Global Justice Information Sharing Initiative

Security Working Group
Meeting Summary

San Diego, California
December 5−6, 2005

Meeting Purpose

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), convened the Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG or "Working Group") on December 5−6, 2005. The meeting purpose was to reorganize, prioritize, and conduct strategic planning with former and new members of the GSWG. An assessment of past accomplishments, near-term projects, and long-range goals were introduced into the planning process in order to develop a new business plan for the GSWG.

Global Security Working Group Participants

Chair Chelle Uecker, Superior Court of California, welcomed the following participants to the meeting in San Diego, California:

Jim Cabral
Integrated Justice Information Systems Institute
Seattle, Washington

Scott Fairholm
National Center for State Courts
Williamsburg, Virginia

Bob Greeves
Bureau of Justice Assistance
Office of Justice Programs
Washington, DC

Robert Hanson
Minnesota Supreme Court
St. Paul, Minnesota

Alan Harbitter
Nortel PEC
Fairfax, Virginia

Monique La Bare
Institute for Intergovernmental Research
Tallahassee, Florida

Tom Kooy
Institute for Intergovernmental Research
Shorewood, Minnesota

Tom Merkle
CapWIN
Greenbelt, Maryland

Terri Pate
Institute for Intergovernmental Research
Tallahassee, Florida

Bill Phillips
Nlets-The International Justice and Public Safety Information Sharing Network
Phoenix, Arizona

Christina Rogers
California Department of Justice
Sacramento, California

John Ruegg
Information Systems Advisory Body
Cerritos, California

Todd Shipley
SEARCH, The National Consortium for Justice Information and Statistics

Richelle Uecker
Superior Court of California Santa Ana, California

Overview

Introductions and Welcoming Remarks

Chair Uecker welcomed the participants and thanked them for attending this important working meeting of the GSWG. She emphasized the importance of the outcome of the meeting and set clear expectations for achieving a draft business plan with outcomes for the Global Executive Steering Committee (GESC) in January. The GESC will be meeting on January 19, 2006, where the GSWG can articulate the objectives and business plans for this session.

Participants were given an opportunity to introduce themselves and speak briefly about their greatest interests or concerns facing the GSWG for the immediate future. These issues ranged from definitions and standards to the need for communication and consistent funding for security technologies.

Chair Uecker welcomed and congratulated the newly accepted vice chair of the GSWG, Mr. John Ruegg, Information Systems Advisory Body. She also noted that although many of the participants present for this meeting have had considerable contact with the Global Security Architecture Committee (GSAC) and other Global groups, only one member from the original GSWG group was present at the meeting and that there are many new members to the working group. Because of illness or other urgent business, Mr. John Powell, National Public Safety Telecommunications Council; Mr. Andy Thiessen, National Telecommunications and Information Administration; and Mr. Joe Hindman, Scottsdale, Arizona, Police Department, were absent.

Chair Uecker reviewed the past and continuing issues of the GSWG and the recent history of this group's progress. She noted that a great deal of transitioning is going on, which presented a "natural" opportunity to determine how to rework the group. A presentation reviewing the past GSWG Business Plan along with the group's mission and vision statements was then given.

Project Updates

Global Security Architecture Committee (GSAC) Update

Ms. Christina Rogers, California Department of Justice, reported the 2005 GSAC accomplishments as follows:

- Consensus on problem/scope statements
- Federated identity and privilege management
  - Definition and approach
- Global federated identity and privilege management initiative and demonstration
  - Participants
  - Schedule/outputs

The Global Federated Identity and Privilege Management (GFIPM) initiative was discussed in detail by Ms. Rogers. The GFIPM initiative will be a demonstration to prove the concept of trusted credentials prior to justice implementation. The initial participants are Criminal Information Sharing Alliance network (CISAnet), Pennsylvania Justice Network (JNET), and the Regional Information Sharing Systems® (RISS). The practical focus of the effort and demonstration is to get information in the hands of justice practitioners and officials.

There was considerable discussion about the issues regarding the reference standard, e.g., Shibboleth versus Security Assertions Markup Language (SAML) (specifically, SAML, Version 2.0) and Liberty Alliance. The group reached consensus that the justice specification has requirements and other component pieces that go along with the previous SAML specification (e.g., messaging). Furthermore, Liberty Alliance has targeted its requirements towards e-commerce, while industry members noted there is no commercial support or tools with Shibboleth.

Others noted that the important aspect was to develop a justice-specific "XML-specified" credential according to the requirements for "log in and user management" of the *National Criminal Intelligence Sharing Plan* (NCISP), which is fundamental to the NCISP. It is a familiar extensible model; the current model is proprietary, but the technologies are evolving.

Piloting is expected to deliver valuable lessons learned by October 2006. Other deliverables from the demonstration include Common Usage Profile specification, usage scenarios, interface specifications, and recommendations going forward. Ultimately, for strategic planning, the GSWG will need to determine what kinds of recommendations are going to be made to GESC. There was a lot of interest in this issue. Timing and the schedules for piloting may need to be altered based on these determinations.

Wireless Action Item

Mr. Jim Cabral, IJIS Institute, briefed the working group on the previous work efforts of the GSWG. Since December 2004, a great deal of work has been done to review and update the security document, which includes 160 pages of best practices information. Following the original format of the *Applying Security Practices to Justice Information Sharing* document, the update has appended the guide with the subject areas specifically geared for wireless technologies.

The next steps are to have the original team revisit the draft document, review content, and make decisions about format. This is a "quick win" for the GSWG, with a significant piece of work ready for delivery. In the future, however, the GSWG should reach consensus during its strategic discussions, whether or not the GSWG should be the body responsible for the annual updates and maintenance of these products.

Messaging Focus Group Update

Vice Chair Ruegg provided a short briefing on what the group had done, along with the current and future activities. This is a new group, with little history; therefore, in order for collaboration to happen, Vice Chair Ruegg noted that some outreach needs to occur.

Global Infrastructure Working Group Update

Mr. Scott Fairholm, National Center for State Courts and GISWG representative, briefed the working group on Justice Reference Service-Oriented Architecture. Mr. Fairholm provided a white paper and diagram developed by Mr. Scott Came, state of Washington, that detailed the following areas.

- What is Service-Oriented Architecture (SOA)?
- What is a service?
- What is architecture?

Mr. Fairholm stated that Global has reached consensus on a common definition for SOA. The definition is a system architecture that seeks to integrate disparate information systems—usually under the control of autonomous business partners—in a manner that retains the independence of these systems from one another's internal architectures.

GISWG is vetting models of the Justice Reference Architecture developed in terms of views, and Mr. Came's white paper was discussed in further detail regarding the types of views. If there is an agreement on the conceptualization of the Justice Reference Architecture and as long as there is communication between the working groups, then Global can begin to put placeholders into the requirements for defining our respective supporting components of the architecture.

The group spent considerable time on discussion that focused on the critical need of GISWG work in setting the GSWG list of priorities and in developing the strategic direction. A consensus was reached that GSWG needs to work parallel with GISWG. As GSWG is developing or defining a Security Reference Architecture, it needs to be complimentary, supportive, or reflective of the GISWG SOA Justice Reference Architecture.

Existing and Emerging Issues

Mr. Alan Harbitter, Nortel PEC, provided a briefing based on his findings, as well as previous GSAC work efforts. The working group members engaged in a lengthy discussion debating the difference between "architecture" for security rather than the terminology "framework."

The working group supported the decision that "framework" better provides a neutral and comprehensive view to information security. By practice, security should not just focus on one area. The GSWG approach should reflect a holistic view of security.

The GSWG goal is to produce products in areas of confidentiality, integrity, availability, and authentication, which was also referenced as the Confidentiality, Integrity, Availability, and Authentication (CIAA)-framework. Mr. Harbitter contends that in doing so, the security framework will begin in critical areas and provide a balanced approach.

Possible Products for Confidentiality

- Standards for network and data encryption
- Standards for data tagging for security purposes

Possible Products for Integrity

- Standards for digital signature and PKI interoperability
- Guidelines for auditing

Possible Products for Availability

- Guidelines for perimeter defense
- Guidelines for public vs. private resource use

Possible Products Authentication

- Common Usage Profile (GSAC progress has been made here)
- ID management model (Liberty Alliance vs. Shibboleth)
- E-Authentication guidelines (National Institute of Standards and Technology [NIST] levels of rigor)

Possible Other Products (overlap between components)

- N:N MOU guidance (It would be nice to have an N:N model)
- Evaluation and rating standards (NIST)

National Information Exchange Model (NIEM) Update

Mr. Bob Greeves, Bureau of Justice Assistance (BJA), briefed the working group on the current status of NIEM. Mr. Mike Daconta is leaving the NIEM Project, therefore, creating a near-term vacuum. Mr. Daconta did a good job pushing NIEM and getting federal organizations to integrate and bridge the gaps between the technical and policy worlds.

Of the issues discussed concerning NIEM, the number one issue is a sense that there is no state and local participation. NIEM has drifted and needs to get into the front lines of state and locals.

The second issue is the governance identification. Ideas have been proposed and a draft governance plan is available. These two issues have been briefed to Mr. Van Hitch, Chief Information Officer of the U.S. Department of Justice (DOJ). There are a couple of major meetings coming up in December 2005 that will be instrumental in the future direction of the Project. This is an opportunity for Global to get involved in the leadership of NIEM.

Other issues regarding NIEM were pointed out by the working group, such as the lack of a strong link between the Global XML Structure Task Force and NIEM communities in terms of pilot project input into the NIEM. Although there are all kinds of federal level pilot projects scheduled, the Virginia/Maryland/DC (CAPwin) project is the only justice-community pilot currently in NIEM. Also, there is no clear funding path for NIEM by DOJ or the U.S. Department of Homeland Security (DHS). Congress, unfortunately, set aside nothing in the budget for NIEM.

Strategic Planning Session

Chair Uecker reconvened the meeting and began with a recap and continued discussion of the compiled issues important to the strategic planning process. Vice Chair Ruegg noted that he had spent the evening reviewing the wireless materials and agreed that it is a tremendous piece of work that is 95 percent ready for publication. He reiterated the strategic value of balancing "quick wins" for the GSWG with the longer term goals and objectives that may stretch even beyond our current scope of planning.

Under the leadership of Chair Uecker and Vice Char Ruegg, Mr. Tom Kooy, consultant for the Institute for Intergovernmental Research, began the strategic planning facilitation. The working group was presented with the previous mission and vision statements. A discussion was generated around whether they should be revisited and reworked.

Several participants reflected on the current language and noted that the GSWG should make the mission statement broader. The discussion from the previous day about the meaning and implications of the terms "framework" versus "architecture" led to decisions to alter the mission language. In the end, it was decided that "framework" may be a more appropriate word than "architecture."

There was also a consensus that the previous vision statement was not a "true" vision. A vision statement should describe a "to be" state. It should define "where" and "why" there is movement in a certain direction, consistent with the "mission."

Ultimately, the GSWG recognized that their mission and vision statements need to align and support those of Global: "To get the right information to the right people at the right time." The GSWG decided on the following wording for their mission and vision statements:

> **Mission**: To foster the trusted sharing of justice information by recommending a security framework and best practices regarding security guidelines, technologies, and procedures.
>
> **Vision**: We envision a future where trusted justice information partners can share information while ensuring its confidentiality, integrity, and availability.

Mr. Kooy continued the facilitation of the critical issues. A process of organizing, grouping, and prioritizing the list of issues was conducted. Using the past lists of projects, the compiled issues raised from the previous day's discussions, and other input, IIR staff provided each participant with groupings of these issues.

The first step was to perform a Mutually Exclusive and Comprehensively Exhaustive (MECE) analysis. Considering the list of issues, the GSWG members evaluate whether the items listed are Mutually Exclusive and Comprehensively Exhaustive. A lengthy process and discussion ensued to collapse, group, and refine the list of issues.

The next process step was for the GSWG to determine logical groupings for these issues. Ultimately, the group expressed the need to be focused on "projects" with deliverable "products" cascading out of the projects. Every product is the outcome of a project, but the larger body of effort and time is within the projects themselves. Subsequently, it was also recognized that "outcomes," "collaboration," and "outreach" were other critical areas but, in many ways, were also directly tied to the projects and their products. GSWG agreed that to be "project-focused" and to articulate the relationship of the outcomes and products of each project, as well as the outreach and collaboration opportunities and requirements with each item.

The Working Group decided to focus on specific deliverables:

1. Executive briefing on security issues
2. Develop electronic technical bulletins on security topics
3. Collaborate with IJIS on pre-RFP toolkit security module
4. White papers on Web services implementations
5. Paper on local and state funding issues
6. Original CD—completed
7. Wi-Fi flyer—completed
8. General/technical recommendation regarding Federated Identity and Privilege Management

9. CD or documentation on the wireless reference material, *Applying Security Practices to Justice Information Sharing*
10. Guidelines for network and data encryption
11. Recommended security resources for implementing SOA
12. Guidelines for data tagging for security purposes
13. Guidelines for digital signature and PKI interoperability
14. Guidelines for auditing shared data access and handling
15. Guidelines for public versus private resource use
16. Recommendation of identity management model
17. Provide guidelines for E-Authentication
18. Protocol for memorandum of understanding for overall security framework
19. Evaluation and rating standards
20. Security framework in support of the *National Criminal Intelligence Sharing Plan*
21. Guidelines for continuity of operations/disaster recovery
22. Recommended security resources as they relate to trusted information sharing
23. Identity theft

These were then aligned with the highest-level view of the current GSWG projects:

1. Refresh the *Applying Security Practices to Justice Information Sharing* document as relates to wireless
2. Create security architecture (CIAA-framework) for the justice community which includes support for the Justice Reference SOA (Note: Has greater implications for design and implementation—defining the intersections of security with all of the SOA views)
3. Maintenance of GSWG products
4. Develop federated identity and privilege management recommendation as a justice specific standard(s) within the security architecture framework, including developing and piloting trusted credentials (Note: Common usage profile)
5. Outreach

In the next phases of the planning, the group began to build the logic path between the projects and the deliverables, mapping along with them the priority rankings that were developed in the discussion process.

Subsequently, the facilitator assisted the group in setting a priority ranking for each project. GSWG participants, for each project subsection, were asked to choose two or three most important issues. In some cases, two or three levels of priorities were captured. Wherever possible, there were also discussion points on timelines and interim deliverables that could be achieved and captured for the GSWG Business Plan. Where noted, special project teams and leads were selected for the "Next Steps" development of these goals and objectives.

Projects

1. **Refresh the *Applying Security Practices to Justice Information Sharing* document as it relates to wireless (Timeline: 6 weeks; priority: high; IIR staff will finalize draft language and redistribute to chairs and authors before December 31, 2005)**

   - Executive briefing on security issues (1)
   - CD or documentation on wireless reference material, *Applying Security Practices to Justice Information Sharing* (9)

2. **Create a security reference architecture (CIAA-framework) for the justice community that includes support for the Justice Reference Architecture**

   Priority 1 Items, Tasks, and Assignments (Note: First person listed is the lead.):
   - Document security framework in support of the *National Criminal Intelligence Sharing Plan* (20) Mr. Harbitter and Mr. Ruegg
   - Defining security requirements for Justice Reference SOA (*Note: Focusing on requirements design and implementation*) (23) Mr. Cabral, Mr. Merkle, Ms. Uecker, Mr. Phillips, and Mr. Fairholm
   - Protocol for memorandum of understanding for overall security framework (18) Ms. Rogers, Mr. Ruegg, Mr. Shipley, Mr. Merkle, and Mr. Hanson

   Priority 2 Items:
   - Guidelines for auditing shared data access and handling (14)
   - Guidelines for digital signature and PKI interoperability (13)
   - Guidelines for data tagging for security purposes (12)
   - Guidelines for network and data encryption (10)
   - Guidelines for public versus private resource use (15)

   Priority 3 Items:
   - Executive briefing on security issues (1)
   - Develop electronic technical bulletins on security topics (2)
   - White papers on Web services implementations (4)
   - Provide guidelines for E-Authentication (17)
   - Evaluation and rating standards (19)
   - Guidelines for continuity of operations/disaster recovery (21)
   - Recommended security resources (technical guides, tutorials, Web sites, standards, etc.) as they relate to trusted information sharing (22)
   - Identity theft management

3. **Maintenance of GSWG products**

   - Original CD—completed (6)
   - Wi-Fi flyer—completed (7)

4. **Develop federated identity and privilege management recommendations as a justice specific standard(s) within the security architecture framework, including developing and piloting trusted credentials** (*Note: Common usage profile*)

   Action Item: Ms. Rogers will coordinate and communicate with the Pilot Team and GSAC.

   - Recommendation of identity management model (16)
     - Integration of identity model into participating systems (July 2006)
     - General/technical recommendation regarding Federated Identity and Privilege Management (8)
   - Develop a Common Usage Profile proposed draft specification
     - Development (45 days)
     - Proposed specification
     - Prototype demonstration
     - GSWG review of proposed specification
     - Present proposed draft specification to GAC (April 2006)
     - Next steps recommendations:
       - Operational testing/demonstration
       - Updated proposed specification
       - Vetting
       - Possible approval/formal recommendation of draft specification
   - Executive briefing on security issues (1)
   - Develop electronic technical bulletins on security topics (2)

5. **Outreach**

   - Executive briefing on security issues (1)
   - Develop electronic technical bulletins on security topics (2)
   - Collaborate with IJIS Institute on pre-RFP toolkit security module (3)
   - Paper on local and state funding issues (5)
   - Security training guidance

High Priority Tasks and Assignments

- Refresh the *Applying Security Practices to Justice Information Sharing* document as it relates to wireless
  - IIR staff will finalize the draft and redistribute to chair, vice chair, and authors before December 31, 2005. Timeline for completion is six weeks.
- Document security framework in support of the *National Criminal Intelligence Sharing Plan* (20)
  - Mr. Harbitter and Mr. Ruegg

- Define security requirements for justice reference SOA (*Note: Focusing on requirements design and implementation*) (23)
  - Mr. Cabral, Mr. Merkle, Ms. Uecker, Mr. Phillips, and Mr. Fairholm
- Protocol for memorandum of understanding for overall security framework (18)
  - Ms. Rogers, Mr. Ruegg, Mr. Shipley, Mr. Merkle, and Mr. Hanson
- Coordinate and communicate with Pilot Team and GSAC (see Project 4 above)
  - Ms. Rogers
- Schedule follow-up conference call regarding the conference call for Friday, January 6, or Tuesday, January 10, 2006
  - IIR

Next Steps

Chair Uecker guided the working group through the follow-up and next steps discussion. Immediate plans included distributing the meeting summary, developing a new business plan, and vetting the wireless document in the next month. The next meeting for the GSWG is tentatively being planned for March 2006. Next steps reminders will be sent, and plans to coordinate the work and meetings of the GSWG and the GSAC will be focused on. Chair Uecker adjourned the meeting and thanked everyone for their hard work.

GSWG Meeting Summary 12-05.doc