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 Monday, October 4, 2004. The meeting purpose was to conduct an in-depth group review of the new content for the wireless security documentation that is currently under development. This documentation will explore the security domains critical to wireless communications and interoperability. Other GSWG deliverables that were discussed include a preprocurement tool-kit to address standards and specifications for new commercial products and key topic papers to raise awareness of the most critical wireless security issues.

Global Security Working Group Participants

Chairman Steve Correll, Executive Director, National Law Enforcement Telecommunication System, welcomed participants to the GSWG. The newest member of the Working Group, Mr. Jim Cabral, was introduced. Mr. Cabral is chair of the Integrated Justice Information Systems (IJIS) Institute Security Committee and senior manager of MTG Consultants LLC. He is replacing Mr. Alan Harbitter as the IJIS Security Committee representative. He was nominated by Mr. Paul Wormeli, Executive Director, IJIS Institute, and appointed by Mr. Correll. The following participants were in attendance:

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
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

Monique La Bare
Institute for Intergovernmental Research
Tallahassee, Florida
The Working Group had used *Applying Security Practices to Justice Information Sharing* as a model document to develop their initial wireless security drafts. Current assignments were to review each section and perform a GAP analysis. These assignments were given to volunteers by Mr. Correll, and each person based their work on the security domains which are outlined below. During the review session, the group critiqued and provided their analysis on each security component. Considerable group discussion occurred for each topic area and these comments will be integrated and compiled into the draft documentation. The due date for the following assignments is October 29, 2004. See the appendix for more information on the status of the assignments. The GSWG would like to have a finished product by January 2005.

**Draft Reviews and Group Discussions**

**Support**
1. Governance assigned to John Powell  
2. Risk Management (NEW SECTION) by Jim Cabral  
3. Physical Security assigned to Jim Cabral  
4. Personnel Screening by Steve Correll  
5. Separation of Duties by Charles Pruitt

**Prevention**
6. Identification and Authentication written by Joe Hindman and reassigned to Andy Thiessen  
7. Authorization and Access Control to be reviewed by Kathy Imel  
8. Information Assurance and Data Integrity by John Powell  
9. Data Encryption (NEW SECTION) to be done by John Powell and Andy Thiessen  
10. Data Classification reviewed by Kathy Imel  
11. Change Management reviewed by Kathy Imel  
12. Public Access, Privacy, and Confidentiality to be reviewed by John Powell  
13. Firewalls, VPNs, and Other Network Safeguards written by Hyuk Byun and David Clopton
Product Two: “Two Pagers” on Wireless Security Topics

The GSWG reached consensus on several topic areas that are so important that they need extra special attention. These “two pagers” (i.e., front and back) flyers will be developed for decision makers, police chiefs, and fire chiefs as the target audience. The deliverable due date is November 1, 2004. Ms. Jennifer Hicks Zeunik will be asked to distribute these flyers at a shared resource table at the upcoming International Association of Chiefs of Police (IACP) 2004 Annual Conference that will be held on November 13-17, 2004. The critical topic areas are:

1. Common wireless attacks—eavesdropping and denial of service; assigned to Ms. Monique La Bare.
2. Disaster recovery—Orlando hurricane and California fires example and sound bites; assigned to Mr. David Buchanan
3. Governance brief—to be codeveloped with SAFECOM; assigned to Mr. John Powell
4. Prerelease tease Pre-RFP Tool-kit; assigned to Mr. Steve Correll and Ms. La Bare.
5. Spectrum sharing for data interoperability issue—coauthored with the National Public Safety Telecommunications Council (NPSTC); assigned to Mr. David Buchanan.

Action Items and Project Status

The action items are based on the top priorities and concepts incorporated from the GSWG meetings, which are identified below.
**Action Item:** Vet SAFECOM Statement of Requirements for Public Safety Wireless Communications and Interoperability (SoR) to the Global Advisory Committee.

**Status:** Completed. The SAFECOM Statement of Requirements was vetted to the Global Advisory Committee on September 28, 2004. The Global Executive Steering Committee endorses and supports the SAFECOM work efforts and the SoR.

**Action Item:** Send Global Service-Oriented Architecture (SOA) document for review to the GSWG. The SOA maps the future for where Global is going, and the GSWG needs to align with the concepts in it.

**Status:** Ms. La Bare will distribute the document to GSWG members. Mr. Fred Cotton will work with the Global Infrastructure and Standards Working Group to determine what comes to the forefront with SOA security issues.

**Action Item:** Update each of the security domains with the wireless security information.

**Status:** Due date is October 29, 2004.

**Action Item:** Develop “two pagers” on the key wireless topic areas selected by the GSWG.

**Status:** Due date for completion is November 1, 2004.

**Action Item:** Begin to work on the Pre-RFP Tool-kit.

**Status:** Contact IJIS for support in gearing new content towards wireless procurement decisions. Find active RFP’s for group analysis (i.e., Wyoming and Wirelink, Joint Integrated Simulation Procedures (JISP) Listserv, and SEARCH, The National Consortium for Justice Information and Statistics). The GSWG needs to get a cross section of Global RFPs in wireless for courts, corrections, law enforcement, and public safety to use in its analysis.

### Next Steps

The GSWG would like to pay particular attention to completing the tasks at hand for the development of the wireless security documentation. The purpose of the next meeting will be to tie up any loose ends in the document review and to begin the work effort on the Pre-RFP Tool-kit list of questions and answers for decision makers. The Working Group was asked to look at their calendars for scheduling purposes as it is critical to complete these assignments and have finished products prior to the first
quarter 2005. The preferred dates for the next meeting were November 29 and 30, 2004. There was no availability on member’s calendars for a meeting in December due to prior engagements.

After review of the assignments, Mr. Correll thanked the participants for the timely completion of their assignments, and with no further business, the meeting was adjourned.
## Appendix—Homework Assignments

<table>
<thead>
<tr>
<th>Assigned To</th>
<th>Section</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Buchanan</td>
<td>1. Disaster Recovery and Business Continuity</td>
<td>Input group edits</td>
</tr>
<tr>
<td></td>
<td>2. Wireless Foreword/Intro</td>
<td>Input group edits</td>
</tr>
<tr>
<td>Jim Cabral</td>
<td>3. Physical Security</td>
<td>Under review</td>
</tr>
<tr>
<td></td>
<td>4. Intrusion Detection Systems and Intrusion Prevention Systems</td>
<td>Under review/to be done</td>
</tr>
<tr>
<td>David Clopton</td>
<td>5. Firewalls, VPNs, and Other Network Safeguards</td>
<td>Submitted edits for group review</td>
</tr>
<tr>
<td>Steve Correll</td>
<td>6. Personnel Screening</td>
<td>Input group edits</td>
</tr>
<tr>
<td>Fred Cotton</td>
<td>7. Critical Incident Response</td>
<td>Under review</td>
</tr>
<tr>
<td></td>
<td>8. Security Auditing</td>
<td>Input group edits</td>
</tr>
<tr>
<td>Kathy Imel</td>
<td>9. Authorization and Access Control</td>
<td>Review access control section</td>
</tr>
<tr>
<td></td>
<td>10. Data Classification</td>
<td>Completed—no changes</td>
</tr>
<tr>
<td></td>
<td>11. Glossary/Acronyms</td>
<td>Need group input and review</td>
</tr>
<tr>
<td></td>
<td>12. Change Management</td>
<td>Completed—no changes</td>
</tr>
<tr>
<td>John Powell</td>
<td>13. Governance</td>
<td>To be done</td>
</tr>
<tr>
<td></td>
<td>14. Information Assurance and Data Integrity</td>
<td>To be done</td>
</tr>
<tr>
<td></td>
<td>15. Public Access, Privacy, and Confidentiality</td>
<td>To be done</td>
</tr>
<tr>
<td>Charles Pruitt</td>
<td>16. Separation of Duties</td>
<td>Input group edits</td>
</tr>
<tr>
<td>John Powell and Andy Thiessen</td>
<td>17. Data Encryption</td>
<td>New section—to be done</td>
</tr>
<tr>
<td>Andy Thiessen</td>
<td>18. Identification and Authentication</td>
<td>Under review</td>
</tr>
<tr>
<td></td>
<td>19. Attack Detection and Prevention</td>
<td>Under review</td>
</tr>
<tr>
<td></td>
<td>20. Known Wireless Attacks</td>
<td>Input group edits</td>
</tr>
<tr>
<td></td>
<td>21. Monitoring In a Peer-to-Peer Transaction</td>
<td>Input group edits</td>
</tr>
</tbody>
</table>