA. One concern we have is the cost of expediting samples and having the budget to do that when necessary. For information quality, the timeliness dimension may come into play. We are going to begin using mobile hand-held collection devices for IAFIS to collect fingerprints. These will be used for identification purposes alone, not to collect and store the flat fingerprints collected by the device.

SEARCH, The National Consortium for Justice Information and Statistics

Mr. Eric Johnson provided a status on SEARCH's efforts in biometrics. SEARCH, The National Consortium for Justice Information and Statistics, is a membership organization of state governor appointees supported by a professional staff. SEARCH has a long association with information and identification technologies, including biometric identification technologies, as well as privacy policy development assistance. It has conducted research, authored position papers, provided technical assistance, worked with federal agencies, and hosted conferences focused on biometric use in public safety and, more recently, homeland security applications.

Questions and recommendations for GPIQWG were as follows:

- Would any existing Global product benefit from a chapter or appendix that discusses biometrics—information quality or privacy products?
- Should GPIQWG focus on the applications of one biometric technology or try to develop observations and recommendations that can be applied to several, if not all, biometrics?
- Should GPIQWG focus on the data-quality aspects of biometrics and draw the correlation between quality and privacy?
- Does GPIQWG want to talk about public expectations of how biometrics are deployed by law enforcement and homeland security, with a view toward cautioning that deviance from public expectations can cause disruption of operational capabilities?
- Should a GPIQWG biometrics product include a layperson's description of how each biometric works along with information that examines some of the myths or unrealistic expectations associated with the biometric?

Vermont Department of Public Safety

Mr. Paco Aumand gave a status on the Vermont Department of Public Safety's biometric efforts. The Vermont Department of Public Safety's Division of Criminal Justice Services includes the Vermont Criminal Information Center, Vermont Forensic Laboratory, Governor's Highway Safety Program, Information Technology Section (data), and Radio Communication Services (voice). Mr. Aumand stated, "This was a good endeavor to ask our staff what the issues were that we faced in Vermont." Regarding familial DNA and applicant fingerprint retention, these databases could be a valuable investigative tool to enable the law enforcement community to provide decisive leads in cases that would otherwise go unsolved.

Vermont's concerns with familial DNA searches are as follows:

- Legal and ethical perspective
 - Vermont's statutes are silent on whether to perform these searches.
 - There are no standards in place to measure familial searches against profiles.
- Concerns over the resources needed
 - The lab and law enforcement resources needed to work the large pool of suspects are significant.
 - Labs would have to perform more searches to shorten the suspect lists.
 - Law enforcement would have to investigate the suspect lists.
- Generally, there is concern regarding extended family members of those with genetic profiles in a DNA database who could be subject to a lifetime of "genetic surveillance," which is an erosion of the Fourth Amendment.
 - Proponents argue familial DNA searches will aid in criminal investigations.

- What privacy policy components might be instituted to mitigate the unnecessary “genetic surveillance” argument?
- Familial DNA also plays a role in proving innocence.
- Vermont’s statutes are silent on the retention of applicant fingerprints. The issue is, Should they be retained when the intent of collection is for identification, not investigation? In Vermont, the answer is “No.” This is a public policy that may be influenced through the discussion of privacy policy issues.

Latent fingerprint identifications—issues that affect information quality:

- Lack of standards
- Lack of resources
 - Financial
 - Human
 - Fingerprints stored in the tristate AFIS
- Contextual bias

Biometric concerns in Vermont

- Familial DNA
 - Privacy and information quality concerns
 - No statutory guidance and no national standards are in place for searching the DNA database.
- Applicant fingerprint retention
 - Privacy concern
 - There is no statutory guidance or privacy policy in place that dictates collection purposes and usage.
- Latent fingerprint identification
 - Information quality concern.

U.S. Department of Homeland Security (DHS) Biometric Efforts

Ms. Crawley provided a status on DHS’ biometric efforts. We have a program focused on biometrics and the issues/concerns that it raises. We have a new civil liberties assessment (CLA) and a privacy impact assessment (PIA). The PIA is available on the Web, although the CLA is not available at this time.

The eVERIFY program represents fundamental rights (e.g., right to work, right to travel). It is an Internet-based system that is voluntary, using the required I-9 form and identification, and matches information against that found in the immigration database and the social security databases. Within three to five seconds of receiving a query, the program provides a response that informs the employer whether there is a match. If there is no match, there is a letter of nonconformance indicating such. The social security system has the oldest series of databases in the country but experiences a variety of problems. For example, if an individual gets married and changes his or her name, there is a potential for the system to contain two or more records for that person. A photo screening tool is now being added in eVERIFY to match the photo on an individual’s immigration card. It is under way but has received a lot of criticism. One of the challenges of using this screening tool is that individuals have only eight days to rectify any discrepancies. Such problems reduce the tool’s potential.

DHS is looking at a number of programs (e.g., a hostile intent program, the use of mobile biometric data units, and a violent intent modeling program). DHS is also trying to ensure that there is no cultural bias in these screening programs. One example with the US-VISIT program is the quality of the data and databases against which checks are run. The bigger the database, the more potential there is for errors. In terms of the PIA, the department has been sensitive to the concerns that have been raised, but a lot of the problems arise from technologies that are not fully understood or potential issues that come into play once users start sharing.

***Global Justice Information Sharing Initiative (Global)
Global Privacy and Information Quality Working Group (GPIQWG) Meeting***

Salt Lake City, Utah
March 26–27, 2009

March 27, 2009—Meeting Summary

Introduction and Charge for the Day

Chairman Capizzi reconvened the GPIQWG meeting at 8:30 a.m. and welcomed everyone back to the second day. He reviewed the goals for the meeting. We need to accomplish two things today: to complete the final draft of the *Information Quality Program Guide* and to come to a consensus on the direction we want to take with biometrics.

Chair

The Honorable Anthony Capizzi
*Montgomery County, Ohio, Juvenile Court
National Council of Juvenile and
Family Court Judges*

Vice Chair

Mr. Phil Stevenson
Arizona Criminal Justice Commission

Mr. Francis (Paco) X. Aumand, III
Vermont Department of Public Safety

Ms. Cindy Southworth
National Network to End Domestic Violence

Ms. Ayn H. Crawley
*Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security*

Ms. Martha W. Steketee
Independent Consultant

Lieutenant Kathleen DeGrasse
Illinois State Police

Randall Wickline
*Criminal Justice Information Services Division
Federal Bureau of Investigation*

Mr. Eric Johnson
*SEARCH, The National Consortium for Justice
Information and Statistics*

Mr. Carl Wicklund, GAC Vice Chair
American Probation and Parole Association

Erin Kenneally, Esquire
eLCHEMY, Incorporated

Ms. Tammy Woodhams
National Criminal Justice Association

Mr. Dominic LaMar
*Space and Naval Warfare Systems Center
(SPAWAR), U.S. Navy*

Guest Observer
Mr. John Loverude
Advanced Technology Systems, Inc.

Mr. Thomas MacLellan
National Governors Association

Staff
Ms. Christina Abernathy
Institute for Intergovernmental Research

Mr. Michael McDonald
Delaware State Police

Ms. Terri Pate
Institute for Intergovernmental Research

Mr. Steve Siegel
Office of the Denver District Attorney

GPIQWG Biometrics

Chairman Capizzi informed the group that subject-matter experts (SMEs) had been appointed for GPIQWG's biometric resource development. For DNA—Mr. Gregory LaBerge, Director, Crime Laboratory Bureau, Denver Police Department; for facial recognition—Mr. Scott McCallum, System Analyst, Pinellas County, Florida, Sheriff's Office; and for fingerprints—Lieutenant Leo Norton, Los Angeles County, California, Sheriff's Department, Records and Identification Bureau. We are also waiting for appointments from the NIJ Sensors, Surveillance, and Biometric Technologies Center of Excellence as well as an SME from the FBI's Biometric Center of Excellence.

Chairman Capizzi referred the group to the GPIQWG Biometric Exploration Process handout (Appendix A) that contains the bulleted comments, issues, and proposed products identified at the December 16, 2008, GPIQWG meeting. We need to talk about who we think we are making these products for as related to biometrics—a target audience.

Comments and suggestions made were as follows:

Audience

- People have not uniformly thought of biometrics as data. The audience is widespread. Those ultimately responsible for controlling and/or entering this data may be a target audience. A primer on the considerations around this may be useful as a way to connect these individuals to the resources that are available.
- The audience could potentially be the public policymakers who pass laws and view the technologies as part of the whole program (rather than the tools). These policymakers may not have the level of appreciation for what the technologies can produce, but more important, for the resulting privacy issues associated with their use. Guidance for policymakers would be helpful.

Apply Previous Products

- What about using what we have already produced? What about a privacy threshold analysis on biometrics? How does this fit in, and is it something we can do as a group now? Why not apply our current products to this—a document that addresses the intersection between biometrics and privacy?
- GPIQWG's model for product development, which has worked before, should be used here—the introductory short piece and then the follow-up educational guidance product.
- GPIQWG could interpret and distill information that is already out there. We could bring in some of our legacy work on privacy policy and information quality issues—a biometric implementation of previous products.

Biometric Primer

- As we talk about information quality, it is easy to get wrapped up in the technology (the biometric "capture"). It is difficult to separate biometrics from the application. Maybe a primer would be a good place to start to illustrate biometric technologies (a laundry list), categories of use (verify identity, determine identity, etc.), and privacy concerns.
- GPIQWG has spent considerable hours trying to learn about this field. In the public policy arena, there is not nearly as much time spent trying to understand biometrics. It would seem that a misunderstanding of biometrics in the field may raise privacy issues. It may be useful to develop a "go to" place to help individuals understand biometrics.
- GPIQWG should focus on policymakers and legislators to make them aware of what they may be doing with biometrics and remind them about the privacy concerns up-front. The first piece should target those folks and raise awareness. What tends to be available right now is a lot of advocacy pieces rather than an objective viewpoint.

- We could abstract the data and say what it is used for (e.g., when you are collecting data, what and how are you using it, raise the privacy issues with categories at the abstract level, such as Do you keep it or not? or Do you share it or not?). Define the decision processes and associate those with privacy.
- Best practices are listed on www.bioprivacy.org. These pretty much follow the Fair Information Principles (FIPs).

Biometric Issues

- An interesting resource is Bioprivacy.org's Technology Risk Ratings, www.bioprivacy.org/technology_assessment_main.htm, which lists technologies (pros and cons of each) and applies a risk rating. It does not, however, talk about how to mitigate these issues, such as through the development of and adherence to a privacy policy. How do we lead the policymakers to focus on privacy policy to help mitigate some of their privacy concerns?
- We should ask SMEs where the risks (hot spots) are in relation to privacy. Ms. Southworth recommended Melissa Ngo (previous American Civil Liberties Union [ACLU] representative, who has worked in biometrics).
- A lot of the issues are associated with linking biometric information, which poses a huge privacy risk. Clearly, we need to focus on issues in the justice system. Familial searches are a perfect example of how technology takes what we think was in the law and goes beyond to areas that had not previously been considered.
- There might be a need for addressing errors or wrongful biometrics (e.g., planted DNA, false fingerprints). How do you correct identity issues?
- There is an inherent assumption that because biometrics are being used in an investigation, the biometric information is somehow exposed beyond its initial purpose. We need to ensure that officers are aware that this information should not be shared. For example, there should be guidelines on how pictures of a battery victim's bruises should be shared. An issue for us is, What happens when we use the biometric technology outside the criminal justice arena just because we have it? Maybe we can focus on those issues, where people want to take it out of the realm for which it was initially intended. The laws generally address only the criminal justice use of the information. It could even be addressed at the "civil justice" level.

Other Comments

- What does this group have to offer to the discussion of biometrics when there are other groups touching on biometrics, including privacy?
- We could do a resource analysis and uncover the gaps for the justice field.
- Public policymakers made the laws concerning fingerprints and information associated with the fingerprints. Then DNA came along, and they followed the same method. There seems to be a disconnect. Also, there is not much around the other technologies such as iris, facial, etc. Maybe GPIQWG should see where laws have holes and suggest amendments.

Target Audience: The group came to a consensus that the target audience for the first piece is policymakers, boards of trustees, and chief executive officers (CEOs). We need to provide a primer or an executive summary that demonstrates the areas of concern (what they should be aware of) so that they are knowledgeable.

Breakout Sessions

Before the group adjourned into breakouts, Judge Capizzi reminded members of their priorities to work toward finalizing the draft products (the IQ Guide and tool) and to further the biometric discussion in a smaller group setting. The breakout groups were as follows:

Information Quality Self-Assessment Tool Breakout Group**Lead: Erin Kenneally**

Kathleen deGrasse
 Eric Johnson
 Dominic LaMar
 Mike McDonald
 Terri Pate

Information Quality Program Guide Breakout Group**Lead: Phil Stevenson**

Christina Abernathy
 Paco Aumand
 Martha Steketee
 Randall Wickline
 Carl Wicklund

Biometrics Resource Development Breakout Group**Lead: Tony Capizzi**

Ayn Crawley
 John Loverude
 Thomas MacLellan
 Steve Siegel
 Cindy Southworth
 Tammy Woodhams

The groups met in breakout session from 9:45 a.m. to 11:00 a.m.

Breakouts Status Report

Judge Capizzi reconvened the group for the purpose of providing status reports from the breakout groups, soliciting suggestions on future GPIQWG products, and outlining the next steps. The following are reports from the breakout groups:

Information Quality Self-Assessment Tool Breakout Group

Ms. Kenneally reviewed the feedback and consensus on changes in the tool.

- Add a sample header—a sample completed dimension.
- FOIA issue—will be addressed in the introduction to emphasize that this is for your own use, someone might raise the issue, refer to your state statutes and in-house council, etc. The group will provide this language.
- Add an “N/A” option to the “Yes/No” choices.
- Separate rational/confidence columns into two separate columns.
- Confidence to low/medium/high.
- Move first-dimension column into the question column.
- Label at top “What is being assessed,” the name of a person doing this, and a date field.
- Remarks column to change to remarks/notes. Will add directions in Number 10—this is what we mean by remarks and notes.
- Will split two-part questions into separate individual questions.
- Issue about maintenance versus use—we will explain “Maintenance means the static care of the record.”
- In the priorities at the front (instructions), add an explanation that if the dimension or element is complete and there are no recommendations, the priority column may be left blank.
- Standardize all the columns to insert check boxes Y/N, so there will be only two columns for written descriptions.
- Number and bullets with subquestions will renumber (4a, 4b, 4c, etc.).
- Add a priority activities summary section.

Information Quality Program Guide Breakout Group

A conference call will be held on Monday, March 30, 2009, among Ms. Steketee, Mr. Wickline, Ms. Woodhams, Mr. Aumand, Mr. Stevenson, and IIR regarding the flow of the information in the Guide. We resolved nearly all of the highlighted changes/recommendations and believe we will have a draft ready to present to the GESC in April 2009. Mr. Stevenson appreciated those who provided review comments and stated that it truly helped move the Guide to completion.

Biometrics Resource Development Breakout Group

Ms. Southworth led this group and described its priorities. The team came up with four priorities. First, the group will do more issue-spotting between now and the September meeting. We would like to hold a conference call among this breakout group, community advocate representatives, and biometric SMEs to identify primary issues. The way to frame this would be to ask individuals for their top questions regarding privacy and biometrics. We could make a request by personal contact and e-mail, asking them to describe what they consider their top two or three issues. Then, at the September meeting, we could create a short primer listing the types of biometrics and issues to consider. Second, adapt information from IBG's privacy.organization list. Third, look at existing best practices. Finally, the breakout group decided that GPIQWG should focus on the retention issue.

Future GPIQWG Products

Mr. Stevenson requested that the group review the 2009 GPIQWG Business Plan, included in the meeting folders, as a guide to what the group will work on this year. We are already working on completion of the first two priorities (the Guide and the tool), but we need to have a discussion on future IQ resources. One suggestion is a quick reference to the Guide. Mr. Stevenson requested suggestions from the group for other products.

- Expanding delivery mechanisms: There may be a whole set of products, such as DVDs, debates, Webcasts, etc., that we could explore beyond the paper format. Given our role as a Federal Advisory Committee (FAC), we need to be cognizant of this role, but we could explore expansion beyond print. This would need to be brought to the GESC for consideration.
- Mr. Wicklund raised the question, "I wonder if we have done a good enough job with civil liberties." Ms. Crawley stated that part of her role on this group would be to ensure that its development of biometric resources includes adequate protection of civil liberties.
- Another area we need to address is the juvenile justice focus. We are considering adding an Office of Juvenile Justice and Delinquency Prevention (OJJDP) member to the group. We have already made some effort in reviewing existing products and determining their relevancy to juvenile justice. One suggestion may be to e-mail our contact with the Utah Administrative Office of Juvenile Court and ask the court to look at the Privacy Guide from a juvenile justice application standpoint. Mr. Stevenson also suggested that GPIQWG consider juvenile justice applicability when exploring biometric resources. Juvenile privacy laws are different in every state.

Action Item: Judge Capizzi will contact the national council and ask whether a privacy expert on staff could give the council a set of products to evaluate for applicability to juvenile justice.

Next Steps and Closing Remarks

Judge Capizzi thanked members for taking time out of their busy schedules to travel to Salt Lake City, Utah, for this meeting and expressed his sincere appreciation for all of their hard work. He emphasized that GPIQWG needs to elevate its effort in product evaluation to determine whether it is having an impact in the field. This may require longer discussions in the future and possibly the design of a product evaluation format. He encouraged members to continue engaging in GPIQWG product development prior to the next meeting to help move the information-quality series products to completion.

The meeting was adjourned at 11:32 a.m.

Attachment A

GPIQWG Biometric Exploration Process Handout

GPIQWG Biometric Exploration Process

The following were comments and product suggestions made by GPIQWG members at the December 16, 2008 meeting.

General Comments

- Issue inventory: We should do an issue inventory. Before we propose a new product, we ought to have a better feel for what the needs are.
- Panel debate and advocate input:
 - It might be helpful to hear presentations from individuals who have issues with biometrics—how they see this as a risk to privacy and/or information quality. From there, GPIQWG could try to build a business case.
 - It might be helpful to hold a panel discussion with the biometrics presenters we heard from today. Scripted questions could prompt agencies to discuss the issues from the opposite viewpoint so that we can discover which questions can be answered and which cannot.
- Implementation of the end product: As GPIQWG moves forward with this issue, it is important to determine, for the product we create, whether there is an audience or agency that can take this product and implement it. It is not productive to create a resource that no one uses. It has to have value, purpose, and usefulness.
- Subject-matter expertise: We need to integrate more expertise than what we have in our membership; determine what kinds of SMEs would best be able to assist us with developing these resources. A representative from the National Institute for Standards and Technology's (NIST's) Biometrics Consortium (<http://www.biometrics.org/>) might be helpful—first-level people who are engaging the technology. GPIQWG needs to bring in practitioners and scientists who have hands-on experience in biometrics—those who are best suited to advise on needed resources and to help develop them.

Proposed Products

- Online resource: Based on the biometrics resource packet, an online, easy-to-access resource on biometrics may be an option.
- Business model/good practices: Develop a business model that justifies why the agency is collecting the biometric information in the first place; why it is being stored; and how the agency gets rid of it. In other words—good practices. We need to bring in people who are raising those questions.
- White paper clarifying biometrics as digital information: Regardless of the specialty, the product in the end is digital information. GPIQWG could draft a short paper identifying what makes biometric information different in digital form from other digital personally identifiable information (PII) and emphasize that agencies have to protect it in the same way as PII (for example, access issues). What happens if the information is kept too long? What happens when the information degrades? A two- or three-page paper might be useful to reinforce the notion that no matter what the differences are, there are still standards associated with any digital information.

Once digitized, biometric information becomes points (for example, points along a face or points of a fingerprint) and loses some of its personally identifiable implications. The system cannot reconstruct a face from points; this results in a loss of ability to identify an individual because of digital characteristics. Agencies may have access to the digital information but may not have access to the sample.

- Retention policies:
 - Biometric retention of DNA samples in criminal justice is a legislative decision. The Federal Bureau of Investigation's (FBI's) Combined DNA Index System (CODIS),

www.fbi.gov/hq/lab/html/codis1.htm, is a highly regulated database that probably does not require this group's intervention. The alternative may be to develop policy. Applicant fingerprints, for example, are not as regulated as those of convicted individuals.

- Regarding storage, however, the particular law written is how the storage of DNA is handled. Retention policies are needed.
 - GPIQWG should focus on the question, Do you hang onto the information if the person is innocent? and develop rules around retention for those who are not guilty. This may also include those who have been convicted, served time, fulfilled their sentencing obligations, and are now free. Is that information retained forever? The law does not require destruction of the information.
- Expungement standards:
 - It is difficult for some to hire a lawyer to get their records expunged. The question is, is expungement a policy or a process? The answer is both. The problem is that there has to be a record of the expungement. Expungement of paper information is obliteration. What does expungement mean electronically? Who has custody of the record? The record has to be removed from all of the systems in which it resides. Expungement is a huge issue that needs to be explored further.
 - In referencing Ms. Plante's mention of expungement (definition and standards), there is already a need for standards advice. GPIQWG might want to focus on the bookends of the spectrum, such as standards for the initial collection (and auditing), to help minimize the difficulty of expungement and destruction at the other end. Questions are, Do we have the right to collect the biometric information in the first place? and Should collection be minimized at the front end?
 - Privacy policy:
 - Right now, we are at the crest of a wave of DNA use. Starting with a privacy policy is the best place to begin, and making a statement about this would be a good start for GPIQWG.
 - Biometrics is primarily a tool used by law enforcement. Policies are needed to help agencies work in this environment and do the right things in the collection and use of the information. While there are custody biometrics, DMV photos, surveillance cameras, etc., these are just tools. It is still necessary for law enforcement officers to go into the field and investigate. Can we establish policies that are helpful and acceptable to them?
 - Resources by modality: Scars, marks, and tattoos are biometric modalities considered in Code of Federal Regulations (CFR), Title 28—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23 (28 CFR Part 23). GPIQWG could explore development of resources for these modalities.
 - Informational awareness publication:
 - GPIQWG has an opportunity to inform an audience as a first step—to open up a dialogue to advise policymakers to set policy (or legislation). We could demonstrate the positives/negatives of biometrics from the privacy perspective.
 - When developing a policy, it is reasonable to answer a list of questions while developing the policy (for example, What does your state say about XYZ? or What is your policy on retention of those proven innocent?). GPIQWG could establish a list of questions with "Yes/No" arguments (pros and cons).
 - There are privacy implications for nonadjudicated offenders. Identifying issues or raising questions may be a good beginning. For example, very few rapes are stranger rapes, but the reason offenders are not convicted has to do with consent.

Attachment B

**Global Privacy and Information Quality Working Group
March 26–27, 2009
Meeting Agenda**

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page One

Arizona Banquet Room

March 26, 2009

8:00 a.m. – 8:30 a.m.

Beverage Service

8:30 a.m. – 9:00 a.m.

Welcoming Remarks and Introductions

*The Honorable Anthony Capizzi, GPIQWG Chair and Judge,
Montgomery County, Ohio, Juvenile Court*

Anticipated Discussion Topics

- ◆ Agenda overview
- ◆ December 16, 2008, GPIQWG draft meeting summary
- ◆ Calls to GPIQWG members
- ◆ Changes in leadership
- ◆ Cost reductions
- ◆ March 16, 2009, Privacy Activities Coordination Meeting, Washington, DC
- ◆ Next GPIQWG meeting

9:00 a.m. – 9:30 a.m.

Global Updates

*Mr. Carl Wicklund, GAC Vice Chair and Executive Director,
American Probation and Parole Association*

Anticipated Discussion Topics

- ◆ January 27–28, 2009, GESC planning meeting
 - Funding for Global
 - 2009 GPIQWG Business Plan—*Judge Capizzi*
- ◆ Global Briefing Booklet
 - Response to priorities for new administration
 - Privacy as a priority
 - Global card (“Elevator Speech”)
- ◆ Global resolution
- ◆ December 9, 2008, Transition Team meeting
- ◆ March 10–12, 2009, National Fusion Center Conference
- ◆ Upcoming GAC dates: GESC, April 22, 2009, and GAC, April 23, 2009, at the Westin Tysons Corner Hotel in Falls Church, Virginia

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page Two

Arizona Banquet Room

March 26, 2009

- 9:30 a.m. – 10:00 a.m. **Global Working Group Updates**
Judge Capizzi
- Working Groups
- ◆ Global Outreach Working Group (GOWG)
 - ◆ Global Intelligence Working Group (GIWG)
 - ◆ Global Security Working Group (GSWG)
 - ◆ Global Infrastructure/Standards Working Group (GISWG)
- 10:00 a.m. – 10:30 a.m. **DOJ/DHS Privacy Partnership**
Ms. Ayn H. Crawley, Director, Civil Liberties Institute, Office for Civil Rights and Civil Liberties, U.S. Department of Homeland Security (DHS)
- Anticipated Discussion Topics
- ◆ March 16, 2009, Privacy Activities Coordination Meeting, Washington, DC
 - ◆ Status of the Privacy and Civil Liberties Portal
- 10:30 a.m. – 10:45 a.m. **Break**
- 10:45 a.m. – 11:15 a.m. **GPIQWG Success Stories**
Mr. Phil Stevenson, GPIQWG Vice Chair and Director, Statistical Analysis Center, Arizona Criminal Justice Commission
- Anticipated Discussion Topics
- ◆ Fusion center privacy and suspicious activity reporting (SAR) policies
 - ◆ Criminal justice agency privacy policy development
 - ◆ GPIQWG product evaluation strategy
- 11:15 a.m. – 12:15 p.m. **Information Quality Self-Assessment Tool Pilots**
Judge Capizzi
- Anticipated Discussion Topics
- ◆ Illinois State Police—*Lieutenant Kathleen deGrasse, Privacy Officer, Illinois State Police*
 - ◆ Montgomery County Juvenile Court Probation Department—*Judge Capizzi*
 - ◆ Utah Administrative Office of the Juvenile Court—*Mr. Wicklund*
 - ◆ Suggestions for revisions based on pilot feedback

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page Three

Arizona Banquet Room

March 26, 2009

- 12:15 p.m. – 1:45 p.m. *Lunch (on your own)*
- 1:45 p.m. – 2:15 p.m. **Information Quality Program Guide**
Ms. Martha Steketee, Independent Consultant
- Anticipated Discussion Topics
- ◆ Status of guide
 - ◆ Review of recent revisions
 - ◆ Incorporation of the *IQ Self-Assessment Tool* (to include pilot feedback)
 - ◆ Plans for fall GAC review and approval
- 2:15 p.m. – 2:45 p.m. **National Academy of Sciences Report—*Strengthening Forensic Science in the United States: A Path Forward***
Mr. Steve Siegel, Director, Special Programs Unit, Office of the Denver District Attorney
- Anticipated Discussion Topics
- ◆ Executive summary
 - ◆ Implications to biometric technology
- 2:45 p.m. – 3:00 p.m. *Break*
- 3:00 p.m. – 3:30 p.m. **Report on Biometric Webcasts**
Mr. Stevenson
- Anticipated Discussion Topics
- ◆ DNA Evidence and Property Crimes
 - ◆ Forensic Failure: Case Reopened
 - ◆ The Future of DNA: Collecting DNA in High-Volume Crimes

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page Four

Arizona Banquet Room

March 26, 2009

3:30 p.m. – 4:45 p.m.

GPIQWG Member Biometric Status and Recommendations

Judge Capizzi

Organizational Status Reports on Biometrics and GPIQWG Recommendations

- ◆ *Mr. Michael McDonald, Director, Information Technology and Communications, Delaware State Police*
- ◆ *Mr. Eric Johnson, SEARCH, The National Consortium for Justice Information and Statistics*
- ◆ *Mr. Paco Aumand, Director, Division of Criminal Justice Services, Vermont Department of Public Safety*
- ◆ *Ms. Tammy Woodhams, Senior Staff Associate, National Criminal Justice Association*
- ◆ *Ms. Crawley, Office for Civil Rights and Civil Liberties, DHS*
- ◆ *Ms. Susan Laniewski, Vice President, Justice Programs, Crossflo Systems, Inc.*

4:45 p.m. – 5:00 p.m.

Next Steps and Closing Remarks

Judge Capizzi

Anticipated Discussion Topics

- ◆ Review of today's action items/writing assignments
- ◆ Setting deadlines
- ◆ Plan for the following day's GPIQWG meeting

5:00 p.m.

Adjournment



Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page Five

Arizona Banquet Room

March 27, 2009

8:00 a.m. – 8:30 a.m.

Beverage Service

8:30 a.m. – 8:45 a.m.

Introduction and Charge for the Day

Judge Capizzi

Anticipated Discussion Topics

- ◆ Charge to the group

8:45 a.m. – 9:45 a.m.

GPIQWG Biometrics

Judge Capizzi

Anticipated Discussion Topics

- ◆ Subject-matter experts
 - DNA—Mr. Gregory LaBerge, Director, Crime Laboratory Bureau, Denver Police Department
 - Facial Recognition—Mr. Scott McCallum, System Analyst, Pinellas County, Florida, Sheriff's Office
 - Fingerprints—Lieutenant Leo Norton, Los Angeles County, California, Sheriff's Department, Records and Identification Bureau
 - NIJ Sensors, Surveillance, and Biometric Technologies Center of Excellence—TBD
 - FBI Biometric Center of Excellence—TBD
- ◆ Realistic issues for GPIQWG focus
- ◆ Target audience
- ◆ Review of suggested biometric products from 12/16/08 GPIQWG meeting and from 3/26/09 GPIQWG Member Biometric Recommendations
- ◆ Next steps for GPIQWG biometric development

9:45 a.m. – 10:45 a.m.

Breakout Sessions

Judge Capizzi

Breakout Discussion Topics

- ◆ *IQ Self-Assessment Tool* revisions from pilot test feedback
- ◆ Biometric resources for GPIQWG development
- ◆ *IQ Program Guide* breakout

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Little America Hotel
500 South Main Street
Salt Lake City, UT 84101
(800) 437-5288



United States
Department of Justice

March 26–27, 2009

Agenda—Page Six

Arizona Banquet Room

March 27, 2009

- 10:45 a.m. – 11:00 a.m. **Break**
- 11:00 a.m. – 11:30 a.m. **Status Report From Breakouts**
Judge Capizzi
Status Reports and Next Steps
 - ◆ *IQ Self-Assessment Tool* breakout
 - ◆ Biometric resources for GPIQWG development breakout
 - ◆ *IQ Program Guide* breakout
- 11:30 a.m. – 11:45 a.m. **Future GPIQWG Products**
Mr. Stevenson
Anticipated Discussion Topics
 - ◆ Exploration of new privacy and IQ products
 - ◆ Products for juvenile justice
- 11:45 a.m. – 12:00 Noon **Next Steps and Closing Remarks**
Judge Capizzi
Anticipated Discussion Topics
 - ◆ Next steps
 - ◆ Review of action items and assignment of tasks
- 12:00 Noon **Adjournment**

