



**Office for Interoperability and Compatibility
Industry Roundtable**

June 2, 2008



Table of Contents

Welcome & Opening Remarks.....	1
PLENARY I: Information Sharing/Geographic Information Systems (GIS) for Emergency Response: Possibilities of the Future.....	2
PLENARY II: Industry Participation in Compliance Assessment Programs: Building Confidence into Your Product	4
PLENARY III: Voice Quality Issue: The Vocoder Challenge	6
Appendix A: Panelist Biographies	9

Welcome & Opening Remarks

The welcome and opening remarks were offered by Industry Roundtable sponsor, Dr. David Boyd, Director of the Command, Control and Interoperability Division (CID) of the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T).

Welcome to the third annual Industry Roundtable—designed to bring emergency responders, policy makers, and industry professionals together to collaborate on the most significant challenges facing interoperability.

The Challenge on the Frontline

- Interoperability is not solely a technology problem that can be solved with the “right” equipment or the “right” communications system. Interoperability is a complex, multi-dimensional issue.
 - Some technology solutions are useful for command elements but are impractical for individual emergency responders.
 - Over 60,000 local agencies are currently using equipment worth billions of dollars. Disregarding current investment in favor of one single solution is not feasible. Rather, we must work toward the common goal of tying systems together—within a system of systems framework—so that the right people at the right time can access the right information during an emergency.
- We must ensure that any system is, first and foremost, operable in an emergency—interoperability cannot exist if the infrastructure meant to support it isn't working.
- Emergency responders, including police officers, fire personnel, and emergency medical services, need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies.
- Many people assume that emergency response agencies across the Nation are already interoperable. In actuality, emergency responders often cannot talk to some parts of their own agencies or within their own locality—let alone communicate with agencies in neighboring cities, counties, or states.
- We must commit ourselves to constructing a dedicated, reliable, cross-discipline system of systems across the country.
- We rely on you, the members of industry, to listen to responders' needs and requirements and work in partnership with them to produce technology solutions. These solutions will work within the system of systems framework so that agencies' investments will continue to serve them even as technology advances and changes.

We Each Have a Role

- The Office for Interoperability and Compatibility (OIC) is working with the emergency response community, industry, and Federal partners to address the multiple dimensions of interoperability in order to improve local, tribal, state, and Federal emergency preparedness and response.
- The development of a successful solution to improve interoperable communications requires a focus on user needs and requirements. The input of both practitioners and policy makers across disciplines, jurisdictions, and levels of government must be included in any solution.
 - As a result, any strategy for improving emergency response interoperable communications must be based on user needs and driven from the bottom up.
 - Practitioner-driven input ensures that both industry and the Federal government's resources are aligned with responders' needs. We must work in partnership to produce technology solutions that will operate within a system of systems framework.

Our Charge for Today

- Today's focus is on new, innovative practices and tools that are changing the interoperability landscape and the role that we have to play.
- We must recognize that standards are the glue that will hold our emergency communications systems together during everyday emergencies and catastrophic events.
 - It is incumbent upon those developing responder tools to meet the needs of consumers—and put their needs first.

- Everyone benefits when industry participates in standards development processes and compliance assessment programs, and develops technologies at the lowest possible cost to the emergency response community.
- The key to improving the current state of interoperability is to develop technology solutions which are affordable to emergency responders.
- We should be able to change the business model that has been based on high-cost license fees and look at how to bring licensing costs down. Lowering costs will ensure that information sharing tools are available to all communities. During any emergency, responders must have access to the critical information they need to perform their duties.
- New technologies as well as new business approaches like those based on open source engineering and different licensing models will put more advanced tools into the hands of agencies. This will be especially beneficial for agencies that might not otherwise be able to afford them.

Conclusion

- We continue to look to our industry partners for better technologies that interoperate more effectively and best serve our emergency responders and the communities they serve.
- We encourage you to:
 - Continue bringing new ideas to the table.
 - Continue listening to the needs of the communities and responders you serve.
 - Continue working with the Federal Government to ensure that the Nation's emergency response community has the necessary tools and resources to ensure communications systems are interoperable when needed.

PLENARY I: Information Sharing/Geographic Information Systems (GIS) for Emergency Response: Possibilities of the Future

Moderator: Dr. David Boyd; Director; Command, Control and Interoperability Division; Science and Technology Directorate; Department of Homeland Security

Panelists

- Kevin McGinnis, Program Advisor, National Association of State Emergency Medical Services Officials
- Joe Ordia, President and Chief Executive Officer, Ordia Solutions
- Theresa Taylor, Commander, Beverly Hills Police Department
- Don Teesdale, Homeland Security Liaison with Maryland State Police Aviation Command

Session Synopsis

Within a system of systems framework, multiple systems—comprised of people, organizations, and technology—must collaborate to develop information sharing methods. When one independently owned system can connect with other local, regional, or state systems, the response community benefits from an improved flow of information and interoperability. Panelists for this session—representing local, state, and Federal efforts that use next-generation Geographic Information Systems (GIS) and information sharing technologies—described their use of the system of systems approach and invited industry to continue to develop these promising solutions.

Key Points

- The age of conventional computer-aided dispatch (CAD), emergency "portals," and database lookups is giving way to systems that are more dynamic, visual, open, interoperable, and multi-modal. New systems are based around mapping, and they create a real-time common operating picture.
- GIS/mapping tools have been used in the military for years. Today standards, competitors, and technical advances are putting these types of systems into the hands of emergency responders more frequently.
- These information sharing systems meet the current needs of responders and planners by providing a shared, complete image of what's going on with less latency.

Summary of Panelist Presentations

- Sergeant Don Teesdale
 - In 2004, Sergeant Teesdale began to focus on improving homeland security for the State of Maryland. He recognized that Maryland State Police were already frequently flying over Maryland's critical infrastructure. However, they were not maximizing their efforts by formally monitoring these sites.
 - Maryland State Police partnered with DHS and the Johns Hopkins University Applied Physics Laboratory to develop the Critical Infrastructure Inspection Management System (CIIMS) for the State. CIIMS offers aerial technology that allows Maryland State Police flight crews to exchange information about infrastructure sites with their partners on the ground.
 - Additional information is available at www.CIIMS.us.
- Commander Theresa Taylor
 - The Beverly Hills Police Department's goal was to develop technology-centric data and voice interoperability to enhance situational awareness for its Emergency Operations Center.
 - The Department developed a portal-based digital dashboard with a secure Web site and XML-based services.
- Joe Ordia
 - Ordia Solutions created the Command Post of the Future (CPOF) program, which allows management of ground resources without having to set up a command post in the field.
 - The virtual command post solution, which is currently focused on law enforcement, integrates personal Global Positioning Service units and has already been piloted in Philadelphia, Pennsylvania, and deployed in Washington, D.C.; Pittsburgh, Pennsylvania; and Richmond, Virginia.
- Kevin McGinnis
 - Mr. McGinnis proposed the Emergency Medical Services Resource Event Monitoring System (EMSREMS) to improve the lack of situational awareness that Emergency Medical Services (EMS) responders experience.
 - EMSREMS would provide an EMS responder a screen depicting the geographic area of interest to the user. The screen would also show the resources and emergency calls in the area and their status.
 - EMS and medical staff could access the EMSREMS through personal digital assistants; mobile data units in ambulances; or personal computers at the ambulance base, emergency room, or helicopter EMS crew desks.

Audience Questions and Answers

For air-to-ground transfer of information, are you syncing units when you get back on the ground?

- *Sergeant Teesdale:* Yes, we synchronize when we get back. The idea is to eventually sync in flight; however, we're not to that point yet. We bring the tablets and sync over the internet with a firewall and provide data back to the decision makers.

What speed is required for your system, and what if there is no network available?

- *Joe Ordia:* We get this question a lot—especially from rural areas. Our system is designed to run on any network that is 56 kilobits per second or higher. Many communities use a commercial wireless service. In Henrico County, Virginia, they use a commercial wireless data card. Some rural communities build their own wireless data infrastructure.

What type of encryption do you use?

- *Joe Ordia:* We use a Secure Sockets Layer at the software level. A lot of cities have their own Virtual Private Network built on top of commercial wireless infrastructure.

When your jurisdiction determines that a specific location is critical infrastructure, how do you vet that with local partners to validate that the location is critical to them and how do they vet their critical infrastructure with you?

- *Sergeant Teesdale*: This is always a concern. Industry knows what's venerable to them. Validating critical infrastructure needs to be done across local, state, and Federal lines. These methods are being developed and practiced.
- *Commander Taylor*: Some critical infrastructure that we are interested in is not located in Beverly Hills. Therefore, we don't have immediate information because we're not responsible for protecting that infrastructure, but we may still need the information. We look to Emergency Operations Center representatives in the region to share its regional critical infrastructure.

Technology exists that addresses 95% of the solution you described, Mr. McGinnis. For example, technology that provides medical surveillance (used in New York City on September 11, 2001), hospital bed resources, etc. Having been a CEO of a company with these capabilities, how does industry try to facilitate greater adoption of technology that is available?

- *Kevin McGinnis*: This is a key problem. I express the needs of EMS to those outside the EMS community and also talk to those inside the community to try and describe which direction we should head. No company has packaged these EMS functional needs into one system to appeal to an EMS user. They need to be integrated and shown to my colleagues. It's a case of "if they see it, they will come."

PLENARY II: Industry Participation in Compliance Assessment Programs: Building Confidence into Your Product

Moderator: Luke Klein-Berndt; Chief Technology Officer; Office for Interoperability and Compatibility; Command, Control and Interoperability Division; Science and Technology Directorate; Department of Homeland Security

Panelists

- Cynthia Cole, Business Operations Director of Standards and Strategy, Motorola
- Jim Downes, Director, Federal Communication Services Division, Office of Emergency Communications (OEC), Department of Homeland Security
- Chad Foster, Program Manager, Standard and Technology Branch, Incident Management Systems/Federal Emergency Management Agency, Department of Homeland Security
- Dereck Orr, Program Manager, National Institute of Standards and Technology (NIST) /Office of Law Enforcement Standards, Department of Commerce
- David Steingraber, Executive Director, Wisconsin Office of Justice Assistance

Session Synopsis

Compliance assessment programs provide industry the ability to formally demonstrate product compliance with a set of standards and provide assurance to the customer community that the compliant equipment or software they've purchased from one manufacturer will integrate with the compliant equipment or software of any other manufacturer. This session detailed two examples of compliance assessment programs: P25 CAP and the NIMS Supporting Technology Evaluation Program (STEP). With both programs, industry and practitioners agree that there is a need to carefully balance oversight against the administrative impact of a Compliance Assessment Program (CAP).

Key Points

- NIMS STEP
 - NIMS STEP provides an independent, objective third-party evaluation of commercial and government hardware and software products related to incident management. NIMS STEP compares NIMS products against a set of standards. The two standards currently in place are the Common Alerting Protocol—a standard message format for all hazards warnings—and Emergency Data Exchange Language—a standard for routing messages to specific locations or divisions.
 - The focus of NIMS STEP has been to provide responders with a common organizational structure, data management systems and software (data messaging standards), and collaboration tools (command and control). NIMS STEP, currently in the pilot phase, looks at

applicable protocols for all hazards involving single or multiple entities. Evaluations take place over a one week period in a controlled environment. Once up and running, an automated tool for vendors to apply will be available at www.nimsstep.org along with all program documentation.

- P25 CAP
 - Since DHS' creation in 2002, billions of dollars in Federal funding have been made available to improve interoperable communications. In addition, annual appropriations legislation has called for OIC to work in conjunction with NIST to create a P25 CAP. The P25 CAP operates as a framework for the assessment of independent laboratories to test manufacturers' P25 equipment."
 - Independent laboratories apply to NIST for recognition as being competent to test equipment for compliance with P25 standards. If recognized, these labs then test equipment and develop test reports indicating a product's compliance with P25 standards. Manufacturers will release a declaration of compliance known as a Supplier's Declaration of Compliance. Results from the tests will be summarized and released in Summary Test Reports. All of this information will be readily available to the emergency response community. The emergency response community will access this information in one location—the Responder Knowledge Base (www.rkb.us).
 - As more manufacturers produced equipment, users realized the importance of interoperability tests and those tests became the initial focus of P25 CAP. Without the P25 CAP, testing is informal and completed by manufacturers with little documentation and limited public reporting. Currently, state and local entities are only able to determine a product's compliance with P25 standards by requesting specific tests from the manufacturer. In the absence of the P25 CAP, this can be problematic for manufacturers such as Motorola, which receives an overwhelming number of requests for customer-specific/procurement-specific tests.
 - The Interoperability Process and Procedures Task Group defined some of the issues users had identified to deal with standards differences across manufacturers. At the same time, users recognized they had to think beyond interoperability by itself and establish a three-pronged compliance program focused on conformance, performance, and interoperability.
 - The P25 CAP establishes a repeatable process and increases the amount of information available to the emergency response community. It also offers this information in a standardized format so that emergency response officials can compare and contrast products. The Compliance Assessment Process and Procedures Task Group publishes a P25 CAP Test Standard and compliance-related Technical Service Bulletin. After this information is published, the P25 CAP Governing Board—representing the collective interest of organizations that procure P25 equipment—reviews the documents and publishes the effective date of any new testing requirements contained within by issuing a Compliance Assessment Bulletin (CAB). Based on these CABs, DHS publishes a revised test suite by which laboratories will be assessed for competence to conduct the new tests.

Audience Questions & Answers

When will lab assessments begin?

- *Dereck Orr*: NIST is currently waiting for clearance from the Office of Management and Budget on the lab application process. Our expectation is that we will begin accepting applications and evaluating labs in July 2008.

Are you only focusing on technology to achieve interoperability?

- *David Steingraber*: The P25 CAP simplifies the technology side leaving time to spend on other non-technical issues. For example, states, through the development of communications interoperability plans, are dealing with other lanes of the Interoperability Continuum such as standard operating procedures, training and exercises, and usage.

How are practitioners used in the process?

- *Dereck Orr*: Test procedures and test plans are all generated from the user side. P25 CAP came about from the user community in order to build confidence in a product's ability to meet P25 standards. P25 subject matter experts, current emergency response professionals, and government employees with the appropriate technical background will be used during lab assessments.

- *Audience Comment:* Practitioners have been used throughout the process and development of P25 and that will continue.

Cynthia, how big of an effort will it be to maintain and sustain the CAP, especially given that there are an increasing number of interfaces and products, and they are frequently changing?

- *Cynthia Cole:* Our key concern is evolving standards, the addition of new tests, and the impact of new interfaces. Smaller suppliers may face additional administrative burdens. Many infrastructure and equipment suppliers are smaller companies, and too many tests could stifle technological creativity.
- *Dereck Orr:* The program does not cover every single test. Users identify the most important standards, and the expansion of tests would be carefully targeted. Overall, Motorola sees the program as very positive and hopes the P25 CAP will bring about a sense of trust and transparency when emergency response entities procure P25 equipment.
- *David Steingraber:* Practitioner and policy-maker input is a key component of the P25 program; their involvement ensures that standards are realistic. As state's often take a system of systems approach to leverage regional dollars, ensuring interoperability across regions through the use of P25 is key. The Federal Government's role in compliance assessment programs needs to be determined on a case-by-case basis. In a perfect world, industry establishes its role and practitioners have confidence in that role.

PLENARY III: Voice Quality Issue: The Vocoder Challenge

Moderator: Denis Gusty; Acting Deputy Director; Office for Interoperability and Compatibility; Command, Control and Interoperability Division; Science and Technology Directorate; Department of Homeland Security

Panelists

- D.J. Atkinson, Lead Electronics Engineer, National Telecommunications and Information Administration (NTIA), Institute for Telecommunications Sciences (ITS)
- John Hardwick, President and Co-Founder, Digital Voice Systems, Inc.
- Dr. Ernie Hofmeister, Technology Fellow, Tyco Electronics M/A-COM
- Charles Werner, Fire Chief, City of Charlottesville, Virginia

Session Synopsis

Voice encoders, or vocoders, are at the heart of all digital communications systems, including the digital radio technology increasingly used by emergency response agencies. While digital radios offer better security, more efficient use of spectrum, and many other new features, the noisy environments in which they're used may pose challenges to the vocoders. This is largely due to the fact that vocoders need to identify and digitize speech above the noise of chainsaws and sirens. Other problems, such as channel errors and fading signals in moving vehicles, may plague the new digital systems more than the analog systems being replaced. This session addressed the actions that have been taken to ensure voice quality so that emergency responders can communicate effectively in critical situations.

Key Points

- In Fall 2006, some U.S. fire departments discovered that in the presence of background noises (common to fire operations), voice audio from digital radios may cause distortion to the degree of becoming unintelligible. These departments notified the International Association of Fire Chiefs (IAFC) and the International Association of Fire Fighters.
- On March 20, 2007, the IAFC issued a Member Alert on the issue.
- The IAFC formed a working group to clarify the problem and work with radio manufacturers and other stakeholders to identify and develop short- and long-term solutions.
- On May 8, 2007, the working group convened and established two sub groups (Testing and Best Practices).
- Fireground noise is both a vocoder and a radio issue.

- A vocoder translates voice into data and compresses the sound. When background noise is mixed in with voice, it's hard for the radio to distinguish between the two.
- Fireground noise is a basic communications issue, and it is also a multi-discipline challenge. There's an issue with signal-to-noise ratio. With narrowband, there's a lot of compression which puts constraints on the system. The community is aware that noise is a significant factor.
- Fireground is a tough environment, but the emergency response community is learning more about it. The vocoder and radio are elements. It will take many techniques and solutions to keep excessive noise out of the environment. It is difficult to process the signal once noise gets in. There's room for research in this area to develop new technologies to address this problem.
- Fire services would like to see voice quality comparable to analog voice quality in a digital environment.
- The vocoder is just one issue. We have to look at communications as a whole, including all system components. When new noise sources arise, each component has to work together, and all must acknowledge that there are tradeoffs when you add new technology to an existing environment.
- Cause of the voice quality and background noise issues
 - In a digital system, there's emphasis on bandwidth compression in order to achieve efficient spectrum usage. That's why we see a difference in voice quality between analog and digital systems. The vocoder works well for law enforcement; however, for fire service it's a challenge.
- Behavioral best practices
 - Users should be properly trained so that they understand their radio (even in noise environments), know when they're in a noise environment, and are aware of ways to shield themselves.
 - Some accessories may help (e.g., throat microphones), but it's not always realistic to use them in a fire environment. Be aware of this and adjust to the environment.
- Lessons learned
 - Make sure all disciplines are included in standards development to develop a universal quality standard.
 - Identify and provide funding to practitioners so they can participate in developing standards.
 - Traditional (non-noise) environments have been used when designing standards, and instead all environments should be considered.
- Discovery of voice quality issues in background noise
 - Knowledge of noise problems has existed for some time and a significant amount of testing has been conducted since 1993. Fire safety noise was missed due to a lack of industry experience about this environment. Since only certain technologies were available at the time, testing was conducted on what industry was aware of at the time and in the environments that were known problems at the time.
 - The proliferation of digital radios has helped bring this problem to the forefront.
- Future technologies that might improve sound quality
 - Industry is constantly working to improve the vocoder and there have been some strides to improve it through noise suppression.

Audience Questions & Answers

As we develop new vocoders, how hard will it be to implement into my system?

- *Ernie Hofmeister*: The upgrade is very dependent on the radio. Our baseline was the Improved Multi-Band Excitation (IMBE) vocoder developed in 1992. Along the way, improvements were made, including the Enhanced Vocoder which provided better noise suppression and additional processing capability. Old radios won't support the new vocoder, and you will have to migrate from the original vocoder to the enhanced vocoder over time.

In its upcoming report about the IAFC working group's findings, will NIST be an honest broker of information, identifying real-world issues beyond the lab environment?

- *D.J. Atkinson*: The recent partnership between NIST, ITS and the IAFC has helped. We can do a test that emulates environments, but the partnership helps by providing interpretation of those test results.

The IAFC will issue statements about what this means in the fireground context, and there will be a best practices document developed.

- *Charles Werner:* On June 3, 2008, the IAFC will provide a portable-radio best practices document for behavioral operations to help deal with fireground noise issues; however, it will not provide a recommendation on the use of digital radios.

Audience Comment: It's a fact that we will go into the future with fireground noise. For fireground, you need an analog system.

- *Charles Werner:* This reinforces the need for further testing. Digital is the future, and the question is how do we get there in a way that works for all involved? There are pros and cons, and one should be aware of the challenges. On June 4, 2008, NIST's scientific report will be released, which addresses the issue.
- *D.J. Atkinson:* And, the value of testing does not stop with a report. Manufacturers need to use the data to improve their products—that's the goal.

Audience Comment: In New York, we had an incident where a guy gave a mayday call and no one heard it. We experience high noise that turns off people's radios at the scene (simplex digital radio operation). We have times when it's just two guys talking and the radio can't determine what to keep in or leave out.

- *Charles Werner:* Again, this validates the need for testing. The manufacturers need to know our expectations.

Audience Comment: We measure all audio quality using analog as the standard. We have a difficult environment: we're on VHF and we will not transition to the new digital 700 megahertz (MHz) system. We need measures from the Federal Communications Commission (FCC) perspective that will allow us to operate analog on a trunked system, and we need industry to develop equipment that will allow an analog capability on a trunked system.

Audience Comment: On our fireground, we are experiencing 98 decibels of noise. We've tested it. We ask that you simulate our environment. We think industry has set the bar too low.

Appendix A: Panelist Biographies

D.J. Atkinson

D.J. Atkinson has been with the Institute for Telecommunication Sciences for 20 years, and is currently a Lead Electronics Engineer in the Telecommunication Systems Planning Division. Much of that time, Mr. Atkinson has been involved in the objective and subjective measurement of speech and voice quality, including 14 years in national and international standards, four years as vice-chair of the ITU Speech Quality Experts Group and two years as Vice-Chair of the P25 Advanced Programmable Interrupt Controller Vocoder Task Group. Mr. Atkinson has spent the last 10 years working to meet the needs of the emergency response community.

David Boyd

David Boyd is the Director of the Command, Control and Interoperability Division with responsibility for research and development (R&D) programs to support command and control, communications, computing, intelligence, surveillance, reconnaissance, cyber security and interoperability for DHS. Before joining DHS, Dr. Boyd served as the Director of Science and Technology for the National Institute of Justice, where he managed R&D programs in every facet of technology affecting law enforcement and corrections, including the forensic sciences, less than lethal technologies, information and communications technologies, and concealed weapons and contraband detection, among others. Dr. Boyd is a retired U.S. Army Officer and a recipient of the 2005 Presidential Rank Award, the highest recognition available in the Federal Civil Service. With graduate degrees in Management and Public Policy Analysis as well as a doctorate in Decision Sciences, he has also published extensively in military, law enforcement, technical, and general circulation publications.

Cynthia Cole

Cynthia Wenzel Cole is the Director of Standards and Strategy - Business Operations in System Infrastructure Operations Group of the Government and Public Safety Division at Motorola and has held that position since June 2007. Her team manages a variety of technology areas including P25 Standards, P25 CAP, Information Assurance, Encryption, Wireline Interoperability Gateways and Deployable Radio Frequency (RF) Sites. Over her 14-year Motorola career Ms. Cole has held a variety of positions such as Trunking System Portfolio Manager, leading the portfolio through transitions to P25 and to packet Internet Protocol-based architecture, and as a System Architect in the System Engineering group focusing on new over the air technologies. For the last two years she has led Motorola's P25 Inter RF-Subsystem Interface strategy, standards and productization efforts. Ms. Cole received a Bachelor of Science degree in Electrical Engineering - RF Design from the University of Michigan.

Jim Downes

Jim Downes is the Division Chief responsible for Integrated Services across all levels of government within OEC and has worked for more than 30 years in wireless communications, primarily in the public safety and Federal law enforcement areas. Prior to transferring to DHS in March 2003, he served as Director of the Wireless Programs Office in the U.S. Department of the Treasury. His responsibilities included oversight of the interoperability-focused efforts of the Public Safety Wireless Network Program. Mr. Downes also served as the Co-Program Manager for the Treasury-Justice Integrated Wireless Network, a joint activity to implement a shared nationwide land mobile radio system. His current responsibilities include management of the Federal Partnership for Interoperable Communications (FPIC), which involves a number of Federal user agencies in addition to state and local participants striving to improve interoperability at all levels of government. Mr. Downes also works closely with the Emergency Communications Preparedness Center, which serves as a Federal focal point for interoperability issues. He also represents DHS and the FPIC in Telecommunications Industry Association standards development activities.

Chad Foster

Chad Foster is the Program Manager for the NIMS Support Center, a program that operates under a cooperative agreement between the Federal Emergency Management Agency and the Justice and Safety Center/Eastern Kentucky University (EKU). In this capacity, Mr. Foster oversees the implementation of the program, which is designed to develop new responder tools, enhance technology integration and interoperability, and provide technical assistance and support to the incident management and response community. Before joining EKU in 2006, Mr. Foster served as Special Projects Coordinator for the Emergency Management Accreditation Program.

In that position, he was responsible for the implementation of special projects, including an assessment of the National Capital Region. From 2002 to 2005, Mr. Foster worked for the Council of State Governments where he directed and managed the organization's public safety and justice policy work. He also served in the U.S. Army for more than five years in various leadership positions both at home and abroad. Mr. Foster received a Masters in Public Administration from the University of Louisville and Bachelor of Science in Mathematical Science from the United States Military Academy.

Denis Gusty

Denis Gusty serves as the Acting Deputy Director of CID's OIC. In addition, he leads OIC's Data program which aims to improve incident response and recovery by developing tools and messaging standards that help emergency responders manage incidents and exchange information in real time. Mr. Gusty came to CID from the U.S. General Services Administration (GSA), where he served as the Director of GSA's Office of Intergovernmental Solutions. Prior to joining GSA, Mr. Gusty served as a Program Manager at the U.S. Department of Labor. In this role, he was responsible for helping to implement the President's Management Agenda by managing the e-Government initiative, GovBenefits.gov. Mr. Gusty has more than four years of experience in developing intergovernmental partnerships and information technology policy and practices.

John Hardwick

John Hardwick is President and Co-Founder of Digital Voice Systems, Inc. (DVSI) a leading worldwide supplier of voice compression technology. He was instrumental in the development of the IMBE vocoder used in P25, and he has been a key participant in the development of numerous vocoders for mobile radio, satellite telephony and other applications. Mr. Hardwick has served as President of DVSI since its founding in 1988. His previous employment included positions at Tektronix Inc, C.S. Draper Laboratories and the U.S. Army Applied Technology Laboratory (Ft Eustis). He holds 19 patents and is the author of several articles and papers on vocoders and related subjects. John Hardwick received a Bachelor of Science, Master of Science, and Ph.D. in Electrical Engineering from the Massachusetts Institute of Technology.

Ernest Hofmeister

Ernie Hofmeister has been employed with Tyco Electronics M/A-COM and its land mobile radio predecessor organizations in Lynchburg, Virginia, for over 15 years. Within this group, he has held various positions in the Systems Engineering, Design Engineering, and Technology departments. Currently, he holds the position of Distinguished Fellow of Technology in the company's Systems Technology group. Current responsibilities include: Coordination of technology strategies and direction; assessment of systems technology/products and potential business partners and suppliers; and provision of a technical position and liaison within the company, industry, and regulatory/standards groups. He previously served as M/A-COM's representative on the Steering Committee of the National Coordination Committee; this Committee provided consultation to the Federal Communications Commission on the rules for the new 700 MHz public safety spectrum. Dr. Hofmeister's formal education includes a Bachelor of Science in Electrical Engineering from Case Western Reserve University and a Master of Science and Ph.D. in Electrical Engineering from Syracuse University; he has also completed several technical and management training programs with General Electric.

Luke Klein-Berndt

Luke Klein-Berndt serves as the Chief Technology Officer for CID's OIC. He leads OIC's standards and technology efforts. He brings more than five years of communications technology experience to CID. Before joining CID, Mr. Klein-Berndt worked at NIST OLES. While there, he specialized in interoperable communications, including P25. He has an extensive background in computer science.

Kevin K. McGinnis

Kevin McGinnis began studying EMS systems in 1974, and has been an EMS system builder ever since. For the past seven years, he has been a Program Advisor for the National Association of State EMS Officials. He specializes in communications systems technology, data systems and rural EMS. Mr. McGinnis serves four other national EMS associations as communications technology advisor as well. He is Vice-Chair of the new 700MHz broadband Public Safety Spectrum Trust, vice-chair of DHS' SAFECOM Executive Committee, and vice-chair of that OIC's Practitioner Steering Group for Data. He received undergraduate and graduate degrees from Brown University and Cornell University in health care delivery systems and hospital administration, and has held Emergency Medical Technician (EMT), EMT-Intermediate and Paramedic licenses in New York and Maine.

Joe Ordia

Joe Ordia is President and Chief Executive Officer of Ordia Solutions, a company he co-founded in 2005 for the singular purpose of equipping public safety agencies and their front line personnel with next generation interoperable technologies to effectively communicate, collaborate, coordinate, command and control (5Cs of Interoperability) during critical incident and disaster response, major event security, multi-jurisdictional/multidisciplinary exercises, for infrastructure and border protection, as well as routine law enforcement and rescue operations. Prior to founding Ordia Solutions, he served as Chief Engineer at General Dynamics Viz for the U.S. Army's CPOF program from 2001-2003. He later served as project manager for the Defense Advanced Research Projects Agency (DARPA) CPOF Pattern Discovery program where he led a team of machine-learning experts in developing solutions to automate the flow of information between operators in the Army CPOF environment. Mr. Ordia was dispatched to Iraq for most of 2004 to execute the successful deployment of CPOF with the U.S. Army's 1st Cavalry Division, 3rd Infantry Division, and 24th Marine Expeditionary Unit. There he provided tactical system support during the first fielding of CPOF to operational units.

Dereck Orr

Dereck Orr is the Program Manager for Public Safety Communication Standards at NIST OLES, and has held that position since December 2002. Previously, he was detailed to DHS to serve as the Chief of Staff of the SAFECOM Office within S&T, to help establish the new program. Mr. Orr also served as a professional staff member of the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, and related agencies under Senator Fritz Hollings. In that position, he was responsible for the appropriations accounts relating to state and local law enforcement issues. Prior to that, he served four years at the Office of Community Oriented Policing Services (COPS) at the U.S. Department of Justice. At COPS, he held positions as a Management Analyst, Special Assistant to the Principal Deputy Director, and Budget Officer of the COPS Office. Mr. Orr received a Masters in Public Policy from the College of William and Mary and a Bachelor of Arts in American History from the University of Texas at Austin.

David Steingraber

David Steingraber chairs Wisconsin's State Interoperability Executive Council. Appointed by Governor Doyle to lead Wisconsin's Office of Justice Assistance in 2003, Mr. Steingraber also serves as President of the National Criminal Justice Association, a national organization representing local, tribal, and state criminal justice and juvenile justice practitioner interests to national policy makers. Mr. Steingraber also serves as a member of the Board of Directors for SEARCH, a nonprofit organization created by and for the states to identify and find solutions to improve justice information sharing. He has over 35 years of law enforcement experience and has served as Chief of Police for several Wisconsin communities. Mr. Steingraber also serves on the Governor's Homeland Security Council and is a former President of the Wisconsin Chiefs of Police Association.

Theresa Taylor

Theresa Taylor is a 27-year law enforcement veteran who presently manages two multi-million dollar projects for the City of Beverly Hills. She is the Commander of the Police Department's Administrative Services Division and has extensive technology project management experience, covering such technologies as closed circuit television, automated license plate recognition, radio infrastructure, and CAD systems. During her career, Commander Taylor has served as the Department's 9-1-1 Communications Manager and as Assistant Division Commander. In this position, she oversaw numerous law enforcement support services. She currently serves as the City of Beverly Hills representative on the Interagency Communications Interoperability System Governance Board, which provides interoperable radio communications to member agencies within the Los Angeles region.

Don Teesdale

Sergeant Don Teesdale serves as an aviator and homeland security liaison with the Maryland State Police Aviation Command. He also serves as the S3 Operations Officer for the 1/224th Aviation Security & Support Battalion of the Maryland Army National Guard. In this role, he is responsible for homeland security missions in the northeast region of the United States. Mr. Teesdale has 21 years of military and law enforcement experience in various aspects of aviation, intelligence and operations. He is dual rated in rotary and fixed wing aircraft and is credited with the initiation of an Airborne Critical Infrastructure Patrol process for police aviation. His request for

assistance from the Johns Hopkins Applied Physics Lab and DHS culminated in the implementation of the CIIMS project.

Charles Werner

Charles Werner is a 34-year veteran of the fire-rescue service and the present Fire Chief for the City of Charlottesville, Virginia. Chief Werner recently received the Virginia Governor's Award for Excellence in Fire Service Management; with this honor, he became the only recipient to win the Governor's Award for Excellence three times. A longtime champion of national and statewide interoperability progress, Chief Werner is a two-time Chair and present member of Virginia's Statewide Interoperability Executive Committee. He also serves on numerous local, state, and National interoperability working groups. As a contributing editor to Firehouse Magazine, Firehouse.com, and Mobile Radio Technology, Chief Werner has authored more than 70 nationally published articles. He is an At-Large Vice President for the Virginia Fire Chiefs Association, a member of the International Association of Fire Chiefs Communications Committee, a member of the National Public Safety Telecommunications Council Governing Board, and Chair of the International Association of Fire Chiefs Technology Council. In March 2008, Chief Werner was elected as Chair of the SAFECOM Executive Committee.