Global Justice Information Sharing Initiative

Security Working Group Meeting Summary

Salt Lake City, Utah
June 9, 2004

Meeting Background and Purpose

A newly structured Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG) was convened on June 9, 2004, in Salt Lake City, Utah, by the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ). The purpose of the meeting was to discuss wireless security topics and to develop a strategy in support of Global. While information sharing challenges are similar for wired and wireless data exchanges, the GSWG would like to focus on developing best practices for justice scenarios that encompass aspects unique to wireless communications.

The Working Group was reconstituted during the last Global Executive Steering Committee (GESC) meeting because of the crucial nature of information sharing, interoperability, and security within the wireless arena. Mr. Harlin McEwen, GESC member and chair of the Communications and Technology Committee, International Association of Chiefs of Police, provided recommendations regarding subject-matter experts as well as direction for the key topic areas. Participants were then selected by Mr. Steve Correll, GSWG chair and Executive Director of the National Law Enforcement Telecommunication System. After review and confirmation by OJP, the candidates were then contacted for a voluntary position on the Working Group. Representatives include members from a broad experience base, from practitioners to subject-matter experts. Preliminary work on targeted topics was conducted by a conference call that was held on May 26, 2004.

This is the first meeting of the reconstituted GSWG, and agenda items included presentations from wireless subject-matter experts; activities of the National Public Safety Telecommunications Council, SAFECOM, and Criminal Justice Information Services (CJIS); and group discussions on the priorities for protecting wireless communications.

Global Security Working Group Participants

Chairman Correll welcomed participants to the GSWG. The following members, federal officials, delegates, and staff were in attendance:

D. J. Atkinson
National Telecommunications and Information Administration
Boulder, Colorado

David Buchanan
County of San Bernardino
San Bernardino, California

David Clopton, Ph.D.
National Institute of Justice
Washington, DC
Gerry Coleman
Wisconsin Department of Justice
Madison, Wisconsin
Steve Correll
National Law Enforcement Telecommunication System
Phoenix, Arizona
Fred Cotton
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California
Ken Gill
Office of Justice Programs
Washington, DC
Alan Harbitter, Ph.D.
Integrated Justice Information Systems
Fairfax, Virginia
Joseph Hindman
Scottsdale Police Department
Scottsdale, Arizona
Kathy Imel
National Law Enforcement and Corrections Technology Center, Rocky Mountain Region
Westminster, Colorado
Patrick McCreary
Office of Justice Programs
Washington, DC
Terri Pate
Institute for Intergovernmental Research
Tallahassee, Florida
John Powell
National Public Safety Telecommunications Council
Denver, Colorado
Charles Pruitt
Arkansas Crime Information Center
Little Rock, Arizona
Monique Schmidt
Institute for Intergovernmental Research
Tallahassee, Florida
Andrew Thiessen
National Telecommunications and Information Administration
Boulder, Colorado

Presentations

Chairman Correll began the meeting with a detailed review of GSWG history and previous work efforts, as well as the current organization and initiatives of the Global Advisory Committee (GAC). Ms. Monique Schmidt, Institute for Intergovernmental Research, followed with a demonstration of the GSWG *Applying Security Practices to Justice Information Sharing* CD to provide additional background materials.

Mr. John Powell, National Public Safety Telecommunications Council (NPSTC), presented wireless security information from the public safety user's perspective. He stated, "Today's users are only looking for a tool to simplify their job and/or make them more efficient; a tool that is no more complex to use than the one it replaces." He explained that the NPSTC is supported by the DOJ Advanced Generation of Interoperability for Law Enforcement (AGILE) program. It includes a federation of thirteen national public safety associations, with a liaison from five federal agencies. It provides oversight for many national public safety communications involving 700 MHz, 800 rebanding, 4.9 GHz, and new technologies. There is a need for an interoperability standard, authentication/privileges (especially for roamers), and message transport and network security. Mr. Powell also explained that Software Defined Radio (SDR) is the wireless future, even with some concerns with SDR security, because it provides an ultimate interoperability solution.

The next presenter was Ms. Kathy Imel, National Law Enforcement and Corrections Technology Center, Rocky Mountain Region, who provided an overview of the issues involved in wireless security for public safety. Public safety addresses first

responders (ambulance, law enforcement, and fire). Public safety mobility is defined as roaming across jurisdiction boundaries while maintaining constant communications across multiple jurisdictions. Public safety must deal with multinetwork interoperability (radio, telephone/cell phone, and computer), as well as device variability. Ms. Imel provided information on public safety mobility functional requirements, issues, challenges, network heterogeneity, and security. The findings presented were based on information gathered for "The Study to Determine the Need for and Feasibility of Implementing a National IP-Based Public Safety Interconnectivity Authentication Process." To achieve all of the public safety mobility requirements identified, the following would be required:

- Deployment of next generation networks
- Seamless interoperability between heterogeneous networks
- Integrated security and applications interoperability
- Support for a variety of devices

Study findings indicate that a national-based IP authentication network is not feasible or practical at this time. Two areas of interest were identified for further study: single sign-on and next generation network development support.

Mr. Andy Thiessen, National Telecommunications and Information Administration, presented information on 802.11 security for public safety communications. Public safety security requirements include access control, integrity, monitoring, privacy, and attack detection and prevention. Mr. Thiessen discussed the fact that security is not a product but a process, and he outlined the characteristics of security protocols, including Wired Equivalency Privacy (WEP), 802.11i (Wireless Protected Access [WPA] and Robust Security Networks [RSN]), 802.1x, EAP (Extensible Authentication Protocol), and known obstacles and attacks. In addition, Mr. Thiessen described the different communications systems that must seamlessly integrate to form the various networks or the "system of systems." It includes the Personal Area Network (PAN), Incident Area Network (IAN), Jurisdiction Area Network (JAN), and the Extended Area Network (EAN). He emphasized that the magnitude of the event dictates the complexity of administration (for example, between multiple regions and disciplines). His recommendation is that the GSWG must work to mitigate current security problems, and he believes that denial of service is the single largest problem. In addition, he states that WPA is recommended over WEP, and RSN will be better than WPA.

Mr. Charles Pruitt, Arkansas Crime Information Center, provided an informative discussion on CJIS wireless security policy updates and challenges. The CJIS security policy is considered sensitive but unclassified and is available to law enforcement individuals and entities.

GSWG Resources

Over the course of the day, the following wireless resources were discussed by the Working Group:

- CJIS policies utilize NIST SP 800-48, "Wireless Network Security."
- AGILE, SAFECOM, and the National Institute of Standards and Technology's Office of Homeland Security utilize the *Statement of Requirements for Public Safety Wireless Communications & Interoperability, The SAFECOM Program Department of Homeland Security* (SOR), Version 1.0, March 10, 2004.
- NPSTC sponsored "*The Study to Determine the Need for and Feasibility of Implementing a National IP-Based Public Safety Interconnectivity Authentication Process,"* NPSTC Support Office, National Law Enforcement and Corrections Technology Center, Rocky Mountain Region.
- AGILE Interoperability CD provides valuable educational and resource materials so the public safety practitioner can gain an understanding of wireless communications.
- The Justice Technology Information Network Web site is www.nlectc.org.
- The National Criminal Justice Reference Service provides resources for safety and preparedness, and the Web site is www.ncjrs.org.
- The Pre-RFP Toolkit was developed by Integrated Justice Information Systems (IJIS) and can be found at www.ijis.org/procure.

Discussions and Assumptions

The GSWG time frame is to produce the objective/deliverable(s) by January 2005.

Intended Audience—Flip Chart

1. Information technology practitioners want to know how to secure wireless systems.
2. Decision makers want to know why to deploy security safeguards.
3. Legislators, government associations, and the National Association of State Chief Information Officers (NASCIO) want an overview.
4. Local and state information security officers (ISO) need to have an education and discussion forum. These practitioners are already pulled together periodically.

SAFECOM

The Group reached consensus that the SOR must be supported by Global. Overall, the SOR focuses on the future functional needs of first responders to facilitate wireless interoperability at all government levels. The SOR is intended to be a future road map for vendors, whereas data interoperability is the new model.

The GSWG would like to pull the SOR into itself to integrate the extensive work that is being done by SAFECOM and to leverage a collaboration opportunity. The focus will be on how to support and how to help the Global constituents, which is a broader

justice community. In addition, GSWG can provide functional requirements that are part of an architecture framework in order to work towards standardization. In turn, the GSWG can review the wireless security noted in the SOR and then provide guidance where needed.

The GSWG discussed the following issues that are critical to extending the outreach of the SOR to the Global community.

- Describe the "fear" and danger by creating law enforcement scenarios that describe how an event can happen to you.
- Format and include models specific to Global constituents and provide an executive overview brochure with decision maker audience-friendly text.
- Pull SOR into GSWG.

Best Practice Topics

While information sharing challenges are similar for wired and wireless data exchanges, the GSWG would like to focus on developing best practices for justice scenarios that encompass aspects unique to wireless communications. These guides will emphasize how the wireless and wired worlds differ and provide recommendations on how to share information right now. In addition, the best practices would provide periodic guidance with respect to wireless that would also track the SOR. The following "best practices" topics were discussed as priorities by the Working Group.

- Two-page guides on the various wireless security topics provision
- Risk mitigation (i.e., 802.11)
- Scalable authentication
- Guidelines and/or a baseline for operational needs provision
- Air interface identification and standardization
- Grant guidance with respect to wireless
- 4.9 GHz Band

Wireless Information Sharing Concepts

The following GSWG activities are heeded by Global practitioners in order to facilitate information sharing on wireless security concepts.

- Delivery methods to get the resources to the practitioner and decision makers (i.e., brochures)
- Educational efforts (i.e., Webinars or post on Web sites)
- Spectrum sharing concepts
- Review wireless security policies to strive to make them better

Pre-RFP Toolkit

The Pre-RFP Toolkit provides guidance in several areas critical to preprocurement planning and readiness assessment, ranging from defining integrated

justice for your community to assessing support and governance, to developing strategic plans and project requirements (both technical and functional). The Toolkit provides links to key resources, templates, and examples from practitioners and vendors who have gone through the procurement process and have implemented successful justice information sharing systems.[1]

The Working Group would like to apply the SOR (appropriately to Global) to the Pre-RFP Toolkit in order to facilitate purchases. This tool would be valuable to practitioners and decision makers, and it would provide a methodology to go through for acquiring security services.

Top Seven Security Issues Related to Wireless That Global Should Address—Flip Chart

1. Describe the "fear" by creating law enforcement scenarios.
2. Vet the SAFECOM SOR to Global.
3. Apply SOR (appropriately to Global) to the Pre-RFP Toolkit.
4. Spectrum sharing concepts/wireless sharing concepts.
5. Pull SOR into GSWG.
6. Format and include models specific to Global constituents and "rewrite" with decision maker audience-friendly text.
7. Immediate steps—risk mitigation.

Priorities—Flip Chart

1. Vet SOR to Global.
2. Describe issues and identify scenarios.
3. Short-term best practices—short list of topics (i.e., authentication). SOR—Practitioner Version, Pre-RFP Toolkit. Give example of best practices RFP to group.

Priorities and Action Items

Issue One: Read through SOR law enforcement scenario to identify security gaps and to perform a gap analysis (SOR Sections 3.4, 4.4, and 5).

Status: GSWG's homework assignment for the next meeting.

Issue Two: Develop three major scenarios—Fire, EMS, Law Enforcement—based on the SOR (Sections 3.4, 4.4, and 5).

Status: GSWG's homework assignment for the next meeting.

[1] www.ijis.com/procure

Issue Three: Identify members of Global to vet the SOR and write a brief summary for Mr. Tom Coty to submit to GAC Chairman Mel Carraway that requests Global support.

Status: Monique Schmidt's homework assignment for the next meeting.

Issue Four: Develop an outline for a white paper for best practice topic(s).

Status: GSWG's homework assignment for the next meeting.

Issue Five: Identify "fear" topics that outline potential problems that can happen during various law enforcement scenarios (i.e., shoot/don't shoot communication).

Status: GSWG's homework assignment for the next meeting.

Closing Thoughts

The Working Group agreed to develop and deliver a message to the local and state levels in order to facilitate information sharing while providing guidance on wireless security topics that support the SOR. This guidance will cover topics that are unique to wireless communications and that provide resources for procurement or technology refresh upgrades. The best practice guides will extend out to the broad Global membership with real life scenarios that plainly explain concepts in a clear and concise method. There is a strong need for risk mitigation that addresses known obstacles and threats, authentication mechanisms, and data interoperability.

Mr. Correll thanked the new members for a very productive and informative meeting, and with no further business, the meeting was adjourned.

summary SWG salt lake-jun04.doc