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

Information Quality (IQ) Assessment Tool Task Team

Washington, DC

February 27, 2007

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), Information Quality (IQ) Assessment Tool Task Team, convened the meeting at 8:30 a.m. on February 27, 2007, in Washington, DC. Mr. Owen Greenspan, SEARCH, The National Consortium for Justice Information and Statistics, led the meeting in the furtherance of and alignment with the GPIQWG's *Vision* and *Mission Statements*.

Attendees

The following individuals were in attendance:

Mr. Owen Greenspan
SEARCH, The National Consortium for Justice Information and Statistics

Barbara Hurst, Esq.
Rhode Island Office of the Public Defender

Mr. Michael McDonald
Delaware State Police

Jeanette Plante, Esq.
Justice Management Division
U.S. Department of Justice

Gerard Ramker, Ph.D.
Bureau of Justice Statistics
U.S. Department of Justice

Mr. Carl Wicklund, GPIQWG Chair
American Probation and Parole Association

Lieutenant Don Grimwood
Ohio State Highway Patrol

Erin Kenneally, Esq.
eLCHEMY, Incorporated

Mr. Mark Motivans
Bureau of Justice Statistics
U.S. Department of Justice

Ms. Barbara Pollitt
Delaware State Police

Ms. Robin Stark
Criminal Justice Information Services Division
Federal Bureau of Investigation

Staff

Ms. Christina Abernathy
Institute for Intergovernmental Research

Meeting Overview and Goals

Mr. Owen Greenspan welcomed the members of the new task team and gave an overview of the meeting agenda (refer to Appendix A), which included the following key topics:

- Overview of Established Work
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Information Quality Evaluation
- Delaware State Police—Auditing Methods
- Ohio State Highway Patrol—Law Enforcement Automated Data System (LEADS)
- IQ Dimensions and IQ Assessment Tool Outline

Mr. Greenspan asked the team to individually come up with seven terms to describe what information quality meant to them and then asked the members to introduce themselves and to share their IQ terms. The goal of the exercise was to determine, based on each member's field of expertise, the terms that describe IQ that are most common to all of the justice arenas represented by the task team and to discover those that may be less common.

Mr. Greenspan put forth the IQ Assessment Tool Task Team's charge to develop a self-assessment tool for justice and posed a question to the group: Is this tool for just one discipline, one product, or multiple tools? He further emphasized that this group has a unique and unusual opportunity to expand the definition of information quality as it applies to justice entities. In the post-9/11 world, we are collecting information more broadly and sharing information more than before. This is a first step towards a change in the way the justice community operates.

GPIQWG Chairman Carl Wicklund provided the group with a brief overview of the Global Initiative, the associations Global represents, and the relationship between BJA and Global. He described the five working groups and their interrelation to one another and talked about the privacy and information quality products developed by GPIQWG.

Overview of Established Work

Mr. Greenspan briefly reviewed the collection of IQ products/works that were provided as read-aheads, not for the purpose of an in-depth understanding of what each agency does on a day-to-day basis but rather as a general overview and as helpful tools to be used in the IQ Assessment Tool development process. These included the GPIQWG's IQ fact sheet entitled *Information Quality: The Foundation for Justice Decision Making*; "The Multiple Dimensions of Information Quality"—excerpt from *Introduction to Information Quality,* a Massachusetts Institute of Technology Information Quality publication by Fisher, Lauria, Chengalur-Smith, and Wang; and the GPIQWG IQ Assessment Tool draft outline developed by the IQ Assessment Tool breakout group at the October 4, 2006, GPIQWG meeting.

During the general discussion of the work established to date, the following key points were made:

- Mr. Michael McDonald, Delaware State Police, emphasized the importance of training and education and their inclusion in this endeavor. Mr. McDonald described Delaware's development of an automated crash system, yet the

focus on IQ is currently lacking, since the point of recording crash data is for insurance purposes rather than potential law enforcement use.

- Ms. Erin Kenneally, eLCHEMY, Incorporated, put forward the concept that users have a tendency to believe that computers are always right and that once data is in the database, it is out of users' hands. This presents a challenge in training and, broadly, in the IQ arena to understand and raise awareness to users of what the computer software is actually doing "to" and "with" the source data.

- Ms. Barbara Hurst, Rhode Island Office of the Public Defender, proposed that the relationship between a computer application and the user is a two-way street. There must be training on the application, but equally as important is the focus on the flexibility of the application to change for the user. Applications that are too rigid promote inaccurate data or data that is insufficiently attached to each other; for example, making certain fields required when, in actuality, the information is not available (therefore, information may be made up).

- Ms. Jeanette Plante, DOJ, charged the group with deciding exactly what we are assessing. The outline developed at the October 4, 2006, GPIQWG meeting shows that we are assessing the output of information, but we need to discuss the information life cycle as a whole: 1) creation/capture, 2) use/maintenance of the information, and 3) disposition (standards for timeliness/accuracy/expungement). This would provide a simple and clean way to categorize the information process. Ms. Plante emphasized that the outline addressed one piece of the information life cycle. No matter what tools this team creates, it is important to look at those larger categories and organize them into these stages (and roles). A diagram of the information life cycle is provided below:

Information Life Cycle Phases:	Components of Each Phase		
	Program Management	Policies and Procedures	Information Technology (IT)
1. Creation/Capture			
2. Use and Maintenance			
3. Disposition			

Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Information Quality Evaluation

Ms. Robin Stark, FBI CJIS, gave a brief presentation on CJIS audits and described the systems that the FBI manages. Ms. Stark emphasized CJIS's charge to evaluate and ensure the integrity and security of the data in CJIS systems. A CJIS audit is, essentially, education and training (here is what is wrong and here is help on how to fix it). Ms. Stark stated that the

audits depended on the source documentation and how good the capture of the information is. Policies and procedures are in place for how the audit is performed, yet CJIS has limited resources to audit all data. Instead, it audits via random selection of agencies that have access to the FBI databases. To determine the audits, CJIS depends on numerous factors (e.g., reports of potential misuse or past problems). One police department in Ohio is always audited because it is the biggest agency, with the largest volume of users. CJIS samples the contributors and users of the agency and reviews their policies and their adherence to those policies. CJIS audits a mixture of agencies within a particular jurisdiction. CJIS also specifically reviews the records agencies contribute to the national databases (National Crime Information Center [NCIC], Uniform Crime Reporting [UCR] Program, National Instant Criminal Background Check System [NICS], Integrated Automated Fingerprint Identification System [IAFIS], and technical security) and assesses validity, accuracy, completeness, and timeliness of that contributed data.

The task team discussion questions were as follows:

Question: Where do you stop in an audit? Do you treat one record as representative of multiple files? For example, an arrest record may be in several national CJIS files, such as the National Incident-Based Reporting System (NIBRS) or NCIC.
Answer: There is no linkage evaluation of the same files within multiple CJIS systems.

Question: Do you prioritize data elements, comparing every piece of information in NCIC with others?
Answer: CJIS is most concerned with searchable fields that are most frequently used and that are more critical to law enforcement on a daily basis, but CJIS does not have the resources to look at all fields (optional fields or less searchable fields).

Question: Are you looking at the information technology (IT) controls in the system (e.g., authentication)?
Answer: Yes, there is a separate audit for those processes. CJIS ensures that agencies have all procedures in place that align with CJIS security policies.

Question: Are there parameters that are privacy-related in any of the audits with which CJIS is involved?
Answer: With regard to sensitive data, CJIS does address the privacy concerns of sensitive data (NCIC files, criminal history).

Question: In terms of selection of the records and number of records to examine, do you know the parameters for how that selection is determined?
Answer: A formula is used to determine this. However, if special circumstances arise in which CJIS needs to deviate from the formula, the justification is described within the audit report.

Question: Is there any coordination between FBI CJIS and the state auditors?
Answer: Yes, CJIS checks with state auditors to confirm whether they have completed their state audits—which generally must be done every two

or three years. States are required to audit every agency that has access to their system.

Question: When agencies are identified, do you audit comprehensively or just a particular task, action, or area?
Answer: It depends on the agency, situation, and whether we know there is a specific misuse or problem.

Question: You audit agencies, but do you audit the systems?
Answer: We audit a mix of both the agency and the access to the national system(s).

Question: Fusion centers do not contribute data but do provide access to the national databases. Does CJIS have any involvement with fusion centers?
Answer: At this time, CJIS does not have that level of involvement with fusion centers since fusion centers do not actually contribute the data or create records. Fusion centers are not subject to the CJIS audit—only the agencies and users who create and contribute the data are subject to CJIS audits.

Question: During IT audits, do you look at system-logging capabilities?
Answer: Yes, CJIS reviews system-logging and password changes in terms of being able to track when the query occurred (mapping).

Question: Do you look at remediation processes for incorrect data?
Answer: Yes, CJIS does look at the remediation in the system. CJIS evaluates user authentication, data security, and access controls.

Question: Do agencies prepare in any way for the audits, such as by doing self-assessments?
Answer: Some of the more proactive agencies prepare and do self-assessments before a CJIS audit. For example, Delaware performs an audit that mirrors the CJIS audit.

Delaware State Police—Auditing Methods

Mr. Michael McDonald and Ms. Barbara Pollitt, Delaware State Police (DSP) Information Technology and Communications department, gave a presentation on DSP audit procedures, records processes, and the methods DSP employs to evaluate information quality. Mr. McDonald and Ms. Pollitt indicated that DSP audit procedures tended to be, proactively, more in-depth than CJIS's audits. Delaware's command center performs all of the entries for its local agencies. DSP has an established main point of contact (POC) at its command center, and everything that is cleared or modified goes through that terminal. Quality control methods are utilized for all data that is added or updated to DSP databases. When corrections are needed, either the command center makes the corrections or instructions are given to the agency to make them. At the end of the month, a report from the command center is mailed to each agency so it can review the results of its IQ evaluations. Second-party reviews are also performed after the POC enters the information, in addition to the audit of that information. Shift

supervisors are provided with a report of errors and review any data that was incorrectly entered.

Mr. McDonald said that DSP would soon begin using a validation tool developed by a firm from Florida (Note: The state of Oklahoma also uses it) to manage the wanted-person file. Any record in NCIC can be pushed to the owner of the data to validate the information. DSP is also going to begin validating local records. A prominent problem is stale or dated information. Delaware will use this tool to validate the records and follow the purge requirements that will be mandated by NCIC for records that are not validated. The user will be given 30-, 60-, or 90-day requirements to validate the data, or DSP will remove those records.

At the local-system level, Delaware performs an automated capture of crime data (with built-in validations for data quality, though not 100 percent comprehensive) with a heavy reliance on supervisors to verify the quality of the information captured. As a result, there are varying degrees of people who look at a record for accuracy. The issue with this method is that as a state police with eight troops, there are eight different ways to do things (for example, correcting a record). There is, however, a group that is responsible for data-quality cleanup if it is known that a record contains inaccurate data. Though currently the group does not audit at the local level, it will begin to do so with the implementation of the automated validation tool. The primary roadblock Delaware faces is resources.

Mr. McDonald described the recent focus on "interpretability" at the national level; for example, a standardized rap sheet or Nlets—The International Justice and Public Safety Information Sharing Network's Collaboration between American Association of Motor Vehicle Administrators [AAMVA] and Nlets for Driver License Exchange [CANDLE] by taking data and putting it in a format that can be interpreted using Extensible Markup Language (XML).

The task team discussion questions were as follows:

Question: Does each state audit Department of Motor Vehicles (DMV) records?
Answer: Not that we are aware of. There are checks on commercial licenses but only upon renewal of commercial records.

Question: Characterize the "why" of the information quality errors that you are encountering. Are there common reasons for the inaccuracies?
Answer: Generally, the cause of errors is human error; most frequently, those are due to missing data or keying in data incorrectly.

Ohio State Highway Patrol—Law Enforcement Automated Data System (LEADS)

Lieutenant Don Grimwood, Ohio State Highway Patrol, gave a PowerPoint presentation on Ohio's Law Enforcement Automated Data System (LEADS). Lieutenant Grimwood stated that Ohio has 88 counties and 700 terminal-entry agencies. The LEADS program is administered by two staff managers, with auditing performed by civilian personnel. LEADS' security auditing department houses three technical-security staff members and four data-security specialists. Auditors have a checkoff list for agencies to follow. (Note: Ms. Stark indicated that FBI CJIS has a 40-page questionnaire for NCIC audits.) Agencies are audited every two years. If it is reported or discovered during an audit that there is misuse of the information in the system, an investigation is performed by a sworn law enforcement officer. There are seven levels of access to data that has undergone a packing process—relaying and filling in the record with

information from records, such as known alias, tattoos, scars, and driver's records. LEADS has its own security policy and disseminates information three ways: via newsletters, technical operational updates, and training. Training and education are provided for the practitioner, operator, and administrator, as well as in-service training and basic operator training.

The biggest difficulty LEADS experiences regarding information quality is at the entry level, which has the highest turnover rate and the lowest pay and requires shift work. Declining budgets cut down on clerical data-entry salaries and staff and thus produce less quality input.

Question: Is there a zero-tolerance policy for errors?
Answer: Not at this time, and the issue seems to be that individuals are not inputting their own information; as such, they are not personally vested. There seem to be two issues: (1) manifestation of errors and (2) enforcement. There may be other agencies that provide incentives that could be useful in the guidance this group develops. Another concept is that audits are viewed as a negative. Auditors are trained to find issues. However, there are no incentives for good audits.

Question: Is there online access to update LEADS records?
Answer: Online access is "read-only," but there are plans to add update functionality.

Question: Do agencies prepare for an audit?
Answer: They do prepare, but the records are pulled by LEADS before the agency is notified. This helps to encourage agencies to check their records continuously rather than just prior to the two-year audit.

Question: To both Mr. Grimwood and Mr. McDonald (Delaware)—Are the results of the audits available to the public?
Answer: Ohio sends the information to administrators, mayors, and commissioners. Delaware provides the information via a report to the terminal agency coordinators.

Question: To both Mr. Grimwood and Mr. McDonald (Delaware)—Has some thought been given to classifying the errors that were gleaned from audits, such as staff ratios and workload measures? How can audit data be linked to other data?
Answer: Ohio—At exit interviews, guidance is provided, as well as suggestions on alternatives to fix the source of the problem. Delaware—With warrants, data could be rolled from crime reports into warrant files so that information is not entered twice. If a warrant is rolled into the NCIC, that data would carry the validation from the crime report. The less frequently data is entered, the higher the level of information quality.

IQ Dimensions and IQ Assessment Tool Outline

Based on the presentations and the group discussion thus far, Mr. Greenspan decided to surpass the agenda item "IQ dimensions/characteristics to quantify" in lieu of pursuing a method for approaching an assessment tool. IQ terminology, itself, may be worked out through the drafting process. Instead, he facilitated a roundtable discussion on the most common types

of queries made—such as a warrant search, criminal history, or driver's license registration—and asked whether that should be the focus of the IQ assessment tool. More needs to be done on the front lines. There are agencies that never have an NCIC audit and are simply unaware of the areas needing improvement. Should recommendations be made for how to sample data for an IQ assessment? Given the most common queries, should this group include those in an assessment? Discussion ensued as follows:

- Auditing Versus Assessment: There is a difference to note between auditing and an assessment. Auditing uses an outsider to determine whether the end product meets a certain criteria, whereas an assessment is internal and is a learning tool that determines problems proactively. Two of the biggest problem areas for IQ are creation/capture and stale data. If a self-assessment determines some problem other than these, then it is even more useful. We need to broaden our view beyond these two areas but also make recommendations on how to improve information.

- Criticality of the Data: We need to focus our assessment on how the data is used and the degree of harm that could result from poor data. For example, if the information in a warrant is inaccurate, it might be more critical. Possibly, rating the criticality of the information and developing an assessment tool based on the critical rating could be beneficial.

- Data Elements: We need to focus on data elements. The initial accuracy at the data-element level is crucial since everything is based upon it. For some data elements, accuracy may be difficult to determine; for example, the spelling of a name. The Florida Department of Law Enforcement (FDLE) did an assessment some time ago and found a high error rate based upon the methodology of the assessment (e.g., a blank field resulted in a bad score). Some data elements are more critical and should be assessed over others that may be less critical. A "form-centric" assessment process is very specific to the data that relates to a specific activity. Consequences should be provided, not just a form.

- What Needs to Be Improved? The Information Life Cycle: The presenters were asked for their perspectives on what they felt would be helpful to improve IQ. We do not ensure IQ only at the creation/capture phase, the use/maintenance phase, or the disposition phase. IQ should be applied to all areas of the information life cycle. We should keep the resources we develop in this type of framework so that users can personally invest in the information they collect, enter, and access. It would be most helpful to begin with the first phase, creation/capture, and try to produce resources such as guidance, checklists, or audit capabilities. It may be something as simple as a program manager's guide for creation/capture. In other words, does the creation/capture vehicle have the following? Has everything been done to minimize IQ errors by providing drop-down boxes for entry fields (minimizing free-text entries)?

  We need to break down the information life cycle phases and the components of each to determine what is most critical to assess. One important recommendation is to emphasize that agencies need to put information quality and the assessment of such in their strategic plan.

If we are still "married" to dimensional scoring of IQ, this would fit within the information life cycle model. We are dealing with a lot of integrated systems that will not go back and reengineer (legacy systems).

- Format of the Exchange: Is subscribing to a common methodology of exchange, such as the Global Justice XML Data Model (Global JXDM), part of this model? The exchange process cannot really be ignored; it is a crucial point for the data that may impact the quality of the information.

Based on the questions raised, Mr. Greenspan proposed spending the remainder of the meeting drafting a list of questions that apply to one very common process, such as fingerprinting or booking, and move forward with a workflow and exchange process. The group decided to pick one dimension of IQ and fit it within the information life cycle matrix and draft questions/assessments to ensure accuracy at each component and phase. This information life cycle framework may be filled out with processes, tools, and questions. We need to craft this product in such a way that we do not dictate a specific solution; rather, we get people asking the right questions that will prompt them to seek out the right solution, even down to instructions as simple as "type more accurately."

For the remainder of the meeting, the attendants began the initial drafting of higher- and lower-level questions an agency might ask according to a specific process, such as fingerprinting or booking. The questions developed are provided below with the intention to grow the list and refine them into a useful self-assessment type of questionnaire.

Information Quality Assessment Questionnaire

High-Level Questions (Information includes fingerprints.)	**Lower-Level Questions** (Information includes booking.)
Do you take steps to ensure that the information captured is accurate, complete, and timely?	How? Automated mechanisms Manual mechanisms
Do you ensure the information is secure?	How? (Secure in transit, in storage) Are data entry personnel screened?
Do you assess the quality of the information?	How routinely do you assess the information?
Do you allow for multiple people to enter the information?	Authorization and authentication

High-Level Questions (Information includes fingerprints.)	**Lower-Level Questions** (Information includes booking.)
Do you specifically assign duties and responsibilities to the people responsible for data capture?	Do you use a turnkey for the booking processes? Is data entry a specialized position?
Do you consider data-entry accuracy and information quality a performance measure? (agency or individual)	
Do you take steps to ensure the captured information entered into your system is accurate, complete, and timely?	
Do you verify?	
How and when do you verify information in the system?	How do you verify information on the arrest report?
Do you verify against some source and what is the source?	
Do you periodically review your collection mechanism for relevance (a business need)?	How do you assess your business case for collecting information?
Do you have a mechanism for correcting information?	
Do you provide training on information quality?	
Do you have a disposition policy?	
Do you have a uniform format for entry? If not, do you have a policy for determining the additional data elements needed?	

High-Level Questions (Information includes fingerprints.)	**Lower-Level Questions** (Information includes booking.)
Do you disseminate data outside of your agency? Do you have written documentation outlining the procedures above?	

Next Steps and Closing Remarks

Mr. Greenspan proposed that at the upcoming half-day IQ Assessment Tool Task Team meeting, to be held in Phoenix, Arizona, March 13, 2007, the group should continue to develop the questionnaire and present a draft to the GPIQWG the following day.

Mr. Greenspan adjourned the meeting at 5:00 p.m.

Appendix A

GPIQWG IQ Assessment Task Team Meeting Agenda

February 27, 2007

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

Information Quality (IQ) Assessment Tool
Task Team Meeting

Embassy Suites Washington, DC Convention Center
900 Tenth Street, NW
Washington, DC ♦ (202) 739-2001

February 27, 2007

Agenda—Page One

Washingtonian Boardroom

8:30 a.m.–8:45 a.m. **Welcoming Remarks and Introductions**

Owen Greenspan, Director, Law and Policy Program, SEARCH, The National Consortium for Justice Information and Statistics

Anticipated Discussion Topic

- *Update on Global and GPIQWG activities*

8:45 a.m.–9:00 a.m. **Meeting Purpose**

Owen Greenspan

Anticipated Discussion Topics

- Explore feasibility of developing an information quality (IQ) self-assessment process for justice agencies.

9:00 a.m.–9:30 a.m. **Overview of Established Work**

Owen Greenspan

Brief overview of the following resources:

- GPIQWG's IQ fact sheet, entitled *Information Quality: The Foundation for Justice Decision Making*
- "The Multiple Dimensions of Information Quality"—Excerpt from *Introduction to Information Quality*, a Massachusetts Institute of Technology Information Quality publication by Fisher, Lauria, Chengalur-Smith, Wang
- GPIQWG IQ Assessment Tool draft outline

9:30 a.m.–10:00 a.m. **FBI CJIS Information Quality Software Demonstration**

Robin Stark, Unit Chief, Audit Unit, Criminal Justice Information Services (CJIS) Division, Federal Bureau of Investigation (FBI)

Anticipated Discussion Topic

- *Methods of Data Quality Control: For Uniform Crime Reporting Programs*, Dr. Samuel Berhanu, Chief, Crime Analysis, Research, and Development Unit, FBI CJIS
- Software demonstration

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

Information Quality (IQ) Assessment Tool
Task Team Meeting

Embassy Suites Washington, DC Convention Center
900 Tenth Street, NW
Washington, DC ♦ (202) 739-2001

February 27, 2007

Agenda—Page Two

Washingtonian Boardroom

10:00 a.m.–10:15 a.m. **Delaware State Police—Auditing Methods**

Michael McDonald, Director, Information Technology and Communications, Delaware State Police

Barbara Pollitt, Systems Auditor, Delaware State Police

Anticipated Discussion Topics
- Insights into Delaware's state auditing processes and procedures

10:15 a.m.–10:30 a.m. ***Break***

10:30 a.m.–10:45 a.m. **Ohio State Highway Patrol—Auditing Methods**

Lieutenant Don Grimwood, Office of Technology and Communication Services, Ohio State Highway Patrol

Anticipated Discussion Topics
- Insights into Ohio's state auditing processes and procedures

10:45 a.m.–11:30 a.m. **Quantifiable IQ Dimensions/Characteristics**

Owen Greenspan

Anticipated Discussion Topics
- How subjective is IQ assessment?
- IQ dimensions/characteristics to quantify
- Methods for quantifying

11:30 a.m.–12:00 Noon **IQ Assessment Tool Outline**

Owen Greenspan

Anticipated Discussion Topics
- Development of one or several assessment tools?
- Tools for single-agency data, data shared between agencies, or both?
- Identify assessment tool components/sections
- GPIQWG IQ Assessment Tool outline

12:00 Noon–1:30 p.m. ***Lunch*** (On Your Own)

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

Information Quality (IQ) Assessment Tool
Task Team Meeting

Embassy Suites Washington, DC Convention Center
900 Tenth Street, NW
Washington, DC ♦ (202) 739-2001

February 27, 2007

Agenda—Page Three

Washingtonian Boardroom

1:30 p.m.–2:45 p.m. **IQ Assessment Tool Breakouts**
Owen Greenspan

Anticipated Discussion Topics
- Designate breakout group members
  - Instrument for single-agency law enforcement data
  - Instrument for data shared between justice agencies in an integrated justice information system
- Charge to breakout groups
- Breakouts develop sample sections/components of IQ Assessment Tool

2:45 p.m.–3:00 p.m. *Break*

3:00 p.m.–4:00 p.m. **IQ Assessment Tool Breakouts (continued)**

4:00 p.m.–4:30 p.m. **IQ Assessment Tool Outline**
Owen Greenspan

Anticipated Discussion Topics
- Breakout group presentations
- Finalize draft outline of IQ Assessment Tool product

4:30 p.m.–5:00 p.m. **Next Steps and Closing Remarks**
Owen Greenspan

Anticipated Discussion Topics
- Review work products to determine utility
- Identify additional assessment tools (e.g., fusion center data, NIEM data)

5:00 p.m. *Adjournment*