Global Justice Information Sharing Initiative

Security Working Group Meeting Summary

Denver, Colorado
December 7-8, 2004

Meeting Purpose

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG or "Working Group") on December 7-8, 2004. The meeting purpose was to finalize the content for the wireless security component as a major update to the *Applying Security Practices to Justice Information Sharing* CD and to begin developing a Pre-RFP Toolkit module in collaboration with the Integrated Justice Information Systems (IJIS) Institute. These documents will explore the security domains critical to wireless communications, information sharing, and interoperability.

Global Security Working Group Participants

Chairman Steve Correll, Executive Director, NLETS - The International Justice and Public Safety Information Sharing Network, welcomed the following participants to Denver:

David Buchanan
County of San Bernardino
San Bernardino, California

Jim Cabral
Integrated Justice Information Systems Institute
Seattle, Washington

David Clopton, Ph.D.
National Institute of Justice
Washington, DC

Steve Correll
NLETS - The International Justice and Public Safety Information Sharing Network
Phoenix, Arizona

Ken Gill
Office of Justice Programs
Washington, DC

Joe Hindman
Scottsdale Police Department
Scottsdale, Arizona

Monique La Bare
Institute for Intergovernmental Research
Tallahassee, Florida

Terri Pate
Institute for Intergovernmental Research
Tallahassee, Florida

Jim Powell
National Public Safety Telecommunications Council (NPSTC)
Denver, Colorado

Charles Pruitt
Arkansas Crime Information Center
Little Rock, Arkansas

Louis Smith
Integrated Justice Information Systems Institute
Louisville, Kentucky

Andrew Thiessen
National Telecommunications and Information Administration
Boulder, Colorado

The Working Group is conducting a major update to the *Applying Security Practices to Justice Information Sharing* CD. Current assignments were to review each section and perform a gap analysis. These assignments were given to volunteers by Chairman Correll, and each person based their work on the security domains that are outlined below. During the review session, the group critiqued and provided their analysis on each security component. Considerable group discussion about the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Division Security Policy, September 2004, Version 4.0, occurred for each topic area, and these comments will be integrated and compiled into the final documentation as a baseline. The due date for the following assignments is January 7, 2004. The GSWG would like to have the CD updated and ready to vet to the Global Advisory Committee (GAC) by early April 2005.

Draft Reviews and Group Discussions

Introduction

Support

1. Governance
2. Risk management (includes critical incident response)
3. Physical security
4. Personnel screening
5. Separation of duties

Prevention

6. Identification and authentication
7. Authorization and access control
8. Data integrity
9. Data encryption
10. Data classification
11. Change management
12. Public access, privacy, and confidentiality
13. Firewalls, VPNs, and other network safeguards

Detection and Recovery

14. Attack detection and prevention
    - Monitoring in a peer-to-peer transaction
    - Known wireless attacks
15. Security auditing
16. Disaster recovery and business continuity
17. IDS/IPS

Appendix

18. Glossary
19. Acronyms

Pre-RFP Toolkit Security Module

Another GSWG deliverable that was discussed included a preprocurement toolkit (Pre-RFP Toolkit) to address new wireless security products and key topics for decision makers.

Prior to this meeting, the GSWG opened conversations with Mr. Paul Wormeli, Director of IJIS Institute, as well as the other developers of the Pre-RFP Toolkit (or "Toolkit"). Mr. Wormeli would like to have input from the GSWG for the future update of their product. To begin collaboration, Mr. Louis Smith, IJIS, provided a demonstration of the Toolkit. The Toolkit is designed to assist managers and practitioners in determining the questions to ask before developing a request for proposal (RFP). It includes 12 components in an excellent CD format. It was recommended that someone from the GSWG go to the next IJIS Institute Industry Working Group (IWG) Pre-RFP Toolkit planning meeting for further agreement on how to collaborate.

Originally, the GSWG came up with the idea of a question-and-answer format for practitioners to use when questioning vendors about the various security capabilities of their products. The GSWG would like to provide more specifics, for example, giving people the right questions to ask in the RFP. The Working Group agreed that the Car 54 Project[1] is the perfect example for a use case scenario depicting the direction of wireless.

After considerable discussion, the Working Group began to outline questions for each of the security domains. From this effort, it was determined that this is a major undertaking and that it would take longer than January to complete. The group wanted to have a more effective approach for a deliverable in the January time frame. The Working Group agreed to hold off on the development of the Toolkit module until Mr. Smith had reviewed the wireless security document and determined whether or not it will meet with IJIS IWG future plans.

Electronic Technical Bulletins (ETBs) on Security Topics

The Working Group spent considerable discussion on an electronic bulletin format and other miscellaneous issues. The security flyer that was developed for distribution at the International Association of Chiefs of Police conference was discussed, and the GSWG liked the format. Instead of flyers, the group developed the concept of electronic technical bulletins for critical security topics. The concept is to send out a briefing—electronically—about once a quarter. It will be approximately one page long, and it will be comprised of three key points, topic discussion, Web links, contacts, and a statement about Global. The group is working with a January timeline for these bulletins. They discussed working on a title, such as the Global Executive Bulletins. Another name for the bulletins that the group discussed was GEM. The priority security topic areas are listed below:

[1] See http://www.project54.unh.edu/

1. Common wireless attacks—eavesdropping and denial of service; assigned to Mr. Andy Thiessen.
2. 4.9 GHz—assigned to Mr. David Buchanan.
3. WAP (wireless access points) How To—assigned to Mr. Thiessen.
4. Wireless procurement.

Regarding wireless procurement, GSWG discussed how to collaborate with the Community Oriented Policing Services office on topics pertinent to their grantees, i.e., development of documentation for new wireless procurement for mobile data terminals and other new wireless hardware that will need appropriate security. In addition, it was noted to bring the need for a Security Assertion Markup Language (SAML) profile for wireless objects to the attention of the Global Security Architecture Committee. This would provide a Web service attribute for device access into systems. For example, system owners could deny access into their applications/systems based on their specific wireless security policies.

Planned Deliverables

1. Major update to the *Applying Security Practices to Justice Information Sharing* CD with a new chapter on wireless security.
2. Global Executive Bulletins.
3. Module for Pre-RFP Toolkit.
4. How-to Guide for WAP.
5. Catalog of wireless security references.
6. Paper on local and state funding issues (assigned to Mr. Joe Hindman).

Next Steps

A conference call is scheduled for January 18, 2005, for the purpose of tying up any loose ends for the major update to the *Applying Security Practices to Justice Information Sharing* CD. No other meeting is scheduled at this time. With no further business, Chairman Correll adjourned the meeting.

Appendix: Homework Assignments

DUE DATE IS JANUARY 7, 2005

Who	What	To be done
Joe Hindman/John Powell	1. Governance	Send/add a paragraph on state and local interoperability concepts.
Jim Cabral/David Buchanan	2. Physical security	Add section on vandalism of unmanned towers. Add section on PDA security.
David Clopton/ Joe Hindman	3. Authorization and Access Control	Add generic role-based access statement.
Steve Correll/Everyone	4. Introduction	Write the Introduction. Group will provide input on the content.
Steve Correll	5. Personnel Screening	Add a sentence about secondary background screening.
Jim Cabral	6. Critical Incident Response	Roll section into the Risk Management Section.
John Powell	7. Data Integrity	Integrate Andy's comments with John's into the original document.
Everyone	**Review CJIS**	Use as baseline for the 4.9 GHz document.
Andy Thiessen	8. WAP HOW TO	Write the "How-to" document.
Jim Cabral/Andy Thiessen	9. Known Wireless Attacks	Write an intro/executive overview paragraph. Write what to look for.