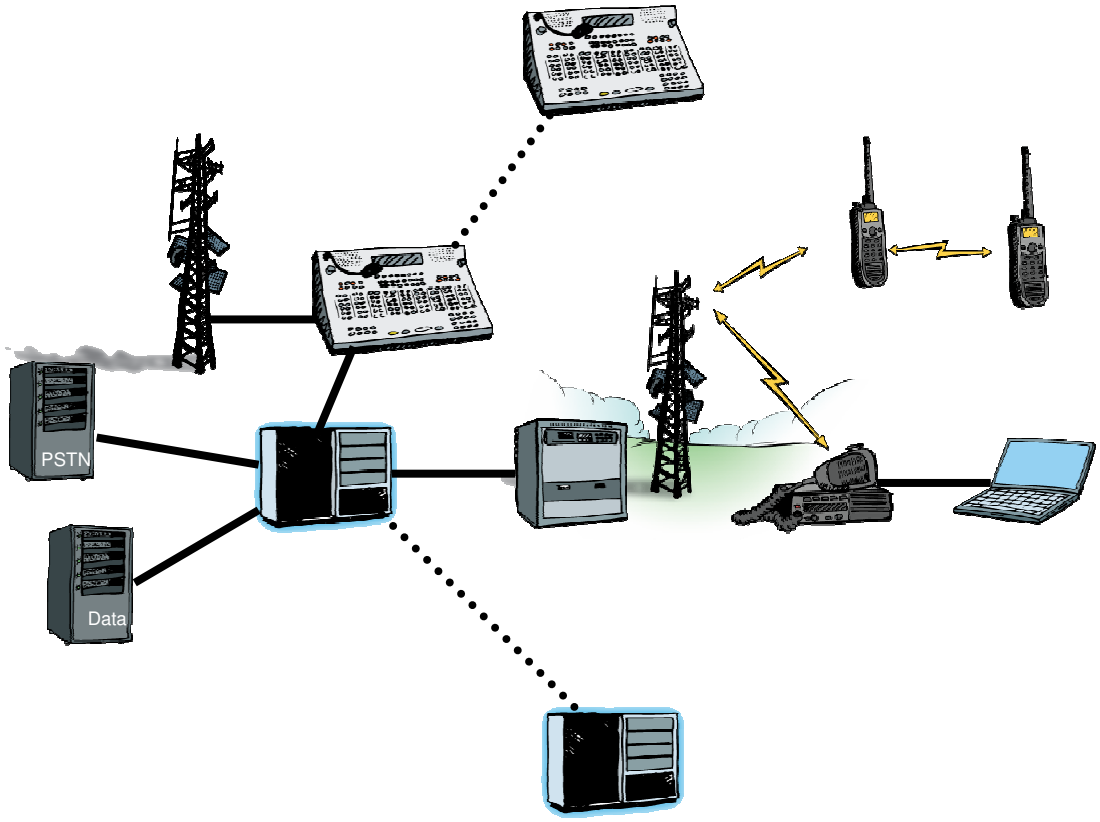
# Office for Interoperability and Compatibility (OIC)

## *Roundtable on Public Safety Interoperability and Voice over Internet Protocol (VoIP)*

## February 20–23, 2007
## San Antonio, TX



## Table of Contents

# Executive Summary

The Department of Homeland Security's (DHS) Office for Interoperability and Compatibility's (OIC), in partnership with the National Institute of Standards and Technology's Office of Law Enforcement Standards (NIST/OLES), hosted a roundtable discussion on February 20-23, 2007, in San Antonio, Texas. The topic of discussion was the use of Voice over Internet Protocol (VoIP) in public safety communications. Meeting participants included industry representatives in the VoIP market, as well public safety and Federal Government representatives.

This four-day meeting had two parts. Part 1 (days 1-2) was called "Strategic Direction." It allowed participants to discuss and define the circumstances, or "environments," in public safety communications where VoIP is currently used or has the capacity to support interoperable communications. Part 2 (days 3-4) was called "Technical Specifics." It allowed participants to delve into one of the VoIP environments defined during day one and two, a "bridging systems interface." (A bridging systems interface adds the functionality of a radio-system-to-radio-system interconnect for systems that do not support direct interconnection.)

The collaboration between public safety, industry, and Federal meeting participants achieved the following:

- Agreement on the public safety environments appropriate for application of VoIP, and agreement on laymen's language to describe each environment
- Agreement on a basic framework for developing implementation profiles for each environment
- Agreement on a working plan for implementation profiles for the bridging systems interface
- Commitment by stakeholders to continue development of the implementation profile for bridging systems interface as well as the remaining environments

This report represents a summary of discussions throughout the meeting, and highlights the decisions of participants. Information in this report was taken from meeting notes and from data collected by the meeting participants.

## Background

Voice over Internet Protocol (VoIP) is a technology that in recent years has shown promise for public safety communications. However, both public safety and industry hold varying perceptions about VoIP's most effective applications as well as its reliability. These perceptions have led to misunderstanding and misinformation between the two communities on VoIP's potential.

To try to clarify the varying perceptions of and requirements for VoIP's role in public safety communications, OIC and NIST/OLES brought together key stakeholders from both the industry and the public safety communities for a series of roundtable discussions.

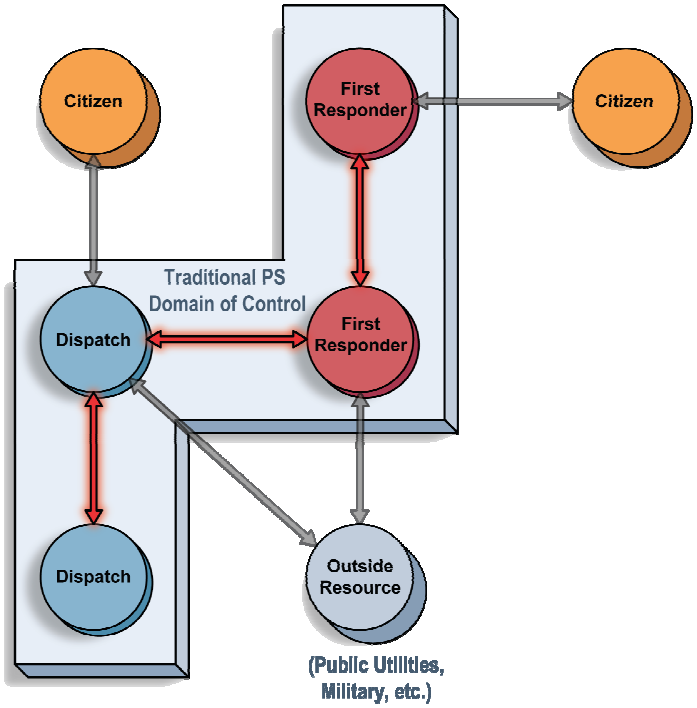
The initial meeting was held August 22, 2006 in Washington, DC. Participants began discussions of standards for VoIP in public safety communications. A second meeting, held February 20-23, 2007, and described in this report, advanced the discussions further by addressing implementation profile development for VoIP environments in public safety. Implementation profiles refer to the minimum set of standards parameters and values necessary to ensure interoperability in any given environment.

## Purpose

The purpose of the meeting was for the industry and public safety communities to work collaboratively to further refine the strategy and tactics for developing appropriate implementation profiles for VoIP in environments that directly involve public safety.

## Scope

This diagram shows the demarcation between areas that were in and out of the scope of the meeting. The areas connected by red arrows, which represent communication between public safety officials, were within scope.




## Public Safety Requirements for VoIP

The following list shows the agreed upon requirements for VoIP communications in the public safety arena. This list was created in the August 2006 meeting. It was amended at the February 2007 meeting:

- Interoperability, compatibility, interchangeability
- Minimum set of standards and features
- Common security framework
- Reliability
- Affordability
- Scalability
- Manageability
- Education/Training
- Leverage Commercial Off The Shelf (COTS) products
- Ability to compare VoIP offering to other alternatives to meet public safety functional requirements

# PART I: STRATEGIC DIRECTION (Days 1 and 2)

## Strategic Direction Outcomes

- Agreement on the public safety environments appropriate for application of VoIP, and agreement on laymen's language to describe each environment
- Agreement on a basic framework for developing implementation profiles for each environment

## VoIP Environments in Public Safety

Participants reviewed and upgraded a list developed at the previous OIC and NIST/OLES meeting in August 2006. This list identifies seven environments in public safety communications where VoIP standards were deemed necessary. Participants at the February 2007 meeting analyzed this list, and confirmed or revised its elements as necessary.

After reaching consensus on the appropriate environments, participants developed a consensus on descriptions, in layman's terms, for seven environments. The purpose was to fully define each of the environments, thus assessing the implementation profile development needed.

The layman's descriptions produced for each of the environments are:

**Radio Site Interface**

- Description: Connects remote portions of a radio system back into that system.
- Example: Connection from a communication center to a mountain-top transmitter
- Example: Project 25 (P25) Fixed Station Interface (FSI)
- Sub-elements (example of technologies):
  - Land Mobile Radio
  - Broadband

**Radio System to Radio System Interface**

- Description: Connect two or more radio systems together via a digital VoIP link.
- Example: P25 Inter-RF Subsystem Interface (ISSI)
- Types:
  - Like-to-like

        - Example: Agency A's P25 Radio Frequency Simulation System (RFSS) to Agency B's P25 RFSS
    - Like-to-unlike
        - Example: P25 RFSS to 700 MHz broadband
        - Example: P25 RFSS to commercial Push-To-Talk (PTT)

**Dispatch Interface**

- Description: Use VoIP to allow dispatchers to communicate with each other.
    - Could be within one dispatch center, or between separate dispatch centers.
- Example: P25 Console Subsystem Interface (CSSI)
- Sub-elements:
    - Dispatch to dispatch
    - Dispatch to core
- Things to consider:
    - What is going on with next generation 911?
    - Public Safety Answering Point (PSAP) to dispatch interface

**Bridging Systems Interface**

- Description: A device that adds the functionality of a radio-system-to-radio-system interconnect for systems that do not support direct interconnection
    - Bridges disparate radio systems.
    - Typically uses baseband audio output of radios as the common format for voice. However, also uses VoIP to connect physically separated bridges.
    - May have different levels of functionalities.
    - Baseband audio is mutually exclusive with end-to-end encryption.
- Sub-elements:
    - Tactical networks
    - Preplanned networks

**Wired End Unit to System Interface**

- Description: A radio operator or a non-radio device communicates with someone at a non-radio device.
    - The device could be a computer on someone's desk in the police station.
    - IP-enabled voice-end systems
    - Non-dispatch user
    - May have an end-unit to end-unit call.
    - Affected by end-to-end encryption requirement
    - Could consider a CSSI-based PC client.

**System to Subscriber Unit (Last Mile Radio)**

- Description: Providing VoIP, or the external appearance of VoIP, directly to the radio handset in the field.
  - Could be an end-user BB device that is IP-addressable.
  - Adds MAC/PHY to the wired end unit to system interface:
    - May contain additional radio channel control information.

**Subscriber Unit to Subscriber Unit**

- Description: The ability for end-user devices to communicate with each other in the absence of infrastructure
  - Subscriber units can be radios, PDAs, wireless laptops, etc.
  - Potential application of Mobile Ad hoc Networking (MANET)?

At the end of the discussion, participants agreed to include the environment Subscriber Unit to Subscriber Unit as a sub-element to the environment, System to Subscriber Unit (Last Mile Radio). Therefore, we concluded with a list of six environments, instead of the original seven.

Following completion of the descriptions, the participants prioritized the list of environments, based on the following criteria:

- What furthers interoperability?
- What most benefits the multi-jurisdictional, multi-agency responders?
- What provides the greatest impact, in the least amount of time for the least amount of dollars?

The prioritized list of environments is the following box:

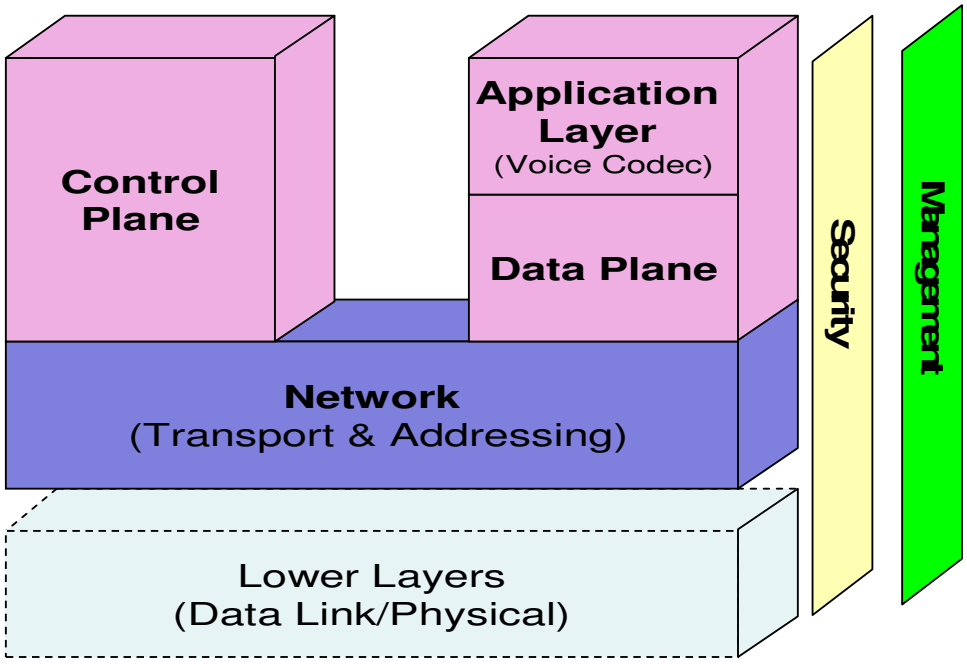
1. Bridging Systems Interface
2. Radio Site Interface
3. Radio System to Radio System Interface
4. Dispatch Interface
5. System to Subscriber Unit (Last Mile Radio)
6. Wired End Unit to System Interface

## *Implementation Profile Framework*

**Implementation Profile:** *The minimum set of standards, parameters, and values necessary to ensure interoperability in any of the given environments described*

On behalf of NIST/OLES, representatives from the Institute for Telecommunication Sciences assisted with a discussion among participants. Consensus was reached on the implementation profile framework shown below. It is the basic framework for creating implementation profiles for the respective environments.

**Implementation Profile Framework for VoIP**




Participants used the public safety requirements for VoIP (reliability, affordability, etc., shown in pg. 5) to discuss the specific technologies/solutions that would fulfill the implementation needs for each layer depicted in the figure.

Participants agreed to use this framework in creating implementation profiles for each of the environments (shown in pg. 8).

Within this framework, participants also agreed:

- Within the control plane, Session Initiation Protocol (SIP) is an appropriate protocol.
- Within the network layer, it was agreed to use IPv4, but with a roadmap to IPv6.

## *General Next Steps for Strategic Direction*

In concluding Part 1 of the meeting, participants agreed to next steps for the strategic direction of VoIP in public safety communications:

- Define the deliverable, the implementation profile:
  - Creation of interface "specifications"
- Discuss resources:
  - Prioritize with other concurrent efforts (e.g., P25).
- Explore options to complete this work:
  - NIST is an American National Standards Institute (ANSI)-accredited Standards Development Organization (SDO).
  - Create or use a "Global-like" organization.
  - Leverage (possibly*)* the Telecommunications Industry Association (TIA).
    - Have a follow-up meeting to initiate the profile for the bridging systems interface (due to prioritization), publish the findings, then turn over the profile to TIA for issuance of formal standard.
- Address intellectual property rights issues.
- Hold another meeting in mid-May or late-May 2007 at a relatively low-cost venue.

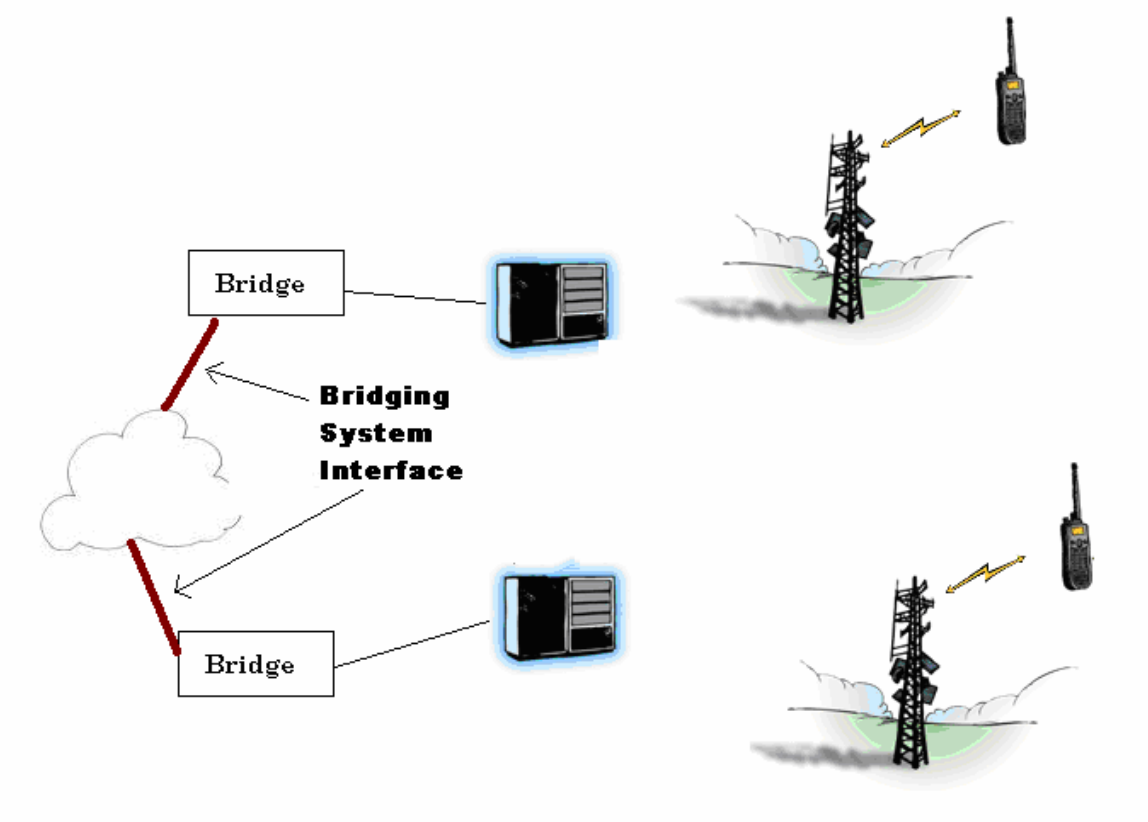
# PART II: TECHNICAL SPECIFICS (Days 3 and 4)

## *Outcomes Regarding Technical Specifics*

- Agreement on a working plan for an implementation profile on the bridging systems interface
- Commitment by stakeholders to continue the implementation profile development for the bridging systems interface

## *Bridging Systems Interface*

The following graphic depicts the topic that the environment meeting participants discussed in detail during Part II of the meeting: the bridging system interface.



**Assumptions** – Participants shared general assumptions about the bridging systems interface. Of note are the following assumptions about their architectures:

*Architectures*

- Stand Alone (On-Scene Tactical Patching):
  - Connecting disparate radios
  - Allows for On-Scene IP connectivity.
  - Local IP Network
- Stand Alone with Radio Infrastructure Connectivity:
  - Connecting to infrastructure
  - Requires backhaul connectivity.
  - Wide area connectivity
- Permanent: Integrated with Radio Infrastructure

**High-Level Requirements** – Participants gathered the following high-level requirements for the bridging systems interface in public safety:

*High-Level Functional Requirements*

- User to user voice communications across multiple bridging/gateway solutions
- Connections can be static or dynamic
- Ability to transmit priority information
- Arbitration of resources:
  - Transmit PTT management information
- Control plane solution for this interface be extensible for features other than voice:
  - Ability to transmit confirmed and unconfirmed call information
- Awareness of channels to which the user is connecting:
  - Operators need to know.
- Minimize lost audio by accommodating end-user access times:
  - Audio drop-outs can mean confusion between, e.g., someone saying, “Shoot!” or “Don’t shoot!”
- No statistically significant voice quality degradation:
  - Set the quality bar high.
  - Ability to measure the quality
  - Example: TSB-88 Delivered Audio Quality (DAQ) definitions

*High-Level Technical Requirements*

- Channel information embedded in the control, if available
- Originating bridge will carry all control information available:
  - Terminating device can accept/reject
- Basic call setup and teardown
- Capabilities exchange
- Choose a common set of codecs.

- Manage a high-latency, low-bandwidth link.
- Technical specs on access time and latency:
  - Where the parameters and their values are measured
    - Example: ITU-T Recommendations Y.1540 and Y.1541
- Define the packaging of voice data.
- Security Requirement:
  - Establish a privacy and integrity solution.
- Manage PTT signaling, and agree on how to transmit information.
- Must have a naming and addressing convention.
- Must perform management and provisioning of the networks.
- "Heartbeat mechanism" to ensure there is still a link or to maintain the link

**Specifics of Implementation Profile** – In an initial effort, participants began to discuss the implementation profile specifics for bridging systems interface. Below is a summary of their conversations:

*Control Plane*

Participants agreed that Inter RF Subsystem Interface (ISSI) and the Open Mobile Alliance Push-to-Talk Over Cellular (OMA PoC) provides much of what is needed. However, either would need refinement to have an adequate implementation profile for the bridging systems interface. Using the public safety requirements as a guide, participants considered and discussed the relative strengths and weaknesses of each option. As each is built on SIP, there was consensus for SIP over Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) as the control plane protocol, with RTP over UDP for the voice stream.

Other protocol considerations were discussed, but without reaching consensus.

Outstanding issues included:

- ISSI:
  - The need to be modified in order to emulate peer-to-peer communications
  - Lack of home RFSS
  - Extension would be needed to accommodate non-IMBE (Improved Multi-Band Excitation) vocoders.
  - Problem with the scalability of the naming convention
  - Vocoder list exchange functionality is missing.
  - No SIP routing information
  - Lack of tone signaling; lack ability to handle dual-tone multi-frequency (DTMF)
- OMA PoC:
  - No support for losing audio when floor is revoked
  - No formal support of early audio
  - It's unclear how the issue of who talks first on point-to-point calls would be handled in an land mobile radio system environment.

*Application Layer*

For the application layer, much of the discussion dealt with the selection of vocoders, in particular the advantage of using IMBE for its role in P25, and the disadvantage of using IMBE regarding its the licensing cost, even in its use for product development.

Agreements include:

- The G.711 standard will be required.
- Another vocoder will be selected, and required, for low-bandwidth communications.
- Standard option vocoders will include:
    - IMBE
    - G.729a algorithm
    - Global System for Mobile Communications
- Roundtable participants will address vocoder negotiation, and consider the ability to change during the VoIP communication if there's a change in bandwidth/latency.

*Data Plane*

Both RTSP and RTP/RTCP were discussed, but the value of the former was thought to be lessened should the interface use a secure tunnel between the bridging solutions. This approach is not without issues of its own, however. IPSec tunnels may impede the ability to multicast, for example. RTP also has issues, for example the ability to carry supplemental voice data, like caller ID.

*Network*

The following assumptions were reached:

- Use UDP/TCP for control.
- Use UDP for data.
- Use IPV4 with a roadmap for a transition to IPV6.

*Security*

The discussions dealt with the issue of security in only a preliminary manner. The topic of end-to-end encryption (which each environment may require as an option) took the most attention.

Other topics included:

- The need to address privacy and integrity in the implementation profile, with IPsec a leading candidate for a solution.

- Future control requirements for:
    - Authentication
    - Authorization
    - Non-repudiation

*Management*

The roundtable did not spend time choosing technologies for this layer. Still, it articulated some of the issues that an implementation profile would have to address. This was helpful in scoping the management areas of the project, as follows:

- Focus on network management:
    - Provisioning, or “administration”
    - Standardized Management Information Base
    - Loop prevention
- Operator control
- Decisions will be needed on whether to centralize or distribute management control.
- Ability to control devices and other items that are behind the bridging device (e.g., base stations, channels, squelch levels, etc.)

# Action Plan

In the final day of the meeting, participants developed a next-steps action plan for continuing the work of developing an implementation profile for bridging systems interface. There will be ongoing discussions to define the implementation profile specifics for the remaining environments.

Key Steps for Completing Implementation Profile for Bridging Systems Interface

*A. Develop Detailed Requirements* ***(at 3 months)***

- From the high level and user technical requirements
- Conops
- Operational Scenarios- high priority
  - Includes management and control
- Formalize Requirements

*B. Define Architecture* ***(at 6 months):***

- System IDs
- Naming conventions
- Demarcation points
- Management architecture
- Security architecture
- Define scope:
  - Phase I – Voice
    - An IP replacement for 4-wire interface between bridging solutions
  - Phase II – Additional features/data or control elements
  - Phase III – Management control functionality

*C. Develop a System Design* ***(at 12-15 months):***

- Entertain and evaluate proposals.
- Gap analysis:
  - e.g., starting points for analysis are ISSI vs. OMA PoC
- Performance analysis

*D. Develop the Interface Specs* ***(at 12-18 months):***

- Must have direction from OIC and NIST/OLES.

*E. Launch Implementation Phase* ***(at 18-24 months):***

- Spec updates
- Lessons learned
- NIST reference implementation of standardized system
- Errata

*F. Conduct Conformance/ Compatibility/ Interoperability Testing* ***(at 24 months)***

**Near-Term Action Plan**

| # | Description | Due Date | Owner |
|---|---|---|---|
| 1. | Define 24-month meeting schedule. | Next meeting | OIC and NIST/OLES |
| 2. | Draft operational scenarios:<br>Some solution providers offer these. | Next meeting | Raytheon and Catalyst |
| 3. | Develop draft reference model:<br>Bring proposals to May meeting. | Next meeting | Industry |
| 4. | Explain motivation for developing implementation profiles/specs:<br>▪ Provide supporting letters from participating organizations.<br>▪ Help manufacturers support a business case. | ASAP | OIC, NIST/OLES, and public safety |
| 5. | Develop group portal. | ASAP | BearingPoint, OIC, or NIST/OLES |
| 6. | Distribute Feb. 2007 meeting notes and slides. | ASAP | OIC and NIST/OLES |
| 7. | Comment on action plan and industry requirements. | End of March 2007 | All meeting participants |
| 8. | Explore potential interface with OMA. | Next meeting | Motorola |
| 9. | Conduct gap analysis between ISSI and requirements (pp. 12-13). | Next meeting | M/A-COM Inc.? EADS N.V.? |
| 10. | Conduct gap analysis of OMA PoC and requirements (pp. 12-13). | Next meeting | Motorola |
| 11. | Distribute to all straw man proposal for base audio over IP exchange to all. | Next meeting | Twisted Pair, etc. |
| 12. | Define a mechanism for handling potential intellectual property rights issues. | ASAP | OIC and NIST/OLES |
| 13. | Identify additional participants. | ASAP | All meeting participants |
| 14. | Start Outreach:<br>▪ *Interoperability Today*<br>▪ Industry Roundtable<br>▪ National Public Safety Telecommunications Council (NPSTC):<br>– E.g., One high-level white paper<br>– Verification<br>– "Plug Fest"<br>– NIST green light<br>– Beta testing | ASAP | OIC, NIST/OLES, and public safety |

# Appendix - Participant List

| Name | Title | Agency |
|---|---|---|
| 1. Ake, George | Project Coordinator | National Institute of Justice (NIJ) |
| 2. Atkinson, D.J. | Lead Electronics Engineer | NTIA-Institute for Telecommunication Sciences (ITS) |
| 3. Behnam, Kameron | Electronics Engineer | NTIA-ITS |
| 4. Botha, Shaun | CTO | Twisted Pair |
| 5. Chapman, Doug | V.P. Product Marketing | Tait Electronics |
| 6. Chu, Thomas P. | Distinguished Member of Technical Staff, Bell Laboratories | Lucent |
| 7. Clark, Melinda | OIC Contractor Support | DHS-OIC |
| 8. Clinch, Guy | Global Solutions Director: Government and Education | Avaya |
| 9. DeRango, Mario | Motorola Fellow, VP Advanced Technology | Motorola |
| 10. Engel, Jordan | OIC Contractor Support | DHS-OIC |
| 11. Floyd, Daniel | Senior Software Engineer | Raytheon |
| 12. Grier, Robin | President | Catalyst |
| 13. Hall, Doug | Senior Scientist | Raytheon |
| 14. Hall, Douglas | Technical Lead | Cisco |
| 15. Harris, Jeff | System Engineer | General Dynamics |
| 16. Harris, Phil | Communications Engineer | L3 GSI/NIJ CommTech L3GSI/National Law Enforcement and Corrections Technology Center-Northeast (NLECTC-NE) |
| 17. Jonker, Jared | OIC Contractor Support | DHS-OIC |
| 18. Jorgensen, Craig | Project Director, P25 | SAFECOM Emergency Response Council/Project P25 |
| 19. Kaluta, Roman | Director, Interoperability Solutions | Raytheon |
| 20. Klein-Berndt, Luke | Chief Technology Officer | DHS-OIC |
| 21. Martinez, Dennis | V.P. Technology | M/A-COM |
| 22. Mathis, Jim | Fellow of Technical Staff | Motorola |
| 23. McClellan, Roy | Director, Standards Development | EADS |
| 24. McEwen, Harlin | Chairman, Communications and Technology Committee | SAFECOM Executive Committee/International Association of Chiefs of Police |
| 25. Mitchell, Rob | Market and Technology Specialist | Twisted Pair |

| Name | Title | Agency |
|---|---|---|
| 26. Mudra, Andrew | OIC Contractor Support | DHS-OIC |
| 27. Nash, Glen | Supervising Telecommunications Engineer | SAFECOM Executive Committee/Association of Public-Safety Communications Officials (APCO) International |
| 28. Navarro, Bob | Asst. Deputy Chief | San Francisco Fire Department/Division of Homeland Security |
| 29. Orr, Dereck | Program Manager | NIST/OLES |
| 30. Perkins, Regina | OIC Contractor Support | DHS-OIC |
| 31. Powell, John | Senior Consulting Engineer Supporting DHS and DOJ | SAFECOM Emergency Response Council/International Association of Chiefs of Police |
| 32. Saluja, Harjot | Senior Product Manager | Airvana |
| 33. Schools, Michael | Manager of Engineering | Catalyst |
| 34. Sheldon, Dave | OIC Contractor Support | DHS-OIC |
| 35. Stafford, Robert | Electronics Engineer | ITS |
| 36. Stofer, Kristi | OIC Contractor Support | DHS-OIC |
| 37. Thiessen, Andy | Lead Electronics Engineer | ITS |
| 38. Unruh, Lincoln | Manager, Advanced Technology and Research | Bearing Point |
| 39. Wells, Carlton | Bureau Chief | State of Florida, State & Local Public Safety Radio Services |
| 40. White, Jennifer | OIC Contractor Support | DHS-OIC |
| 41. Wilson, Chris | Business/Technology Manager | Motorola |
| 42. Wilson, Richard | Senior Engineer | Nortel |