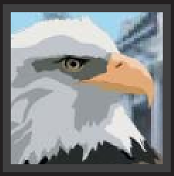
The InterAgency Board

2006 Annual Report
2007 Standardized Equipment List



Dedication

Dedicated to those brave Americans who stand forever vigilant to protect this country from those who would attempt to deny us our freedom. May their strength give us strength.

IAB Champions

Arlington County (VA) Fire Department

Austin (TX) Police Department

Austin-Travis County (TX) Emergency Medical Services

Boise (ID) Fire Department

Boston (MA) Fire Department

California Urban Search and Rescue Task Force 1

Centers for Disease Control and Prevention

Chicago (IL) Fire Department

Christus Schumpert Health System

City of Chicago (IL) Office of Emergency Communications

City of Las Vegas (NV) Office of Emergency Management

City of Tulsa (OK) Security

Contra Costa County (CA) Office of the Sheriff Star

Creve Coeur (MO) Fire Protection District/ FEMA Task Force 1 Urban Search and Rescue

Delaware Emergency Management Agency

Department of Defense, Joint Program Executive Office for Chemical and Biological Defense

Department of Defense, Research, Development and Engineering, Command, Edgewood Chemical Biological Center

Department of Homeland Security, Domestic Nuclear Detection Office

Department of Homeland Security, Federal Emergency Management Agency

Department of Homeland Security, Office of Grants and Training

Department of Homeland Security, Science and Technology Directorate

Douglas County (GA) Fire Department

Downers Grove (IL) Fire Department

Federal Bureau of Investigation, Hazardous Materials Response Unit

Fire Department, City of New York (NY)

Georgetown University Walsh School of Foreign Service

Homeland Security Management Institute, Long Island University/Naval Postgraduate School

International Association of Chiefs of Police

International Association of Fire Chiefs

International Association of Fire Fighters

International Personnel Protection

Jefferson County (CO) Sheriff's Office Bomb Squad

Kettering Fire Department/Ohio Task Force 1, FEMA Urban Search and Rescue

Lawrence Livermore National Laboratory

Lawrence (KS) Police Department

Los Angeles City (CA) Fire Department

Los Angeles County (CA) Fire Department

Los Angeles Sheriff's Department, Emergency Operations Bureau

Louisiana State Police

Massachusetts Department of Fire Services

Miami Township (OH) Division of Fire and EMS

Mid-America Regional Council

Montana Bioterrorism Training Project

Montgomery County (MD) Communications Center

Nashua (NH) Fire Department

National Association of Emergency Medical Technicians

National Bomb Squad Commanders Advisory Board

National Emergency Management Association

National Fire Protection Association

National Guard Bureau, Operations

National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

National Institute of Justice

National Institute of Standards and Technology, Office of Law Enforcement Standards

National Interagency Fire Center

National Memorial Institute for the Prevention of Terrorism

National Naval Medical Center

National Tactical Officers Association

New Castle County (DE) Police Department, Emergency Medical Services

New Orleans (LA) Police Department

New York State Police

Orange County (CA) Fire Authority

Orange County (CA) Sheriff's Department SWAT Team & Terrorism Early Warning Group

Orlando (FL) Fire Department

Orlando (FL) Police Department

Phoenix (AZ) Fire Department

Placer County (CA) Health and Human Services

Responder Knowledge Base

Sacramento County (CA) Sheriff's Department

Sarasota County (FL) Fire Department

Seattle (WA) Fire Department

Seminole County (FL) Sheriffs Office

South Central (PA) Counter-Terrorism Task Force

Suffolk County (NY) Police Department

Technical Defense

Technical Support Working Group

Terrorism Research Center

Texas Task Force 1 (TEEX)

Thayer School of Engineering at Dartmouth

United States Army Center for Health Promotion and Preventive Medicine

United States Army Natick Soldier RDEC

United States Capitol Police

United States Coast Guard, National Strike Force

United States Department of Health and Human Services

United States Occupational Safety and Health Administration

United States Department of Veterans Affairs

United States Environmental Protection Agency

United States Fire Administration

United States Marine Corps, Chemical/ Biological Incident Response Force

United States Marshals Service

United States Naval Research Laboratory

United States Secret Service

University of Connecticut

University of Montana

University of Toledo

University of Washington

Virginia Department of Emergency Management

Wake County (NC) Emergency Management

Walker County (GA) Emergency Services

Washington State Hospital Association

Yale University Emergency Medicine

Table of Contents

The InterAgency Board (IAB) 2006 Annual Report and the 2007 Standardized Equipment List (SEL)

2006 IAB Chair

Robert J. Ingram

Chief in Charge, HazMat Operations
Fire Department, City of New York

Robert Ingram is a 32-year member of the Fire Service, starting his 26th year with the Fire Department, City of New York. He is assigned as the Chief in Charge of FDNY's Hazardous Materials Operations Division. He has 20 years of experience in hazardous materials response and has worked on weapons of mass destruction issues since 1997. Chief Ingram's experience includes training, Federal Emergency Management Agency urban search and rescue, field operations, inter-agency exercises, and standards development. He has been a member of the IAB since 1999.

Letter from the Chair, Robert Ingram

2006 has been a very busy, exciting, and decisive year for the IAB. Our February meeting resulted in several charter changes, two of them significant in our path forward. The membership approved the formation of a new committee: the Compatibility and Interoperability Committee (CIC). This committee will support the work of the Interoperable Communications and Information Systems SubGroup as well as work with all of the SubGroups to identify compatibility and interoperability issues in responder equipment, systems, and training programs.

The membership voted to take a stand on the issue of "all hazards." Our charter was changed to focus on "all hazards with a special interest in WMD equipment issues." Since the Office for Domestic Preparedness and the Department of Homeland Security (DHS) began weapons of mass destruction (WMD) grant funding programs, first responders have used these funds for equipment that not only benefits terrorist and WMD response but can also be used in daily industrial accidents involving hazardous materials. Increasingly, this was done with the quiet acknowledgement of DHS grant managers, although politically and publicly, no one would admit this. Hurricane Katrina pushed this issue public, but still federal politicians and DHS officials were slow to change. The IAB strongly believes that it is necessary for the federal government to broaden homeland security to include "all hazards."

Our membership continues to grow with approximately 125 members, supported by subject matter experts in all SubGroup areas. More importantly, we have added law enforcement, health, and public works members at the local, state, and federal levels, strengthening our unique position of being able to provide a cross-disciplinary point of view to critical issues facing responders in homeland security. Our prioritized needs assessments are available to all federal agencies who are tasked to resolve interoperability and compatibility issues in equipment standards, technology, and training.

The IAB has shared its agenda with the International Association of Chiefs of Police's Homeland Security Committee, the International Association of Fire Chiefs' Hazardous Materials Round Table Group, and the standards developing community through the DHS Homeland Security Standards panels. The IAB stands firm in its commitment to require standards and testing for all equipment and training that will be used by first responders in the security of our homeland. We have reengaged with the Department of Defense (DoD) in several departments: research and development, laboratory testing, the 1401 Technology Transfer Program (providing military technology to first responders), and most recently the Guardian Program. This interface to share information on equipment systems and resource management will be critical in jurisdictions that are home to DoD installations.

In 2006, the IAB continued to communicate with the Occupational Safety and Health Administration (OSHA) on the issue of harmonization with the National Fire Protection Association (NFPA) in personal protective equipment (PPE) terminology, performance standards, and first responder training standards. Although it is a long and slow process, we are cautiously optimistic with the recent news that OSHA will seek public comments on 29 CFR 1910.120 in the late spring. The IAB will continue to seek and support revisions in this critical area and provide recommendations.

Two critical issues facing responders, particularly law enforcement members, in 2006 will continue to be a top priority in 2007: PPE and responder training and tactical competencies. The IAB has focused on bringing the National Institute for Justice and the NFPA together to address the critical issue of developing standards for PPE for law enforcement personnel. Five years after September 11th, 2001, and after countless millions of dollars have been spent on PPE, a memorandum of understanding between the two organizations was being drafted in the late fall of 2006, but the bottom line remains—the law enforcement community still does not have written standards. This effort must move forward.

The IAB worked hard in late 2005 and early 2006 with ASTM and NFPA to avoid possibly conflicting response standards for various disciplines in hazardous materials/WMD events. Law enforcement personnel, several from the IAB membership, were added to the NFPA 472 Committee to revise the standard to make it more applicable to all disciplines. A tremendous amount of work was done, changing the core competencies at the operations level to make them a solid foundation for all disciplines. Mission-specific competencies were added for agencies to choose from when developing training curriculums for their personnel tasked with more aggressive offensive missions. But based on recent conversations, more effort is required to address all responder needs and will remain a priority for the IAB in 2007. If we cannot integrate our multidisciplinary responses into a single standard, how can we expect to become interoperable?

Working with DHS Grants and Training representatives in our February and June meetings on the Exercise and Evaluations Guides, it became very clear to the IAB membership that we have serious concerns with the initial Target Capabilities List (TCL). A position paper was drafted, and as the chair I met with the leadership of the TCL group. Our concerns were its size, “in the weeds” detail, one-size-fits-all attitude, lack of a clear vision on how it should be used, the fact that it was not being used at the local levels, and the fact that Phase II was moving ahead without a thorough evaluation of Phase I. Recommendations included forming a committee to remove much of the detail into an appendix, making the document more user friendly, and drafting a front-loaded, clear description on the intended use of the document and the benefit to local and state agencies. We also recommended putting a hold on Phase II until an evaluation of Phase I was complete. I left the meeting with the feeling that the TCL group was being driven more by political timelines for a “product” than the idea of developing a useful tool. I was happy to receive news in late summer that a committee was being formed to review Phase I, our recommendations, and others submitted. Even better, it was to be co-chaired by local agency representatives. Our happiness was to be short-lived. After a few meetings, a reorganization occurred, and the committee is now headed by the same federal people who led the work on the initial TCL. How do you conduct an unbiased review of your own work? At the recent National Emergency Managers Association’s Homeland Security Meeting, several agency representatives voiced similar TCL concerns. The IAB and all organizations must continue to raise these issues in 2007 as well as provide recommendations.

In this coming year, the IAB will continue to support the NIOSH National Personal Protection Testing Laboratory (NPPTL) in its work on respiratory standards and testing, which has provided critical information for responders. We will continue to support Memorial Institute for the Prevention of Terrorism’s Responder Knowledge Base as a tremendous tool for local and state responders to use as a one-stop shop for DHS’ Authorized Equipment List, the IAB’s Standardized Equipment List, standards and test information, and specific manufacturers’ products. We will also be communicating with the Centers for Disease Control and Prevention for specific information on the use and effectiveness of N-95’s and other respiratory protection against exposures.

The IAB commitment to responder health and safety through standardization remains our top priority for 2007.

Out of many voices, one set of priorities.

Sincerely,

Robert Ingram, Chair, InterAgency Board

The InterAgency Board Charter

The IAB is a user-working group supported by voluntary participation from various local, state, federal government, and private organizations.

Mission

The InterAgency Board (IAB) for Equipment Standardization and Interoperability is designed to establish and coordinate local, state, and federal standardization, interoperability, compatibility, and responder health and safety to prepare for, train and respond to, mitigate, and recover from any incident by identifying requirements for an all-hazards incident response with a special emphasis on chemical, biological, radiological, nuclear, or explosive (CBRNE) issues.

Scope

The IAB supports local, state, and federal responders' efforts in homeland security by the following activities:

- Providing an independent operational viewpoint to federal agencies.
- Facilitating integration among local, state, and federal response communities to promote proper selection and use of the best available equipment and procedures to optimize safety, interoperability, compatibility, and efficiency.
- Developing, maintaining, and updating a Standardized Equipment List (SEL) which is aligned with the Authorized Equipment List (AEL) and provides the responder a reference to the type of equipment required to prepare for, train and respond to, mitigate, and recover from an all-hazards incident with a special emphasis on CBRNE issues.
- Advocating for, assisting in, and promoting the development and implementation of performance criteria, standards, requirements and test protocols for AEL/SEL-listed all-hazards incident response equipment with a special emphasis on CBRNE issues.
- Encouraging the coordination of local and state response communities with established military and federal acquisition programs for procurement of AEL/SEL-listed all-hazards incident response equipment with a special emphasis on CBRNE issues.
- Sharing knowledge, expertise, and technology regarding the detection, identification, warning, protection, decontamination, response management, and medical management of all-hazards incidents among local, state, and federal response communities with a special emphasis on CBRNE issues.
- Providing a structured forum for the exchange of ideas among operational, technical, and support agencies for national preparedness to promote interoperability and compatibility among local, state, and federal response communities.
- Identifying and prioritizing all-hazards incident response equipment requirements with a special emphasis on CBRNE issues.
- Encouraging manufacturers and governmental, military, and private agencies to sponsor priority research and development projects to satisfy local, state, and federal all-hazards incident response equipment requirements.
- Providing assistance and/or guidance to agencies, associations, and manufacturers, requiring operational testing of new and emerging equipment and technologies.
- Preparing and publishing an annual report to articulate the activities and accomplishments of the IAB.

Organizational Structure and Responsibilities

***IAB Chair*—The IAB Chair is selected from the ranks of the local and state membership. Confirmation shall occur by a simple majority vote of the general membership present at the meeting at which the annual report is finalized. The Chair is elected to a two-year term starting the first meeting of odd years. The Chair administers, organizes, and facilitates the actions of the IAB. The Chair provides recommendations to the Federal Agency Coordinating Committee and direction to the SubGroup chairs.**

***Federal Agency Coordinating Committee (FACC)*—A coordination committee that provides the interface between the IAB and sponsoring federal government agencies. The FACC consists of the federal officials from contributing agencies and departments. The FACC shall:**

- Coordinate and leverage ongoing federal research, development, testing, and evaluation (RDT&E) efforts to meet the responder requirements as identified and prioritized by the IAB.
- Solicit and coordinate mission support for the IAB, which includes activities such as organizational staff support, contributory funding, project sponsors, meetings, technical support, the IAB business cycle, and resulting products.
- Meet with the IAB Chair on a regular basis to review SubGroup recommendations and actions.
- Meet to coordinate federal requirements for action by the IAB.
- Attend general membership meetings.
- Review and approve the annual operating budget for the IAB, and maintain a support staff to facilitate the operation of the IAB.

SubGroups/Committees

- ***SubGroups*—**The IAB has five SubGroups as listed below. The SubGroups are composed of subject matter experts who address domestic preparedness equipment, systems, and protection issues related to a specific commodity area. The role of each SubGroup is to maintain and update its portion of the SEL and to address the ways and means by which technology can support all-hazards response concerns. Additionally, the SubGroups take the lead for developing the functional requirements for equipment, identify interoperability and compatibility issues, and develop priorities for standards development within their respective commodity areas. The SubGroups identify existing standards that may be incorporated into the Equipment Standards Suite without change, identify standards that may be incorporated into the suite after modification, and recommend areas for development of standards where none currently exist.
  - Personal Protective and Operational Equipment (PP&OE)
  - Detection and Decontamination (D&D)
  - Interoperable Communications and Information Systems (ICIS)
  - Medical (MSG)
  - Training (TSG)
- ***Committees*—**The IAB has three additional Committees:
  - Standards Coordination Committee (SCC) consists of SubGroup and Committee co-chairs and subject matter experts from various standards-development organizations. The SCC is responsible for coordinating all-hazards equipment, training, and operational standards projects of the IAB SubGroups with other organizations and enforcing authorities. As the

various SubGroups of the IAB determine minimum performance, reliability, quality, and other qualification requirements for their respective commodities, the SCC, representing regulatory, consensus, and voluntary standards organizations, will endeavor to create national harmonization by incorporating the requirements into their standards. The SCC will also serve as a reviewer during the development of qualification requirements by other SubGroups to:

    - ◆ Alert SubGroups and request reconciliation when contradictory requirements for complementary equipment are proposed;
    - ◆ Alert SubGroups when proposed requirements are contradictory to federal or state regulations;
    - ◆ Raise attention to similar or additional requirements under internal development within the regulatory, consensus, and voluntary standards organizations; and
    - ◆ Provide technical and nontechnical advice for improvements.

  - Science and Technology (S&T) consists of SubGroup and Committee member representatives and subject matter experts in the research and development (R&D) field. The mission of the S&T Committee is to identify interagency (local, state, and federal) first responder R&D requirements and innovative technologies (fieldable in the next 6 months to 5 years) that address all-hazards detection, individual and collective protection, medical support, decontamination, communications systems, information technology, training, and operational support.
  - Compatibility and Interoperability Committee (CIC) consists of member representatives and subject matter experts who address domestic preparedness equipment, systems, and protection issues related to specific interoperability and compatibility issues.

- *Co-Chairs*—Each SubGroup/Committee elects two co-chairs, one from the local and state ranks and a second from federal ranks. The co-chairs shall be elected for two-year terms with the elections for the local/state co-chair and the federal co-chair being conducted on alternating years. The first local and state co-chair will have a term of one year to achieve this alternating cycle. Co-chairs may be re-elected when their term has ended; there are no "term limits" for the co-chairs. The duties of SubGroup/Committee co-chairs are as follows:
  - Direct the efforts to accomplish the scope of IAB activities as identified in this charter.
  - Provide liaison with the IAB Chair.
  - Complete and provide to the chair, via the support staff, all administrative reports as required by the IAB Chair.
  - Serve as a member on the SCC.
  - Provide membership recommendations. It is the responsibility of the co-chairs to review membership participation annually and to ensure SubGroup membership represents the interest across the entire responder community.
  - Assign a SubGroup member representative to liaison with other SubGroups and Committees as needed or directed by the IAB Chair.

- *Membership*
  - Participate in the SubGroups/Committees and lend their expertise and support to the IAB Mission.
  - SubGroup/Committee membership will be limited to 20 voting members.

- SubGroup membership may be augmented with additional subject matter experts, as non-voting members, for specific projects or with members of other SubGroups in a nonvoting status.
- Nomination for membership can be made by any IAB member to the SubGroup/Committee co-chairs.
- Members are appointed by a majority vote of the two SubGroup/Committee co-chairs and the IAB Chair.
- Individuals may serve as voting members in only one SubGroup; however, they may participate in a nonvoting status in other SubGroups.

Execution

The IAB shall conduct its mission during three formal board meetings annually and SubGroup/Committee sessions and working groups as needed.

- Meeting agendas will be set by the IAB Chair.
- Agenda work items shall include, but not be limited to:
  - Publish an Annual Report of work
  - SEL data development and publication
  - Prioritization of equipment, standards, and training requirements
  - Evaluation of existing standards that link to AEL/SEL items
  - Establish the priority needs of the responder community regarding equipment, standards, interoperability and compatibility, and training issues and gaps

The InterAgency Board Structure

The IAB is organized into Committees and SubGroups that are chaired by a First Responder, supported by a Federal Co-Chair, and staffed with subject matter experts in that Committee's/SubGroup's area of interest. Each Committee/SubGroup is responsible for maintaining its subsection of the Standardized Equipment List (SEL). The Federal Agency Coordinating Committee is the exception as it is chaired by a Federal Chair and composed of supporting federal government representatives.

The InterAgency Board (IAB)

The IAB Chair is selected from the ranks of the local and state membership. The Chair administers, organizes, and facilitates the actions of the IAB.

State & Local Chair
Robert J. Ingram, HazMat Operations - Fire Department, City of New York

Federal Agency Coordinating Committee (FACC)

The FACC is a coordination committee that provides the interface between the IAB and sponsoring federal government agencies.

Federal Chair
Les Boord, National Institute for Occupational Safety and Health (NIOSH), National Personal Protective Technology Laboratory (NPPTL)

Standards Coordination Committee (SCC)

The SCC ensures that weapons of mass destruction (WMD) response equipment and technology is integrated in the existing standards boards and regulatory bodies.

Co-Chair
Glenn P. Jirka, Miami Township (OH) Division of Fire and Emergency Management Service (EMS)

Federal Co-Chair
Kathleen Higgins, National Institute of Standards and Technology (NIST), Office of Law Enforcement Standards (OLES)

Science and Technology (S&T) Committee

The S&T Committee is focused on advanced concepts entering development and newly emerging technologies that might be applied to crisis and consequence management.

Co-Chair
Vincent Doherty, Long Island University/Naval Postgraduate School

Federal Co-Chair
Gabriel Ramos, Technical Support Working Group (TSWG)

Compatibility and Interoperability Committee (CIC)

The Compatibility and Interoperability Committee (CIC) serves as the focal point for the coordination of interoperability and compatibility issues identified by the IAB. The CIC consolidates and prioritizes equipment, standards, training and operational interoperability and compatibility concerns identified by the IAB SubGroups and Committees.

Co-Chair
Robert Ingram, HazMat Operations, Fire Department, City of New York (FDNY)

Federal Co-Chair
Philip Mattson, National Institute of Standards and Technology (NIST), Office of Law Enforcement Standards (OLES)

Personal Protective and Operational Equipment (PP&OE) SubGroup

The PP&OE SubGroup addresses individual equipment, support systems, and area protection for WMD response.

Co-Chair
Douglas Wolfe, Sarasota County (FL) Fire Department

Federal Co-Chair
William E. Haskell III, National Institute for Occupational Safety and Health (NIOSH), National Personal Protective Technology Laboratory (NPPTL)

Interoperable Communications and Information Systems (ICIS) SubGroup

The ICIS SubGroup deals with communications, information management, technical information support, and public awareness issues.

Co-Chair
Christopher Lombard, Seattle (WA) Fire Department

Federal Co-Chair
William Snelson, United States Marshals Service

Detection and Decontamination (D&D) SubGroup

The D&D SubGroup concentrates on intrusive and non-intrusive detection; monitoring, sampling, and analysis of suspected toxins; and methods to mitigate or dissipate a contamination.

Co-Chair
James Schwartz, Arlington County (VA) Fire Department

Federal Co-Chair
Elaine Stewart-Craig, Research, Development and Engineering Command (RDECOM), Edgewood Chemical and Biological Center (ECBC)

Medical SubGroup (MSG)

The MSG engages the issues of casualty treatment for victims of a conventional or non-conventional WMD attack and also preventive measures to avert victimization.

Co-Chair
Thomas Walsh, Seattle (WA) Fire Department

Federal Co-Chair
Stephen Skowronski, Centers for Disease Control and Prevention (CDC)

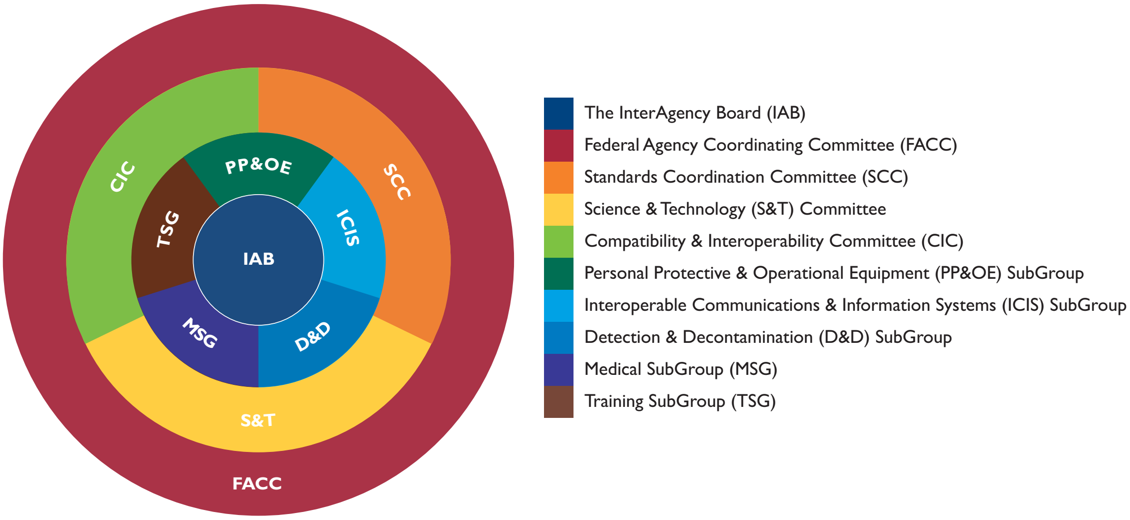
Training SubGroup (TSG)

The TSG aims to improve responder mission performance through review of and input to training, doctrine, and guidance.

Co-Chair
Alan "A.D." Vickery, Seattle (WA) Fire Department

Federal Co-Chair
Barbara Biehn, Department of Homeland Security, Office of Grants and Training (G&T)

Organizational Chart


CIC
PP&OE
SCC
TSG
ICIS
IAB
MSG
D&D
S&T
FACC
The InterAgency Board (IAB)
Federal Agency Coordinating Committee (FACC)
Standards Coordination Committee (SCC)
Science & Technology (S&T) Committee
Compatibility & Interoperability Committee (CIC)
Personal Protective & Operational Equipment (PP&OE) SubGroup
Interoperable Communications & Information Systems (ICIS) SubGroup
Detection & Decontamination (D&D) SubGroup
Medical SubGroup (MSG)
Training SubGroup (TSG)

Mission

The Federal Agency Coordinating Committee (FACC) provides the interface between the IAB Chair and the sponsoring federal government agencies. It coordinates the interests and initiatives of the federal community with the first responder community.

Membership

The FACC includes the U.S. Department of Defense (DoD); the U.S. Department of Homeland Security (DHS), which includes the Federal Emergency Management Agency (FEMA), the Office for Grants & Training (G&T), and the Science and Technology Directorate; National Institute for Occupational Safety and Health (NIOSH)/National Personal Protective Technology Laboratory (NPPTL); and the National Institute of Standards and Technology (NIST)/Office of Law Enforcement Standards (OLES). A brief description from each of the federal partners is listed below.

Department of Defense—Chemical and Biological Defense Program

The Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Programs [ATSD(NCB)] leads the Department of Defense (DoD) Chemical and Biological Defense Program (CBDP). Acquisition and advanced development of Chemical and Biological Defense related materiel is the responsibility of the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD). The Special Assistant to the Secretary of Defense (Chemical and Biological Defense) [DATSD(CBD)] assists in the oversight of this program. The CBDP is a key part of a comprehensive national strategy to counter the threat of chemical and biological (CB) weapons as outlined in The National Strategy to Combat Weapons of Mass Destruction (WMD), December 2002.

Chemical and Biological defense capabilities must support the diverse requirements of military operations supporting national security as well as homeland security missions. The CBDP funds research to exploit leading-edge technologies to ensure that U.S. forces are equipped with state-of-the-art capabilities to defend against CB threats through the far term.

Federal Agency Coordinating Committee (FACC)

CHAIR

Les Boord
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

Membership

Barbara Biehn
Department of Homeland Security, Office of Grants and Training

Bert Coursey
Department of Homeland Security, Science and Technology Directorate

Kathleen Higgins
National Institute of Standards and Technology, Office of Law Enforcement Standards

Pete Nacci, PhD
Department of Homeland Security, Office of Grants and Training

Michael Walter, PhD
Department of Defense, Joint Program Executive Office for Chemical and Biological Defense

Through the DoD Installation Protection Program, the CBDP has significantly strengthened its efforts for protecting its installations against chemical, biological, radiological, and nuclear (CBRN) threats. This program includes providing those emergency response personnel responsible who for responding to CBRN events at an installations with the equipment and training they need to protect them and respond to the event.

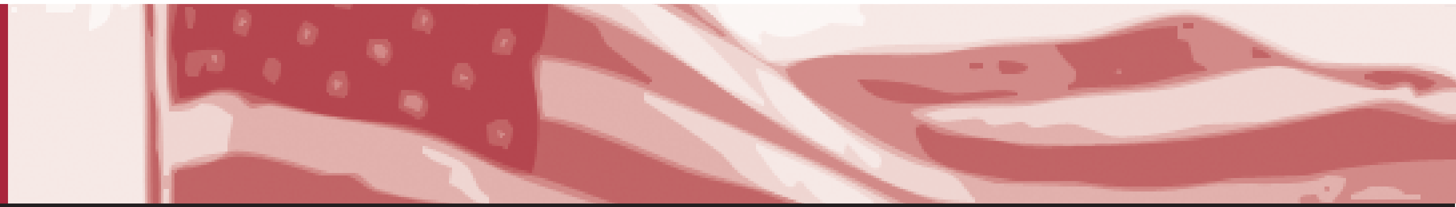
As one of the founding organizations of the IAB, DoD continues to support all facets and areas of the IAB. DoD personnel serve on the FACC, participating in the development the overall IAB strategy, and hold memberships in all SubGroups and Committees in the IAB.

Department of Homeland Security, Office of Grants and Training

The Office of Grants and Training (G&T) contributes to the Department of Homeland Security's critical preparedness mission by enhancing the capacity of States, territories, local agencies, tribal governments, and the private sector to prevent, protect against, respond to, and recover from incidents of terrorism, natural disasters, and other emergencies. G&T provides a broad array of assistance to America's emergency responders through funding, coordinated training, equipment acquisition, technical assistance, and support for State and local exercises.

G&T assistance programs are designed to assist jurisdictions in meeting the target capabilities and national preparedness priorities prescribed by the National Preparedness Goal. The eight national preparedness priorities are:

- Regional Collaboration
- Implementation of NIMS and the National Response Plan
- Implementation of the National Infrastructure Protection Plan
- Communications Interoperability
- CBRNE Detection, Response, and Decontamination
- Medical Surge and Mass Prophylaxis
- Citizen Preparedness
- Planning



Department of Homeland Security, Science & Technology Directorate

The DHS S&T Directorate serves as the primary R&D arm of homeland security, using the nation's scientific and technological resources to provide federal, state, and local officials with the technology and capabilities to protect the homeland. The focus is on catastrophic terrorism—threats to the security of our homeland that could result in large-scale loss of life and major economic impact. S&T's work is designed to counter those threats by both evolutionary improvements to current technological capabilities and development of revolutionary, new technological capabilities. The Standards Office, within S&T, is the organization through which DHS adopts standards, and it is important to note that the first standards adopted by DHS were those adopted by the IAB. The S&T Standards Office provides the majority of the funds that support the standards development requirements identified by the IAB.

National Institute of Standards and Technology, Office of Law Enforcement Standards

NIST is America's premier national laboratory for metrology and standards. An agency of the U.S. Department of Commerce, NIST was charged at its founding in 1901 with advancing measurement science, standards, and technology in support of U.S. industry and the country's economic security and quality of life. As technology progressed, NIST's capabilities expanded into world-class expertise in chemistry, physics, manufacturing, materials engineering, building and fire research, optics, electronics, and electrical engineering. Today, NIST is recognized worldwide as a leader in many areas of science and technology and boasts a history that includes three Nobel Prize laureates.

Beginning with the Great Baltimore fire in 1904 and the rise of forensic sciences in the 1910s, government agencies concerned with public safety and security turned to NIST for technical assistance. For decades, these cooperative efforts were informal. In 1971, in response to a Congressional mandate, NIST created its Office of Law Enforcement Standards to partner with the U.S. Department of Justice and other agencies in establishing minimum performance standards for critical law enforcement equipment, such as body armor, handcuffs, metal detectors, and mobile radios. Here, too, NIST's capabilities quickly expanded to include technologies used by the fire service, corrections and security personnel, and forensic investigators.

OLES was invited to join the IAB Standards Coordination Committee in 1999. In 2000, the office was named executive agent of the standards development effort and quickly organized a coalition of government agencies and professional associations that has been extraordinarily effective in developing performance standards related to CBRNE detection, decontamination, and personal protection technologies and in issuing publications that help agencies select, maintain, and properly use this equipment. The performance standards developed by the coalition have been adopted by DHS as a basis for equipment procurement at all levels, and a multiyear plan is in place to continue this important work.

National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

The National Institute for Occupational Safety and Health (NIOSH) conducts a range of efforts in the areas of research, information, and service. The NIOSH program portfolio focuses on relevance, quality, and impact. This is achieved through strong involvement of partners and stakeholders through the entire research continuum (conceiving, planning, conducting, translating, disseminating, and evaluating). The programmatic and support structures provide a foundation for staff to carry out its mission to provide national and world leadership to prevent work-related illnesses and injuries.

The NIOSH program portfolio is organized into eight sectors representing industrial sectors and 15 cross-sector programs around adverse health outcomes, statutory programs, and global efforts. The personal protective technology (PPT) cross-sector mission is to prevent work-related illness and injury by advancing the state of knowledge and application of PPTs. The technology includes the technical methods, processes, techniques, tools, and materials that support the development and use of personal protective equipment (PPE) worn by individuals to reduce effects of their exposure to a hazard.

NPPTL was created by NIOSH in 2001 when Congress underscored the need for improved PPE and encouraged research for PPTs. The mission is to prevent work-related injury and illness by ensuring the development, certification, deployment, and use of PPE and fully integrated intelligent PPE ensembles. This will be accomplished through the advancement and application of PPT standards.

NPPTL is organized into three branches: Technology Evaluation, Technology Research, and Policy and Standards Development. While the work of the laboratory addresses all PPE, respiratory protection is the cornerstone of NPPTL's activities.

The Technology Evaluation Branch performs testing, evaluation, and quality assurance checks. More than 8,500 approvals have been issued to approximately 85 approval holders at more than 100 manufacturing sites in 18 countries. The objective of the respirator certification program is to ensure that workers have access to respiratory protection that meets appropriate standards. Products are evaluated for compliance with applicable provisions of standards before manufacturers are permitted to label the respirator as NIOSH-approved. The quality program conducts periodic audits of respirator performance and investigates reported problems with deployed units to ensure continued compliance of previously approved respirators.

The Technology Research Branch conducts research related to innovative technologies for respiratory protection, sensors for PPTs, human performance, and PPE ensembles, including ensembles for first responders that provide improved protection against CB agents. Some of the group's projects address technical aspects of respirator fit testing, including a facial anthropometrics program to establish respirator fit test panels, determining the appropriate frequency and percentage of respirator fit test failures that require the user to change respirator model or size, and validating the annual fit-testing requirement. The branch is also investigating the potential of enhancing respiratory protection through recent advances in nanotechnology. In addition, the branch is working on further developing and applying mathematical models to help predict end-of-service-life and changeout schedules for respirators. Researchers are developing innovative methodology for evaluating overall integrity of protective ensembles against chemical and aerosol hazards. Other research involves permeation calculators for chemical-protective clothing.

The Policy and Standards Branch develops and updates standards to ensure the safety and health of respirator users. This group is working on a quality assurance module that will align the 42 CFR Part 84 standards with contemporary quality assurance practices and procedures. Criteria for total inward leakage are being established as a requirement for the certification of respirators. This branch also develops guidance documents to assist first responders in the use of equipment designed to protect against chemical, biological, radiological, and nuclear agents. The Policy and Standards branch is also involved in developing standards that will be used to protect respirator users against CBRN agents.

NPPTL applies state-of-the-art science to meet the increasingly complex occupational safety and health challenges of the 21st century. Our strategic research programs will ensure that the development of new PPE technologies keep pace with the changing needs and requirements of employers and workers.

Role and Functions

The FACC provides the funding for operation of the IAB. Continued representation by multiple federal agencies allows the IAB to maintain its independence as an organization as well as to best use the resources and expertise of the federal community. Those agencies/departments that fund the IAB have voting rights on the FACC.

Upon unanimous agreement between the federal partners, NIOSH served as the FACC Chair of the IAB in 2006. The FACC Chair is elected on an annual basis.

The FACC leverages ongoing federal RDT&E efforts to meet the responder requirements as identified by the IAB. The Chair of the IAB and the FACC work together to prioritize initiatives within the IAB and the federal community. The FACC also coordinates ongoing IAB initiatives within the federal community to ensure task completion and to prevent duplication of efforts. This interagency relationship benefits both the IAB and the federal community by improving protection and response.

Highlights for 2006

- SEL published in Annual Report, and available for download from the IAB website. The SEL is also available interactively on the Responder Knowledge Base (RKB), which is funded by DHS G&T through the Memorial Institute for the Prevention of Terrorism (MIPT).
- Established IAB Compatibility and Interoperability (CIC) Committee. Established mission, updated IAB charter, outlined objectives, and secured initial membership for Committee.
- Significant accomplishments in aligning content and taxonomy of the AEL with the SEL with the Responder Knowledge Base (RKB). Continued coordination with the RKB.
- IAB members reviewed and provided feedback to DHS on the Universal Task List and Target Capabilities List.
- Increased IAB visibility with booth exhibitions at GOVSEC/US LAW/READY and FPED.
- Supported conferences with panel and speaking engagements from IAB members at over 15 conferences and events including the "Technologies for Critical Incident Preparedness Conference".
- Continued development of the IAB website and list-serve capabilities with integrated profiles, live calendar, polling backbone, automatic updated mailing lists - creating a one stop data repository able to be updated by IAB membership and Program Office staff.
- Updated the IAB Charter to reflect the CIC Committee and adopted charter revisions.
- Continued management of "Strategic Planning" work session and subsequent "Ad Hoc" group for long term strategic planning.
- Collaborated with RKB on the establishment of a WEBEXONE site for IAB Co-Chairs and IAB Program Office reporting and (SCC and S&T) priority list management.
- Electronic integration and updated process for S&T requirements matrix into the RKB. Implemented a new S&T prioritization process to gather SubGroup S&T requirements.
- Management of over 20 IAB meetings, work sessions, or related meetings with IAB member participation.
- Provided multiple agency funding for continued operation of the IAB.

The FACC continues to work with the SCC to address the IAB's list of priorities, particularly with the development of CBRNE equipment standards, and to coordinate this development with other public and private standards development organizations, both within and outside the federal government.

The FACC reviews and approves the annual operating budget for the IAB and maintains a support staff to facilitate operations. The FACC meets with the IAB Chair on a regular basis to review SubGroup recommendations and action items.

FACC Chair

Les Boord

Director
National Personal Protective Technology Laboratory,
National Institute for Occupational Safety and Health

Les Boord's current position is Director, National Personal Protective Technology Laboratory at NIOSH. His background includes nearly 30 years of experience in the field of personal protective equipment. He has considerable experience with respiratory protective equipment with a major emphasis on open- and closed-circuit self-contained breathing apparatus, supplied air respirators, and open- and closed-circuit escape breathing devices. He has been involved with the design, testing, evaluation, manufacture, and marketing of breathing-protection products and other PPE in capacities ranging from design engineer to senior vice president of an international manufacturer of breathing-protection and gas-detection equipment. He holds several respirator patents and has worked in the standards development and review process with American National Standards Institute (ANSI), International Standards Organization (ISO) and NFPA. At NPPTL Les has worked as the Program Manager for developing CBRN respirator standards. In his current position he is responsible for the research, standards development, and respirator certification activities of the laboratory. He also serves as the NIOSH Program Manager for the Personal Protective Technology Cross Sector Program. Les currently participates on the IAB FACC, on the NFPA Technical Correlating Committee (TCC), and the NFPA 1981 Committee for Open-Circuit Self-Contained Breathing Apparatus for Fire and Emergency Service. Other standards work includes participation in the ISO Respirator Committee.

Mission

The mission of the SCC is to coordinate IAB equipment standards projects with those of outside organizations and enforcing authorities and with the first responder community. The objective is to promote local, state, and federal preparedness for responding to all-hazards incidents, especially those involving CBRNE issues. By focusing the nation's resources and expertise in a common effort to establish minimum performance standards to which critical equipment can be tested, certified, and evaluated, the SCC helps to provide first responders with objective guidance for making informed decisions regarding the purchase and proper use of that equipment. As a result, both first responders and the citizens they serve can have greater confidence in the technologies that their lives depend on.

Membership

The SCC includes representatives from federal and private standards development organizations, as well as the co-chairs of the IAB SubGroups and Committees. NIST/OLES serves as the SCC's executive agent and is charged with administering, maintaining, and promulgating the CBRNE equipment standards identified for development or adopted by the IAB.

Roles and Functions

The SCC supports and coordinates the SubGroups' efforts to identify and meet standards requirements within the first responder community. Specifically, the SubGroups identify existing standards that must be modified and areas in which new standards must be developed, and the SCC assists with:

- Identifying gaps in the existing body of standards
- Prioritizing standards projects based on first responder needs
- Determining minimum performance, reliability, and quality requirements for needed standards

Standards Coordination Committee (SCC)

CO-CHAIR

Glenn Jirka
Miami Township (OH) Division of Fire and EMS

FEDERAL CO-CHAIR

Kathleen Higgins
National Institute of Standards and Technology, Office of Law Enforcement Standards

Membership

Barbara Biehn
Department of Homeland Security, Office of Grants and Training

Roberta Breden
Department of Homeland Security, Office of Grants and Training

Les Boord
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

Vinny Doherty
Long Island University/Naval Postgraduate School

Stephen Graham
United States Army Center for Health Promotion and Preventive Medicine

William Haskell
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

- Incorporating appropriate minimum performance requirements into existing standards developed by regulatory, consensus, and voluntary standards organizations
- Facilitating development of new standards by regulatory, consensus, and voluntary standards organizations
- Promoting the adoption of IAB-recognized standards

The SCC also tracks and reviews the progress of standards projects and serves as a feedback loop to the SubGroups by:

- Alerting SubGroups when contradictory requirements are proposed and facilitating reconciliation of those requirements
- Notifying SubGroups when proposed requirements contradict federal or state regulations
- Identifying existing standards, performance requirements, and test methods that could streamline development of standards for equipment listed in the SEL
- Alerting SubGroups to similar or complementary development efforts under way within regulatory, consensus, and voluntary standards organizations
- Providing advice for improving performance requirements

Partnerships

The success of the IAB's standards efforts relies on its partnerships with regulatory agencies and standards-development organizations. The SCC serves as the IAB's liaison to these partners in matters relating to equipment performance requirements, test methods, certification requirements, selection, use, and care and has initiated interagency agreements, memoranda of understanding, and informal working relationships with many federal, nonprofit, and private standards agencies, including the following:

- ANSI
- ASTM International

Robert Ingram
Fire Department, City of New York (NY)

Christopher Lombard
Seattle (WA) Fire Department

Gabriel Ramos
Technical Support Working Group

James Schwartz
Arlington County (VA) Fire Department

Stephen Skowronski
Centers for Disease Control and Prevention

William Snelson
United States Marshals Service

Elaine Stewart-Craig
Research, Development, and Engineering Command, Edgewood Chemical and Biological Center

Debra Stoe
National Institute of Justice

Thomas Walsh
Seattle (WA) Fire Department

Douglas Wolfe
Sarasota County (FL) Fire Department

Alan "A.D." Vickery
Seattle (WA) Fire Department

Subject Matter Experts

Robert Johns
Domestic Nuclear Detection Office

Don Hewitt
Responder Knowledge Base

- DHS
- DoD
- U.S. Department of Energy
- ECBC
- U.S. Environmental Protection Agency
- NFPA
- National Institute of Justice (NIJ)
- NIOSH NPPTL
- NIST/OLES
- OSHA

IAB Adopted and Referenced Standards

The SCC establishes and maintains an updated standards list that identifies standards for CBRNE and all-hazard response equipment. The list appears at the end of the SEL and contains standards officially adopted by the IAB and additional standards that SEL users will find valuable for reference.

Accomplishments

During the past year, the IAB has successfully influenced the development or revision of several CBRN and all-hazards related standards, specifically the following:

- NIOSH: *CBRN Powered Air-Purifying Respirator Standard*
- NFPA 1994: *Standard on Protective Ensembles for First Responders to CBRN Terrorism Incident*
- NFPA 1981: *Standard on Open-Circuit Self-Contained Breathing Apparatus for Fire and Emergency Services*
- NFPA 1971: *Standard on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting*

The SCC served as IAB's liaison on the joint AOAC/ANSI/ASTM working group responsible for the development of the document entitled *Standard Practices for Bulk Sample Collection and Swab Sample Collection of Visible Powders Suspected of Being Biological Agents from Nonporous Surfaces*. It also represents the IAB on the newly formed AOAC/NIST working group on handheld assays for specific biological agents.

Additionally, through the SCC IAB has continued to promote the DHS G&T program that requires that grants for the purchase of CBRNE equipment be spent on equipment that meets DHS-established or adopted performance standards.

Current Initiatives

The following are among the equipment performance standards activities to which the SCC is currently contributing:

- Revision of NFPA 1999, Standard on Protective Clothing for Emergency Medical Operations

- Development of the ANSI American Industrial Hygiene Association Respirator Use for Emergency Response and Operations Against Terrorism and Weapons of Mass Destruction
- NIOSH, ECBC, and NIST development of standards and test procedures for all classes of CBRN respirators, including work currently under way on CBRN combination self-contained breathing apparatuses (SCBAs), CBRN supplied-air respirators, and closed-circuit SCBAs
- Harmonization of older OSHA chemical-protective clothing standards with existing personal protective clothing and equipment consensus standards
- TSWG efforts to develop percutaneous toxicity data for airborne challenge agents

Summary

The importance of standards in preparing for and responding to all-hazard and CBRNE threats cannot be overstated. The IAB is in the vanguard of America's effort to rapidly develop critical equipment standards, and by coordinating the activities of the IAB SubGroups and harmonizing the efforts of agencies and organizations throughout the public and private sectors, the SCC continues to make valuable contributions to the safety of first responders and the security of the United States.

SCC Chairs

Glenn P. Jirka

Deputy Chief of Operations
Miami Township (OH) Division of Fire and EMS

Chief Jirka began his career as a firefighter with the Savoy [IL] Fire Department while working on his postgraduate studies in analytical chemistry at the University of Illinois. During his career, Jirka served as a Field Instructor for the University of Illinois Fire Service Institute and a Program Manager for the University of Missouri Fire Service Institute, held an appointment as Adjunct Assistant Professor of Nuclear Engineering at the University of Missouri, and served as a member of Search and Rescue Team Missouri Task Force One Urban, including a deployment to the World Trade Center disaster on September 11, 2001. Chief Jirka is the author of several journal articles and book chapters; a member of the Advance Rescue Technology Editorial Board; and a member of several professional organizations, including the NFPA Hazardous Materials Protective Clothing and Equipment Technical Committee (Chair), NFPA Fire and Emergency Services Protective Clothing and Equipment Technical Correlating Committee, International Association of Fire Chiefs, Ohio Fire Chiefs Association, International Fire Service Training Association Hazardous Materials Committee, and the Ohio Department of Homeland Security Hazardous Materials Technical Advisory Committee. Jirka was recently recognized by the Greater Montgomery County Fire Chiefs as the 2005 Fire Fighter of the Year.

Kathleen M. Higgins

Director, Office of Law Enforcement Standards
National Institute of Standards and Technology
Assistant to the Director for Homeland Security

Kathleen Higgins began her career as a forensic chemist, serving in the public sector, cofounding a private forensic laboratory, and working in forensic science education. After managing materials development programs for the U.S. Postal Service Engineering and Development Center for several years, she was appointed Director of the Office of Law Enforcement Standards at NIST. Under her leadership, the office has grown from a handful of programs with a budget of $1 million to more than 50 active projects with a budget near $60 million. In 2001 the Department of Commerce awarded Ms. Higgins its Silver Medal for Outstanding Achievement, and George Washington University honored her in 2002 for extraordinary service to the federal government and the nation. In November 2003, she was appointed Assistant to the Director for Homeland Security at NIST. Ms. Higgins is the author of several forensic science journal articles; a Fellow of the American Academy of Forensic Sciences; and a member of several professional organizations, including the ASTM E54 Committee on Homeland Security Applications (Chair), the International Association for Identification, the National Fire Protection Association, the International Association of Bomb Technicians and Investigators, and the International Association of Chiefs of Police (Homeland Security Committee). Ms. Higgins was recently appointed Chair of the U.S. delegation to the International Organization for Standardization's Strategic Advisory Group on Security.

"Out of Many, One"
IAB
THE INTERAGENCY BOARD
Local, State, and Federal Standardization and Interoperability

Mission

The S&T Committee's mission is to identify interagency (local, state, and federal) first-responder research and development requirements and innovative technologies (fieldable in the next six months to five years) that address CBRNE detection, individual protection, collective protection, medical support, decontamination, communications systems, information technology, and miscellaneous operational support.

Role and Functions

The primary functions of the S&T Committee are to develop and update the IAB S&T Requirements Matrix for inclusion in the SEL, coordinate IAB representation on federal requirements boards, record and collate requirements of individual SubGroups, report to SubGroups on federal requirement initiatives, and assess innovative government- and industry-developed technologies. The IAB S&T Requirements Matrix (following this section) identifies future technology needs for detection, individual protection, collective protection, medical support, decontamination, communications systems, information technology, and operational equipment.

Initiatives and Progress

During 2007, the S&T Committee accomplished the following:

- Designated SubGroup Chairs as mission area leaders responsible for detailed review and prioritization of S&T needs and projects.
- Designed and piloted a new Web-based, requirements survey to prioritize R&D requirements from SubGroups.
- Reviewed the draft 2006 SEL to ensure future needs were included in the S&T Requirements Matrix.

Science & Technology (S&T) Committee

CO-CHAIR

Vincent J Doherty
Long Island University/Naval Postgraduate School

FEDERAL CO-CHAIR

Gabriel Ramos
Technical Support Working Group

Membership

Lance Brooks
Department of Homeland Security, Science and Technology Directorate

Brett Burdick
Virginia Department of Emergency Management

Gerard Fontana
Boston (MA) Fire Department

James Neilson
Austin (TX) Police Department

Sam Pitts
United States Marine Corps Chemical Biological Incident Response Force

Neal Pollard
Georgetown University Walsh School of Foreign Service

- Reconciled the S&T Requirements Matrix with previous federal interagency research and development requirements efforts.
- Updated the S&T Requirements Matrix for publication in the Annual Report.
- Prioritized SubGroup requirements for industrial and federal partners.
- Coordinated input into federal requirements meetings to leverage IAB-prioritized requirements submissions.

Ongoing Initiatives in 2007

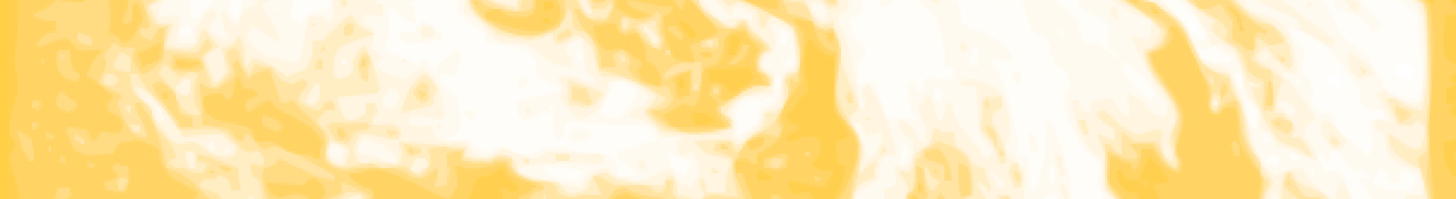
The S&T Committee will complete work on and update content in an "innovative technologies" reference database that provides information on types of emerging technical advances, status of development, industry or government source, and possible need for new standards development because of the emerging technology. The guide will cover the eight focus areas within S&T and will receive input from designated SubGroup Chairs. This information will be published in an electronic "matrix" that will link with requirements as well as existing technologies, allowing the information to be cross-referenced. The S&T Matrix has begun to be integrated as a content area of the Responder Knowledge Base.

The S&T Committee will continue to fine-tune a Web-based survey instrument to collect the R&D priorities of the membership along SubGroup categories and publish the top five R&D priorities from the Board.

Identified Requirements

The following requirements were identified by the SubGroups as priority items that should receive special consideration by R&D initiatives.*

- Three-dimensional emergency responder tracking technologies



Thomas Richardson
Seattle (WA) Fire Department

Ron Shaffer
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory

Debra Stoe
National Institute of Justice

Subject Matter Experts

Susan Ballou
National Institute of Standards and Technology, Office of Law Enforcement Standards

Jay Hagen
Seattle (WA) Fire Department/Department of Homeland Security, Office of Grants and Training, Senior Fellow/Practitioner

Nancy Suski
Lawrence Livermore National Laboratory

Vanessa Castellanos
National Institute of Justice

- Vehicle and aircraft conversion technologies to transport ambulatory and nonambulatory people during major incidents where evacuation is necessary
- Mass decontamination systems that have the ability to be operational in a very short time period and are completely mobile
- Improved rapid ambulance decontamination technology
- Computer-aided dispatching (CAD)-to-CAD interface to further interoperability and compatibility issues
- Communications system for underground transportation and emergency operations
- Improved air-purifying respirators for incident overhaul and recovery operations
- Improved explosive detection technology, both point and stand-off detectors and identifiers
- Dermal exposure standards for toxic industrial chemicals (TICs)
- Digital hands-free speaker technology to improve SCBA microphone/facepiece
- Modeling/simulation standards
- Technology to field a device for stand-off triage on victims in contaminated areas by personnel in noncontaminated areas
- Pseudo satellite to enhance incident communications when other communication links have failed
- Standards for how clean is clean after decontamination operations
- Combined detector with multiple methodologies for chemical warfare agent/TIC detection

*Note—These requirements have been identified by the SubGroups of the IAB and are not prioritized at this point.

The Science and Technology Committee submits the following short technology success briefs to highlight small advances in methodolgy and technology that may result in requirement solutions in the future.

A BREATHABLE, CHEMICAL-BLOCKING COMPOSITE MATERIAL FOR CHEMICAL PROTECTIVE ENSEMBLES

Butyl rubber has been used by scientists, industrial workers and emergency responders as part of their chemical-protective ensembles for decades. The material is effective and efficient but has many drawbacks, such as bulk, weight and nonbreathability.

According to *Science News*[1], scientists have developed a process to combine a lyotropic liquid crystal which has two different ends—one end water-repelling and the other water-loving—with liquid butyl rubber. The resulting material yielded a flexible material consisting of a three-dimensional network of rubber and nanometer-scale pores that contain water. Chemical warfare agents which are generally water-repelling cannot pass through the pores. In early testing, researchers used a mustard gas–like chemical on a patch of composite material. Permeation of the chemical through the composite was longer as compared to butyl rubber but also allowed enough water vapor to pass through the composite to meet the military standards for comfort.

[1] “For Sweat’s Sake,” *Science News*, Vol. 171, No. 1 (Jan. 6, 2007), p. 13.

BIO DETECTOR TECHNOLOGY MAY TAKE A LEAP FORWARD USING A TINY SILICONE DEVICE TO DECREASE THE TIME TO DUPLICATE DNA.

State-of-the-art biological detectors and identification methodologies isolate and replicate microbial DNA to amplify a sample through cycles of hot and cold temperatures that may take several hours. As reported in Newsweek, a small biotech company from upstate New York, Thermal Gradient, has developed a device that uses microscopic preheated and cooled silicon layers that reduce the amplification time from hours to four minutes.[2]

The Department of Homeland Security has awarded an initial $500,000 contract to Thermal Gradient to develop an instant biological airborne-detection system for deployment in places of public assembly and transportation hubs. The company is also looking to develop a deployable unit for the U.S. Army in battlefield conditions.

[2] “A Faster DNA Test,” *Newsweek* (Jan. 15, 2007), p. 15.

Summary of Current Research & Development by SEL Category

Project	Description	Managing Agency / Participant(s)	Availability
SEL Category 01 - Personnel Protective Equipment			
Land Warrior project	Integrated protection, detection, and communications ensemble for soldiers.	www.natick.army.mil	FY07 and beyond
Development of Computer-aided Face Fit Evaluation Methods	Establish updated database of facial characteristics that can be used by respirator manufacturers to develop better products, and by NIOSH for certification.	NIOSH/NPPTL	FY07
Next generation of turn-out gear for fire service	Protective Fire Fighter ensemble that provides integrated chem/bio protection.	www.tswg.gov	FY07
Drink System for Powered Air Purifying Respirator (PAPR) and Self Contained Breathing Apparatus (SCBA)	Provides hydration capabilities while wearing a facepiece.	www.tswg.gov	Technical Design Available upon request from vendor.
Physiological models and countermeasures for PPE	Develop better methods for assessing the physiological effects of wearing protective clothing ensemble and cooling garments.	NIOSH/NPPTL	FY08
CB/Smoke Escape Hood	Provides 15 minute escape capabilities from smoke and chem/bio incidents.	www.tswg.gov	FY07
CB Escape Hoods	Provides 15 minute escape capabilities from chem/bio incident.	www.tswg.gov MSA Response Hood ILC Dover Scape Hood Survivair Quick Pro	Available
Body Armor Cooling System	Lightweight, low-cost, cooling capability designed to be worn under body armor.	www.tswg.gov www.technicalproductsinc.us	Available
Long Duration Tactical SCBA	A lightweight, low-cost, low-profile, long-duration closed-circuit SCBA (rebreather) for law enforcement tactical operations.	www.technicalproductsinc.us www.tswg.gov	FY07
Hazmat/USAR ensemble	NFPA 1994 Class II rated ensemble. Form fitting, composed of durable materials that withstand urban search and rescue operations.	www.tswg.gov Inter-Spiro Aerostar Gore	Available
End of Service Life Indicator for Respirator Cartridges	System to indicate remaining service life of chemical filter cartridges.	NIOSH/NPPTL/DoD	Ongoing development
SEL Category 02 - Explosive Device Mitigation and Remediation			
Next Generation Bomb Suit	Improved bomb suit with integrated chemical protection.	www.tswg.gov	FY07
Vehicle-Borne IED Detection	Remote detection enhancement, x-ray based screening system for vehicles.	www.tswg.gov Quantum Magnetics	FY07
Suicide Bomber Detection	System using terahertz, millimeter wave, or non-imaging detection.	www.tswg.gov Qinetiq	FY07
Next Generation Handheld Explosives Detector	Improved handheld explosive detector for residue, imaging and personnel screening.	www.tswg.gov	FY07
Improved Canine Bomb Detection Performance	Improved screening and training techniques for optimal canine and handler bomb detection performance.	www.tswg.gov	FY07
Joint Robotics Program	Improved IED response robotics.	www.tswg.gov	FY07

Summary of Current Research & Development by SEL Category - *Continued*

Project	Description	Managing Agency / Participant(s)	Availability
SEL Category 03 - CBRNE Operations & Search & Rescue Equipment			
Modular Portable Air Filtration Unit	CBR positive pressure air filtration system for small rooms.	www.tswg.gov www.germfree.com	Available
3-D Personnel Locator	Device to locate personnel in three dimensions Ongoing development	www.tswg.gov DHS	
SEL Category 04 - Information Technology			
Sensor Web	A wireless telemetry based sensor communications system.	www.tswg.gov JPL	Available
SEL Category 04 - Information Technology (Software)			
Hand Held Hazard Assessment Tools	Software tools compatible with hand held PDAs or laptops that rapidly assess chemical spill hazards.	www.tswg.gov www.aristatek.com Georgia Tech	Available
SEL Category 05 - Cyber Security Enhancement Equipment			
Passive Network Mapping Tool	Rapidly assess cyber network performance	www.tswg.gov	Ongoing development
Detection of novel attacks against network servers	Intrusion detection of network servers against viruses and cyber attacks	www.tswg.gov	Ongoing development
SEL Category 06 - Interoperable Communications Equipment			
Small, Portable Voice Radio Repeater System	Hockey puck sized radio repeater system to maintain voice communications in collapsed buildings and tunnels	www.tswg.gov	FY08
SEL Category 07 - Detection			
Biological Aerosol Threat Warning Detector	Hand held, low cost UV LED detector providing real-time detection and warning (alarm) of hazardous biological aerosols.	www.tswg.gov GE Global Research	Ongoing development
Biological Aerosol Mass Spec (BAMS)	Real-time detection, identification, and warning of hazardous biological agents in complex interferent backgrounds	www.tswg.gov LLNL	Ongoing development
Self Indicating Radiation Dosimeter	A beta/gamma self-reading radiation dosimeter badge measuring cumulative dose for rapid assessment of radiation exposure so responders can quickly assign triage levels.	www.tswg.gov JP Labs	Available
Active LWIR (Long Wave Infra Red) plume tracking system for Facility Monitoring	Spectral imaging of a Toxic Industrial Chemicals (TIC) release in a large confined space.	www.tswg.gov	Prototype available
Facility Alarm System for Airborne Biological Toxins	A highly specific detection system using novel Field Asymmetric Ion Mobility Spectrometry (FAIMS) technology to monitor indoor facilities and HVAC systems for the presence of biological toxins.	www.tswg.gov www.draper.com	FY06
Non-PCR Detection of Bio Agents	A gold nanoparticle and antibody-based field portable assay for rapid detection and identification of biological agents, which is much simpler to use and operate than conventional PCR methods.	www.tswg.gov www.nanosphere-inc.com	FY06
SmallCAD	Portable handheld detector that combines SAW and IMS detection technologies for improved sensitivity and low false alarm detection of TICs and CWAs	www.tswg.gov www.saic.com	Available
Detection of Toxic Adulterants in Food	A compact and simple to use test kit that rapidly and accurately detects poisons in food though the use of color change chemistry.	www.tswg.gov Appealing Products Inc.	Available

Summary of Current Research & Development by SEL Category - *Continued*

Project	Description	Managing Agency / Participant(s)	Availability
SEL Category 07 - Detection - *Continued*			
Real-Time Radioisotope Detection and Reporting	Hand-held device that rapidly detects radioisotopes and wireless capability to transmit gamma spectral data to DOE Triage Systems for confirmation of radiological spectral data.	www.tswg.gov www.saic.com	Prototype available
Toxic Industrial Chemical Monitor for Facility HVAC systems	An alarm system that detects and monitors for presence of TICs & WMD agents in HVAC systems using two complementary detection technologies with a low rate of false alarms	www.tswg.gov Avir	Available
Distributed Chemical Sensing and Transmission	A fiber optics based distributed sensing system that rapidly detects, identifies and alarms the presence of TICs and CWAs at below IDLH levels.	www.tswg.gov IOS	Prototype Field Demo in FY06/07
Alpha and Beta Contaminate Detection in Water	An automated batch analysis system to detect alpha and beta emitters in static and flowing potable water systems.	www.tswg.gov EPA SRNL	FY07
SEL Category 08 - Decontamination			
Mass Personnel Decontamination Protocols	A handbook containing consensus-based best practices and procedures for CBR mass decontamination	www.tswg.gov www.cbiac.apgea.army.mil	Available
Enzymatic Decontamination	Decontamination solution using enzymes to breakdown chemical and biological contaminants on equipment and in the environment.	www.sbccom.army.mil	Unknown
Disinfection By-products Database	Database of gas/vapor by-products resulting from the decontamination of various building materials.	www.tswg.gov www.utexas.edu	Available
Electrostatic Decontamination System	A spray-on decontamination solution for rapid (UV light activated) neutralization of chemical and biological agents.	www.tswg.gov www.cleanearthtech.com	Available
Low Cost Personnel Decontamination System	A kit to quickly remove and neutralize chemical agents from skin and mucous membranes	www.tswg.gov LLNL	FY07
Atmospheric Plasma Decontamination	Neutralize biological agents on sensitive items without damaging materials through the use of room temperature anti-microbial gases (plasma).	www.tswg.gov Atmospheric Glow Tech	Available
WMD Overpack Bag	Durable, puncture-resistant, impermeable and chemically resistant overpack bag with robust sealing mechanism to prevent the spread of contamination from a chem-bio contaminated source, operational equipment or improvised dispersion/dissemination device.	www.tswg.gov www.ilcdover.com	Available
Expedient Mitigation of a Radiological Release	Easily applied and removable adsorbent coating systems to mitigate the spread of radiological contamination.	www.tswg.gov Istron Argonne National Labs DHS (S&T)	Available
Plant and Animal Tissue Gasifier	A transportable gasification system for large scale disposal of contaminated plant material and animal carcasses.	www.tswg.gov BGP Inc. EPA USDA	FY08
Expedient Chemical/ Biological Release Mitigation	A self-contained kit providing respiratory protection, protective gloves, adsorbent materials, and overpack containment. Used to mitigate an improvised chem-bio dissemination device.	www.tswg.gov www.battelle.org	Prototypes Available

Summary of Current Research & Development by SEL Category - *Continued*

Project	Description	Managing Agency / Participant(s)	Availability
SEL Category 09 - Medical			
Bio-dosimetry Assessment Tool (BAT) Integration	Software with information resources and tools for emergency response and health care providers to help identify and manage radiation casualties.	www.tswg.gov AFRRI	Available
Ocular Scanner for Chem/Bio Agents	Portable hand-held and automated triage tool for non-invasive assessment of acute or chronic exposure to TICs, CWAs, and toxins.	www.tswg.gov MD Biotech	FY06/FY07
SEL Category 10 - Power			
Fuel Cell for Continuity of Operations	Develop and demonstrate fuel cell technology to improve the logistical sustainment of critical response operations.	www.tswg.gov	FY07/FY08
CBRNE Training Technologies			
WMD Panic Response Operations (WMD-PRO) Course	Accredited Consequence Management training course for Federal, State, and Local personnel covering the psychological impacts and effects of a Weapon of Mass Destruction (WMD) incident.	www.tswg.gov Early Responders Distance Learning Center at Saint Joseph's University	Available
Food Protection and Security Training for Critical and Overseas Facilities	Modular, CD-ROM, and web-based training program for food supply chain personnel covering food protection, supply chain traceability, risk management, communication, and International Food Security law.	www.tswg.gov www.cfsan.fda.gov	Preliminary Course materials Available
Agricultural Bioterrorism Response Training	Accredited, modular, agricultural bioterrorism response training curriculum for classroom, CD-ROM, or web-based distance learning applications.	www.tswg.gov www.aphis.usda.gov	Preliminary Course materials available mid-FY05
Low Cost Shelter-In-Place Equipment and Training for Public Buildings	Training video that outlines specific steps and procedures to prepare an effective sheltering-in-place plan and kit for public buildings/facility managers.	www.tswg.gov	Available
Explosives Simulant Kit	Training kit to educate first responders on explosive signatures and warnings.	www.tswg.gov www.cbiac.apgea.army.mil	Available
Miscellaneous			
CB Building Protection Protocols	Software that assists engineers in the design/retrofit of collective protection systems for buildings/ critical facilities.	www.tswg.gov www.utrc.utc.com US Army Corps of Engineers	Available
Nano-material and nanotechnology research and development	Application of nanotechnology materials for chemical-biological detection and protection.	www.raytheon.com	FY06

S&T Chairs

Vincent J. Doherty

Associate Professor, Homeland Security Management Institute
Long Island University/Naval Postgraduate School

Vincent Doherty, is a retired, 25-year veteran of FDNY, where he was the Executive Officer of HazMat Operations and the former Company Commander of Hazardous Materials Company 1 (HazMat 1), New York City's premier hazardous materials response unit. Captain Doherty received his B.S. from St. John's University and an M.A. in Security Studies, Homeland Security and Defense from the Naval Postgraduate School. Prior to joining the Fire Service, he was a research/quality control chemist in the Diagnostics Division for Fisher Scientific, Orangeburg, N.Y. Captain Doherty is a contract instructor for the International Association of Fire Fighters, National Fire Academy, and FDNY and is currently Chair of the Science and Technology Committee of the IAB. He was also a member of New York City's Federal Emergency Management Agency Urban Search and Rescue Task Force 1. Presently, Mr. Doherty is the Director of Program Outreach for the Center of Homeland Defense and Security, Naval Postgraduate School and an Associate Professor for the Homeland Security Management Institute, Long Island University.

Gabriel Ramos

Chemical Biological Program Manager
Technical Support Working Group

Gabriel Ramos is a program manager for TSWG, providing management and technical oversight for the execution of the CBRN countermeasures rapid R&D program. He has 20 years of experience developing and evaluating CB capabilities for DoD and the federal interagency combating terrorism community. Mr. Ramos has a B.S. in chemical engineering from the Polytechnic University, Brooklyn, N.Y. and is also a graduate of the U.S. Army School of Engineering Logistics Product/Production Engineering Program.

Mission

The CIC serves as the focal point for the coordination of interoperability and compatibility issues identified by the IAB. The CIC consolidates and prioritizes equipment, standards, training, and operational interoperability and compatibility concerns identified by the IAB SubGroups and Committees. The CIC works in coordination with the SCC and S&T Committees and SubGroups to develop interoperability and compatibility requirements and identify potential solutions.

Membership

The CIC consists of member representatives and SMEs who address domestic preparedness equipment, systems, and protection issues related to specific interoperability and compatibility issues. It includes representatives from each of the IAB SubGroups and Committees. The CIC is a very young group and is seeking to expand the membership to have members representing the IAB organizational structure and also practitioner representatives from the emergency services, standards development organizations, and DHS and other federal agencies.

Roles and Functions

The CIC complements and supports the standards development activities of the SCC and the technology development recommendations of the S&T Committee by the following:

- Coordinating and consolidating interoperability and compatibility issues identified by the SubGroups, SCC, and S&T Committees
- Identifying potential solutions in terms of standards, equipment development, training, or policy requirements to assist the responder community
- Coordinating efforts in the IAB Committees and SubGroups in identifying specific interoperability and compatibility issues
- Providing input to support SCC and S&T Committee activities

Compatibility and Interoperability Committee (CIC)

CO-CHAIR

Robert J. Ingram
Fire Department, City of New York (NY)

FEDERAL CO-CHAIR

Philip Mattson
National Institute of Standards and Technology, Office of Law Enforcement Standards

Membership

Roberta Breden
Department of Homeland Security, Office of Grants and Training

Chris Callsen
Austin-Travis County (TX) Emergency Medical Services

Timothy Fisk
Orlando (FL) Police Department

Greg Noll
South Central (PA) Counter-Terrorism Task Force

Martin Hutchings
Sacramento County (CA) Sheriff's Department

Luke Klein-Berndt
National Institute of Standards and Technology

- Drafting studies, white papers, and other reports on IAB interoperability and compatibility issues as needed
- Identifying existing programs that are addressing interoperability and compatibility issues,
- Summarizing IAB interoperability and compatibility issues, priorities, and potential solutions in the IAB Annual Report

Accomplishments

The CIC is the newest committee in the IAB, established in 2006. It enables the IAB to fully serve as the "InterAgency Board for Equipment Standardization and Interoperability." Prior to the establishment of the CIC, there was no single focal point for addressing noncommunications compatibility and interoperability issues. The major accomplishment of the CIC for 2006, other than getting established, is the initial draft of a summary report of compatibility and interoperability issues raised by the IAB SubGroups. The table listing the compatibility and interoperability issues identified by the IAB is at end of this section.

Developing working definitions for the terms "interoperable" and "compatible" was critical, especially when using these terms to address noncommunications systems. The following definitions were agreed upon:

- Compatibility—Systems that work together to accomplish a common task with no modification or conversion required and that do not interfere with other systems (e.g., all hose and hydrant couplings are the same, or everybody speaks the same language).
- Interoperability—Use of converters, adaptors, translators, etc. to enable systems to work together to accomplish a common task (e.g., use of adapters for hose couplings or the use of a translator).

Initiatives for 2007

The CIC will continue to expand and examine compatibility and interoperability issues in the next

Subject Matter Experts

Ed Bailor
United States Capitol Police (Retired)

year by the following:

- Collect and or develop working definitions for terms used by the IAB as needed
- Expand the membership of the Committee through recruiting dedicated CIC members
- Gather new compatibility and interoperability issues identified by the IAB
- Develop a methodology for prioritizing compatibility and interoperability issues
- Develop a matrix to indicate potential solutions for compatibility and interoperability issues, in terms of standards development, technology development, guidance, etc.
- Expand on selected issues with short white papers more fully explaining the background, concerns, and potential solutions for compatibility and interoperability issues

Summary

The CIC will expand its efforts and will serve as the focal point for compatibility issues for the IAB. The CIC will serve to enable the IAB to truly be the emergency response community's voice for equipment standardization and interoperability. The following table lists the compatibility and interoperability issues identified by the IAB SubGroups in 2006.

IAB Compatibility and Interoperability Issues—2006

SubGroup	Issue	Description*
D&D	Wireless communications	Lack of plug-and-play communications systems
D&D	Standard Material Safety Data Sheets (MSDS)	Lack of standard format for MSDS
D&D	Standardized CB reporting	Lack of standardized incident reporting, to delineate between suspicious and credible incidents
D&D	Environmental sampling methods	Need for standardized environmental sampling methods
D&D	Hose connections	Lack of compatibility and interoperability of hose connections
D&D	Compatible chemical detector libraries	Raman hazardous materials identification need for compatible libraries, legal issues—manufacturers' proprietary libraries
D&D	Threat assessment process	There are multiple threat assessment tools, however guidance is needed to assist in identifying the proper tool to use and how to interpret results.
D&D	Environmental sampling strategies and evidence	Conflict between environmental sampling strategies and evidence/forensic collection
D&D	How clean is clean?	Decontamination methods can not be adequately evaluated until a determination is made as to the level of cleanliness that is necessary
D&D	ASTM sampling standard	Elements in the first responder community have issues with ASTM suspicious powder sampling standard. What is bio sampling? Standard field screen method and technology.
D&D	Single detector for chemical warfare agents/Toxic Industrial Chemicals (TICs)	Responders need one device that will detect multiple agents (including both chemical warfare agents and TICs) instead of carrying two or more detectors
Medical	Medical credentialing	Standardization by skill set that translates nationwide and intrastate.
Medical	Standardization of batteries	From radios to all universal medical equipment
Medical	Uniform public health surveillance	Common data set/definitions between jurisdictions
Medical	Guidance on health/EMS/WMD equipment	Universal guidance for health disciplines for equipment purchases listed on the AEL is desirable. This needs to be coordinated between DHS and HHS.
PP&OE	Compatibility of wireless systems	All wireless systems (heads-up display on SCBA) during operations must be compatible and interoperable to eliminate interference and crosstalk
PP&OE	Compatibility of Special Weapons and Tactics (SWAT) body armor with SCBA	Current ballistic tactical vests hinder wearing the harness for SCBA
PP&OE	Dexterity issues with gloves	Inability to perform job functions while wearing cumbersome PPE gloves, i.e., weapons manipulation, bomb render-safe procedures, HAZMAT detection equipment manipulation, evidence collection, medical triage, etc.
PP&OE	Helmet and facepiece compatibility issues.	Law enforcement has difficulty acquiring proper sight alignment/sight picture and target acquisition while using weapons due to distortion from facepiece and standoff (inability to acquire proper stock/cheek weld). SCBA facepiece/bombsuit facepiece interoperability— profile of the facepiece compatible with only one manufacture's product. Limits interoperability of systems. Respirator impedes correct fit/usage of all helmets (firefighting, ballistic, Urban Search & Rescue)
PP&OE	Interoperability of wireless PASS/accountability systems	Many different units show up; Personal Alert Safety System (PASS) and/or accountability system must pick up all groups during operation; current PASS systems are not designed to be interoperable because there is no standard for their development.
PP&OE	Underwater/open-water communications (wireless) limitations	Limited communication with base station unless hard-wired; need wired equivalent wireless devices. Hardwire limits operations.

IAB Compatibility and Interoperability Issues—2006 - *Continued*

SubGroup	Issue	Description*
PP&OE	Rehydration issues	Lack of rehydration capability in PPE, in particular respiratory protection. The technology and standards do exist but not widely in use. Limits duration responders can safely operate without danger of dehydration.
PP&OE	Fire hydrant couplings	There are different standards for fire hydrant couplings. The use of differing couplings can complicate multiagency response. There are issues with fire hydrant security.
PP&OE	Film for bomb squad portable X-ray systems	The one remaining manufacturer of film used by the bomb squad portable X-ray systems is discontinuing production. This loss will require bomb squads to procure new systems.
PP&OE	SCBA compatibility	The air cylinders used in SCBA are not interchangeable from one manufacturer to another. The need for interchangeable air cylinders has been raised in a number of forums.
Training	NFPA 472/OSHA 1910.120	NFPA 472/OSHA 1910.120–crosswalk NFPA 470 series, HAZWOPER and other federal related standards, provide layman's interpretation and equipment implications to drive consistency of the application of standards
Training	NIMS resource typing definitions	Revisit initial 120 NIMS resource typing definitions (example: SWAT—fit in with HAZMAT EOD definition.) Conduct NFPA 1670/1006/470 series cross-walk. Highlight impact of typing changes on PPE, equipment, and professional qualifications.
Training	Safety considerations	Define roles, responsibilities, and professional competencies of an all-hazards safety officer.
Training	Information sharing	Information-sharing among various working groups. Establish a feedback loop (e.g., from NIMS resource typing working group back to IAB).
Training	Common terminology	Common terminology for training and exercises.
Training	Blending of responder roles.	Blending of SWAT/HAZMAT/EOD/EMS roles and missions has implications of PPE selection and use and training.
Training	Competency mapping	Competency mapping for tasks to training hours required. For example, LE equipment training matched to performance beyond awareness training.
Training	Modeling/ simulations standard	Modeling/simulations standard for state and local responder applications. There needs to be open standards developed for modeling/simulation training tools to allow for compatibility between systems. The first step should be a review of the current status of modeling/simulations. SCORM compliance; open-architecture models; JXML language.
Training	Incident management training and qualification systems	There is a need to establish a training and qualification system that provides an urban focus on incident management. Urban responders need training and qualification in upper-level incident management positions, but existing training and qualification is primarily provided by National Wildfire Coordinating Group (NWCG) and other wildland training and qualification organizations. Currently, it is difficult for urban responders to obtain access to training and get signed off and qualified for positions because of wildland focus.
Training	Simulation evaluation criteria	Currently, industry approaches emergency responders and government decision makers with the 'next greatest solution." However, no resource provides all decision makers with minimum evaluation criteria.
ICIS	Simulation efforts are diverse, with no common architecture	Data inputs and outputs differ, not compatible with different platforms, training burden, etc.
CIC	Urban search and rescue robot communications and sensor interoperability and compatibility	Communication between operator and robot and/or telemetry from sensors is difficult at incident site, complicated by large number of other communications systems in use interfering with each other and with robots.
CIC	Multiple Responder Coordination to a Bomb Squad Issue	Formation of categories and strategies for first responders, other than bomb squad, to a bomb squad call out need to be developed.
CIC	Explosive Detection K-9 Basic Odor Test	There is a lack of a national basic odor recognition standard for non-Federal explosive detection K-9s. A standard needs to be developed with associated certification program for explosive detection K-9s.

CIC Chairs

Philip J. Mattson

Program Manager, Critical Incident Technologies
Office of Law Enforcement Standards
National Institute of Standards and Technology

In addition to serving as the Program Manager for Critical Incident Technologies at NIST/OLES, Philip Mattson serves on detail to the DHS Standards Office at the Science and Technology Directorate. Mr. Mattson manages programs with multiagency funding to facilitate the development of a national suite of standards for CBRNE protective and operational equipment for the emergency response community. He is the Federal Co-Chair of the IAB CIC and a member of the ASTM E54 Committee on Homeland Security Applications, chairs the E54.08 Operational Equipment Subcommittee, and is a member of the ANSI Homeland Security Standards Panel and the NIJ Personal Protective Equipment Technology Working Group. At DHS Mr. Mattson serves as the Program Manager for Standards Identification and Development in the Office of Standards, and directly manages a portfolio of projects which includes the DHS-funded protective equipment standards development efforts. A registered Professional Engineer, he received a B.S. in nuclear engineering technology from Oregon State University, an M.S. in physics from the Naval Postgraduate School, and extensive training in nuclear weapons and radiological incident management. Mr. Mattson served 20 years as an officer with the U.S. Army Corps of Engineers and as a nuclear physicist with the Defense Nuclear Agency and Defense Special Weapons Agency.

Robert J. Ingram

Chief in Charge, HazMat Operations,
Fire Department, City of New York

Robert Ingram is a 32-year member of the Fire Service, starting his 26th year with FDNY, assigned as the Chief in Charge of the Hazardous Materials Operations Division. He has 20 years of experience in hazardous materials response and has worked on WMD issues since 1997. Chief Ingram's experience includes training, FEMA urban search and rescue, field operations, interagency exercises, and standards development. He has been a member of the IAB since 1999.

Mission

To address the issues of personal protective and operational equipment standardization and interoperability and make recommendations for PPE and operational equipment based on threat assessment, operational requirements, and job functions.

Role and Functions

The PP&OE SubGroup addresses the personal protection and operational equipment needs of responders to potential CBRNE events. The SubGroup recommends personal protective ensembles based on both the hazard to be encountered (hazard type and, where applicable, physical state) as well as the job function likely to be performed. As the ensembles and accessories or ancillary items necessary to meet this "hazard/risk" assessment are identified, the SubGroup will look to identify where performance standards either exist or are lacking. The PP&OE SubGroup supports the development of personal protective, explosive device mitigation, operational, and search and rescue equipment performance criteria and standards. In addition to these areas, the PP&OE SubGroup has added extensive support for surface/subsurface water and tactical law enforcement operations for the 2007 edition of the SEL.

The PP&OE SubGroup is comprised of members and subject matter experts (SMEs) from a wide array of emergency response organizations of varying size, as well as federal partners, and standards organizations. The synergistic effect of this membership creates the ability to push forward initiatives that will provide systemwide improvements and standards development. The composition of the PP&OE SubGroup includes:

- Response Organizations—Fire service, law enforcement, emergency medical service, medical first receivers, hazardous device operations, hazardous materials, search and rescue and water operations.
- Standards Organizations—NFPA and ASTM International
- Federal Partners—Representing NIOSH; Department of Veterans Affairs; U.S. Coast Guard; DoD including the Center for Health Promotion and Preventive Medicine; and the DHS National Fire Academy

Personal Protective & Operational Equipment (PP&OE) SubGroup

CO-CHAIR

Douglas E. Wolfe
Sarasota County (FL) Fire Department

FEDERAL CO-CHAIR

William Haskell
National Institute for Occupational Safety and Health
National Personal Protective Technology Laboratory

Membership

Armondo Bevelacqua
Orlando (FL) Fire Department

Richard Duffy
International Association of Fire Fighters

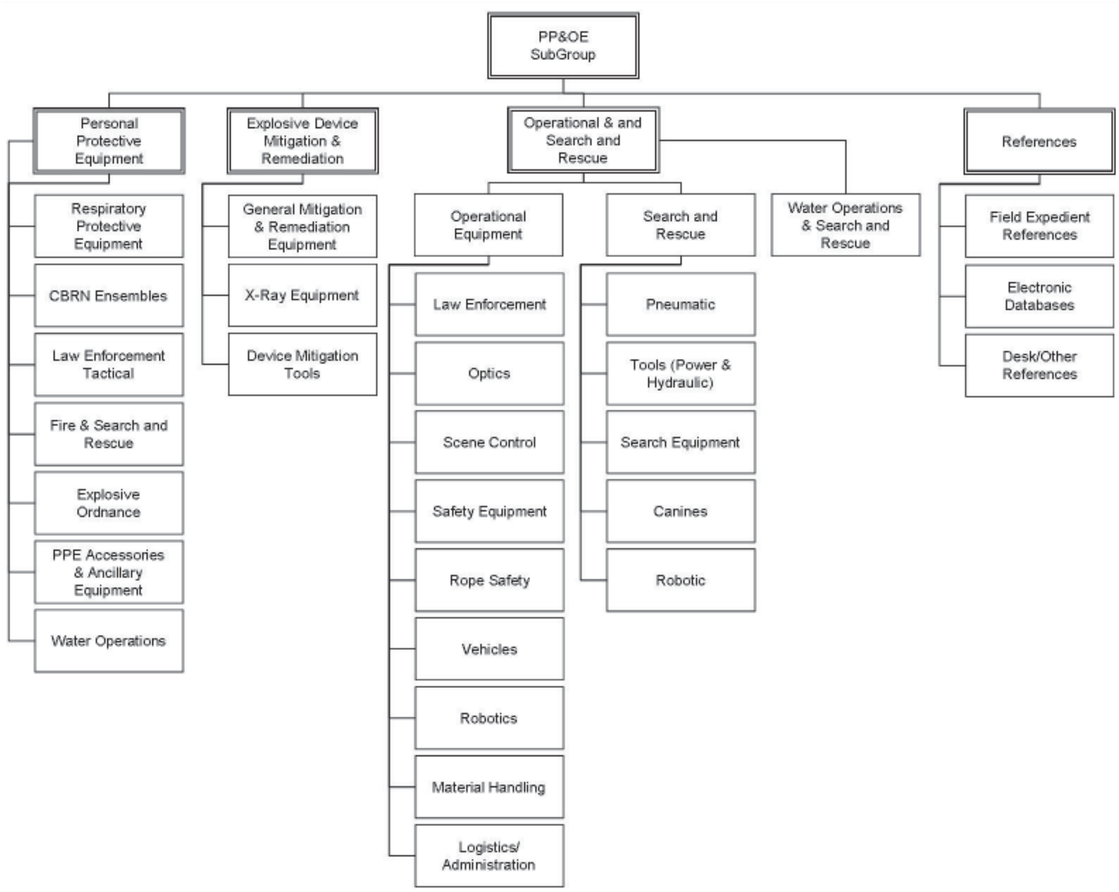
Lt. John Hahn
United States Coast Guard National Strike Force

John Hancock
Department of Veterans Affairs

Martin Hutchings
Sacramento County (CA) Sheriff's Department

Eric Imhof
Contra Costa County (CA) Office of the Sherriff

Joel Leson
International Association of Chiefs of Police



Jeff Marcus
Los Angeles (CA) Fire Department

David McBath
New York State Police

Rick Reddy
Boise (ID) Fire Department

Irene Richardson
United States Army Center for Health Promotion and Preventive Medicine

Axel Rodriguez
United States Army Natick Soldier RDEC

Mark Saxelby
California Urban Search and Rescue Task Force 1

Bruce Teele
National Fire Protection Association

Ron Watson
Los Angeles County (CA) Fire Department

Wayne Yoder
Department of Homeland Security, Federal Emergency Management Agency, National Fire Academy

Subject Matter Experts

Jeffrey Stull
International Personnel Protection

Tim Dorsey
Creve Coeur (MO) Fire Protection District/ FEMA Task Force 1 Urban Search and Rescue

Eric Ashburn
Walker County (GA) Emergency Services

Chris Hays
National Tactical Officers Association

- Professional Organizations—International Association of Fire Fighters (IAFF), International Association of Chiefs of Police (IACP), National Tactical Officers Associations (NTOA), and the National Bomb Squad Commander's Advisory Board (NBSCAB)

This membership serves to enhance partnerships between local, state, federal, military, and professional organizations and the standards development community. Through these partnerships, protective clothing, equipment, expertise, technologies, and standards are being developed. Ongoing federal and military research and development programs are being leveraged and, in some cases, fast-tracked for the benefit of the emergency response and public safety community. Bringing all the stakeholders to the table in a cooperative manner has been, and will continue to be, essential to the success of this SubGroup.

Initiatives and Progress

During its 2006 meeting cycle, the PP&OE SubGroup identified its major strategic initiatives:

- Made significant revisions to the PPE and Operational Equipment Sections of the Standard Equipment List working closely with the Responder Knowledge Base RKB) staff.
- Inclusion of personal protective and operational equipment needed for operations in surface/subsurface water environments and support of NFPA standards development for this mission.
- Inclusion of personal protective and operational equipment for tactical law enforcement mission.
- Expanding the membership to ensure adequate representation of the tactical law enforcement mission.
- Advocate the development of performance criteria and development of standards for law enforcement PPE for protection against CBRN hazards.
- Advocate the development of data to provide guidance relating to effects of dermal exposure values necessary to aid in the proper design and selection of CBRN protective ensembles
- Support improvements in existing test methods for measuring chemical resistance of materials against chemical warfare agents (CWAs) and toxic industrial chemicals (TICs).

Standards That Have Been Developed or Revised

The PP&OE SubGroup closely monitors the development of various standards. Many of the PP&OE SubGroup members served dual roles of various standards development committees. Significant changes in standards that occurred during the last business cycle that are endorsed by the SubGroup include the following:

National Fire Protection Association Standards

- NFPA 1951, Standard on Protective Ensembles for Technical Rescue Operations, 2007 Edition
- NFPA 1971, Standard on Protective Ensemble for Structural Fire Fighting and Proximity Firefighting, 2007 Edition
- NFPA 1981, Standard on Open-Circuit Self-Contained Breathing Apparatus (SCBA) for Emergency Services, 2007 Edition
- NFPA 1982, Standard on Personal Alert Safety Systems (PASS), 2007 Edition
- NFPA 1983, Standard for Life Safety Rope and Equipment for Emergency Services, 2006 Edition
- NFPA 1994, Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents, 2007 Edition

- NFPA 2112, Standard on Flame Resistant Garments for Protection of Industrial Personnel Against Flash Fire, 2007 Edition
- NFPA 2113, Standard on Selection, Care, Use and Maintenance of Flame-Resistant Garments for Protection of Industrial Personnel Against Flash Fire, 2007 Edition

National Institute for Occupational Safety and Health Standards

NIOSH Statement of Standard for CBRN Powered Air-Purifying Respirators, October 2006

PASS performance issues addressed in new edition of NFPA standard

The 2007 Edition of NFPA 1982, Standard on Personal Alert Safety Systems (PASS) is now available

Background

Access to NFPA 1982 In late 2005, NFPA published an alert notice entitled “PASS alarm signals can fail at high temperatures “ on the NFPA website advising emergency responders, especially fire fighters, of high temperature exposures causing the loudness of PASS alarm signals to be reduced. This reduction in loudness can cause the alarm signal to become indistinguishable from background noise at the incident scene. This problem was brought to the attention of the NFPA Technical Committee on Electronic Safety Equipment by the National Institute for Occupational Safety and Health’s (NIOSH) Fire Fighter Fatality Investigation and Prevention Program.

NIOSH reported that during the investigation of four fire fighter fatalities that occurred from 2001 to 2004, the PASS alarm signals were not heard or were barely audible. The PASS had been certified as compliant to NFPA 1982, Standard on Personal Alert Safety Systems (PASS), 1998 Edition, and involved both stand-alone PASS and SCBA-integrated PASS.

Laboratory testing of PASS by the National Institute for Standards and Technology’s (NIST) Fire Research Division has shown that this sound reduction begins to occur at temperatures as low as 300° F (150° C) and affected all PASS evaluated by NIST that were certified to the 1998 edition and earlier editions of NFPA 1982.

The new, 2007 edition of NFPA 1982

The alert notice reported that the NFPA Technical Committee on Electronic Safety Equipment (the Technical Committee), in cooperation with NIOSH and NIST, was studying the issue and would incorporate revisions into NFPA 1982 as solutions were developed and consensus around addressing the issue was achieved. The Technical Committee has now completed the new, 2007 edition of NFPA 1982, which contains revisions providing for strengthened performance requirements and testing addressing the alarm signal degradation issue identified in the alert notice. The new edition also addresses other issues that have been brought to the attention of the Technical Committee by NIOSH and others, including problems caused by vibration, probably during transportation, and water ingress into the electronic and power supply compartments. The principal changes contained in the 2007 edition of NFPA 1982 are summarized as follows:

1. New water immersion requirements and testing for PASS where PASS is exposed to 350° F for 15 minutes and then to water submersion in 1.5 meters (4.9 ft) also for 15 minutes for each of 6 cycles; and PASS examined to determine no water ingress, all PASS signals must function properly, and electronic data logging functions must operate properly; following this, PASS is re-immersed in the test water for additional 5 minutes with the power source compartment(s) open, and following the 5 minutes the PASS is removed from water and wiped dry, then the electronics compartment is opened and examined to determine no water ingress;

2. New high temperature functionality requirements and testing to now have PASS mounted in a circulating hot air oven at 500° F for 5 minutes and the PASS alarm signal must function at or above the required 95 dBA sound level, electronic data logging functions must operate properly, and no part of the PASS can show evidence of melting, dripping, or igniting;
3. New tumble-vibration requirements and testing for PASS where PASS is "tumbled" in a rotating drum for 3 hours and the PASS alarm signal must function at the required 95 dBA sound level and electronic data logging functions must operate properly;
4. New "muffling" of the alarm signal requirements and testing for PASS where PASS is mounted on a test subject and evaluated in five positions (face down w/arms extended, supine left, supine right, fetal right w/knees drawn to chest, fetal left w/knees drawn to chest), and the alarm signal must function at or above the required 95 dBA sound level

Continued Reporting of PASS Performance Issues Encouraged

The Technical Committee anticipates that further knowledge concerning PASS performance will be gained as PASS designed and certified to the 2007 edition of NFPA 1982 become available cooperation with NIOSH and NIST, will continue to monitor the performance of PASS in order to assure that any issues and developments can be addressed through further revisions to NFPA 1982 as appropriate. Emergency services organizations and emergency responder personnel can greatly assist in this monitoring activity by reporting any PASS malfunctions and other problems with proper functioning of PASS directly to both the certification organization whose certification mark appears on the PASS, and to NIOSH – NPPTL. Be sure to give your contact information so they can follow up with you.

- SEI, the Safety Equipment Institute (certification organization), can be reached by e-mail at info@seinet.org.
- NIOSH – NPPTL, the National Institute for Occupational Safety and Health – National Personal Protection Technical Laboratory, can be reached by e-mail at NPPTL_PASS@cdc.gov.

Standards Gaps Identified by the PP&OE SubGroup

The PP&OE SubGroup has identified the need for improved standards efforts in the following areas:

- Standards for law enforcement PPE and technology suitable for tactical operations
- Canine standards for both the explosive and search missions
- Standards for explosive device mitigation equipment, such as disrupters and containment systems
- Identification of standards relating to water response equipment for surface and subsurface missions
- Performance criteria and standard for air-fed protective ensembles

Future and Continued Initiatives

Continue to expand the PP&OE SubGroup's efforts in developing an "all hazards" approach to its SEL topic matter.

Continue to endorse the alignment and integrated presentation of the SEL and AEL, to provide the response community with best access possible to IAB commentary and grant allowability information.

Ensure that the development of all standards relating to the performance and testing of include mandatory requirements for independent third-party testing and certification of products and equipment.

Continue to advocate for PPE standards for the law enforcement community that maintain necessary hazards-based levels of CBRN protection while, at the same time, meeting their specific mission-related requirements for fit, form, and function.

Serve as the primary emergency response community advocate though out the development of the national personal protective equipment roadmap.

PP&OE Chairs

Douglas E. Wolfe

Captain, Special Operations Coordinator
Sarasota County (FL) Fire Department

Douglas Wolfe, Special Operations Coordinator for Sarasota County (FL) Fire Department, has served with the IAB PP&OE SubGroup since 1999. He has spent 23 years in the fire service, including 16 years in hazardous materials emergency response. Captain Wolfe is an adjunct faculty member for the National Fire Academy and has coauthored numerous hazardous materials and terrorism response training programs for that academy, the FBI National Academy, the National Aeronautics and Space Administration, and numerous other state and federal organizations. He is the Florida Professional Fire Fighters' nominee to the Florida State Emergency Response Commission and serves on the Florida State Working Group for Domestic Security.

William Haskell

National Institute for Occupational Safety and Health/
National Personal Protective Technology Laboratory
Centers for Disease Control and Prevention

Bill Haskell is protective ensemble program coordinator for NIOSH National Personal Protective Technology Laboratory (NPPTL). NPPTL was established in 2001 by congressional directive to provide world leadership for the prevention and reduction of occupational disease, injury, and death for workers who reply on personal protective technologies. The NPPTL Mission is to prevent work-related illness and injury by ensuring the development, certification, deployment, and use of PPE and fully integrated, intelligent ensembles. Mr. Haskell serves on the NFPA Technical Correlating Committee for Fire and Emergency Services Protective Clothing and Equipment and NFPA technical committees for hazard materials, electronic safety, structural/proximity, special operations, and emergency medical service protective clothing and equipment. Mr. Haskell is a member of the ASTM International F23 Protective Clothing and E54 Homeland Security Committees and the IACP Homeland Security Committee. Prior to joining NPPTL he worked for 24 years at the Army Research Laboratory and the Army Soldier Systems Center. Mr. Haskell holds a B.S. in civil engineering and an M.S. in plastics engineering from the University of Massachusetts at Lowell.

Welcome to the ICIS section of this year's annual report. It has been a busy and exciting year for the ICIS SubGroup. We welcomed many new faces and saw some of our pillars move on to new and exciting work.

Mission

The mission of the ICIS SubGroup is to identify and make recommendations on a model suite of practices, capabilities, applications, and equipment that provide for secure and assured communication and information systems.

Role and Functions

The primary means by which the ICIS SubGroup accomplishes its mission is through the quick, efficient, and beneficial exchange of information, whether voice or data (i.e., communications). Communications continues to be listed among the top problems in after-action reports for major incidents and drills throughout the nation. "Interoperability" (or "interoperable communications") continues to be one of the most-used buzzwords in the realm of emergency response on all levels.

The ICIS SubGroup continues to recognize there are many groups working solely on improving incident communications. Some of these groups are tasked with developing long-term solutions, some are developing wide-reaching solutions, and some are mission- or discipline-specific.

Our role is unique in that we provide a direct two-way link between the first-responder community and our federal partners. We try to relay immediate or short-term communications needs from the responder community to the federal partners, by placing these partners in direct contact with the first responders themselves. We do not intend to circumvent representative agencies; in fact, many IAB members also participate in representative organizations (IAFF, Association of Public Safety Communications Officials International (APCO), International Association of Fire Chiefs, IACP, etc.). A strength of the ICIS SubGroup and the IAB as a whole has been that we continue to insist that our state and local representatives remain active in the response community. This relationship serves to

Interoperable Communications & Information Systems (ICIS) SubGroup

CO-CHAIR

Chris Lombard
Seattle (WA) Fire Department

FEDERAL CO-CHAIR

William Snelson
United States Marshals Service

Membership

Joseph Booth
Louisiana State Police

Ron Burch
Phoenix (AZ) Fire Department

Amy Donahue, PhD
University of Connecticut

Mark Hogan
City of Tulsa (OK) Security

Harlin McEwen
International Association of Chiefs of Police

Susan McGrath, PhD
Dartmouth College

Robert McKee
Texas Task Force 1

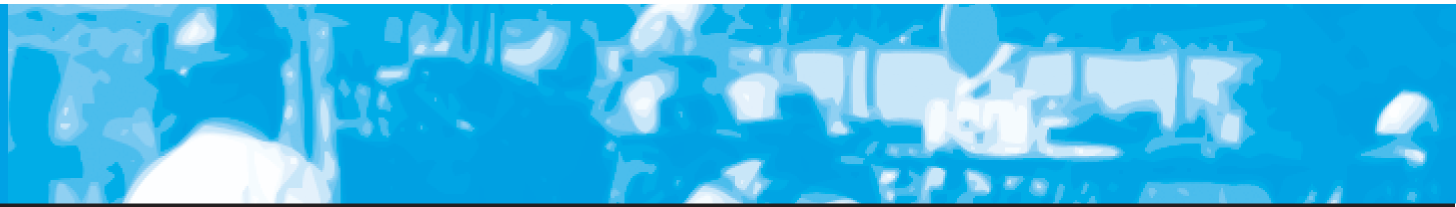
confirm or clarify to the federal partners those needs being expressed by the representative agencies. As an example, during the "white powder" scares that followed the anthrax-tinged mail in Washington, D.C., hazardous materials responders (from FDNY, Chicago, LA County Fire, LA City Fire, Seattle Fire, etc.—four of the five largest fire departments in the nation) were able to rapidly develop an impromptu, national, standardized response—all via a few phone calls.

While providing this upward flow of information, the SubGroup also acts as a conduit to disseminate information from the federal level down and throughout our respective disciplines. Information regarding grant programs, technology trends, resources, ongoing research and development, etc. is quickly shared with responders around the nation. Again, our goal is to provide another means to get information out to those who may not otherwise receive it.

As a SubGroup of the IAB, we continue to emphasize standards. The ICIS SubGroup has been involved in the development of standards for communications interoperability. Specific standard areas include but are not limited to the following:

- CAD-to-CAD interfaces
- Records management systems (RMS)-to-RMS interfaces
- CAD-to-RMS interfaces
- Radio interoperability (P-25)
- Communications support personnel (Communications Unit Leader, Communications Unit Technician, etc.)
- Cybersecurity

The SubGroup's members all have multiple titles (and wear multiple hats). Most are involved in a wide range of public safety communications–oriented groups, including SAFECOM, NFPA, Telecommunications Industry Association, communications committees for the IACP, Association of Public-Safety Communications Officials–International, and DHS's SAVER Program. SubGroup members also represent DHS, NIJ, the U.S. Department of Justice, DoD, and FEMA. They are engaged in practice, policy-making, and analysis. Through these agencies/associations and through other means,



Jeff Rodrigues
City of Chicago, Office of Emergency Communications

John Sullivan
Los Angeles Sheriff's Department, Emergency Operations Bureau

Mark Willow
New Orleans (LA) Police Department

Subject Matter Experts

Matt Devost
Technical Defense

Don Hewitt
Responder Knowledge Base

Walt Kaplan
Chemical Biological Incident Response Force Training Manager

Luke Klein-Berndt
National Institute of Standards and Technology, Office of Law Enforcement Standards

Mark Morrison
Louisiana State Police

Dereck Orr
National Institute of Standards and Technology, Office of Law Enforcement Standards

David Tritch
Kettering Fire Department/Ohio Task Force 1, FEMA Urban Search and Rescue

Mike Tuominen
National Interagency Fire Center

the SubGroup has been able to provide input and feedback on a wide range of communications-related issues and policy.

SubGroup Accomplishments

As mentioned above, some of our primary accomplishments have been the placement of knowledgeable public safety experts on groups that are starting to make significant progress in communications-related endeavors (i.e., hooking up the right people with the right people). In addition to the ongoing information exchange efforts (SEL maintenance, RKB-related work, etc.), our SubGroup expanded on four significant areas of work.

The SubGroup began a project with Dartmouth College pertaining to cybersecurity for public safety. We continued our work with NIST on Project 25 standards. For CAD-to-CAD interfaces, we began to investigate the emerging National Information Exchange Model (NIEM) framework currently being developed as a partnership between the Department of Justice and DHS. Finally, we began a significant effort towards the development of national standards for individual public safety responder communications personnel.

We began the year with an exciting conference at Dartmouth's Thayer School of Engineering. Dartmouth has been working closely with DHS to better quantify and qualify the threat posed by problems with or a lack of cybersecurity. This exciting venue provided an opportunity for public safety–related users (i.e., first responders from fire departments, EMS agencies, law enforcement agencies, city information technology managers and others) to meet with research staff and other experts. The users were able to get a quick education on the status of past, current, and pending cybersecurity issues. Other issues presented and discussed included the development of (gaming) simulators for use by public safety. Included at the end of this section (and available as a separate document) is an appendix containing the final report/outcome from the conference.

Another focus area for the SubGroup involved the refinement of the DHS Exercise and Evaluation Guides, the Universal Task Lists, and the Target Capability Lists (TCLs). In the spirit of "Don't just complain; provide suggestions for improvements and be willing to work on them," our SubGroup (led by member Dr. Amy Donahue) began a concentrated effort to improve the federal guides and lists. Dr. Donahue composed a white paper with the support and input of both this SubGroup and that of the entire IAB regarding the TCL process. Based on the paper, some modifications were made to the TCLs benefiting the entire first-responder community. Dr. Donahue and Vincent Doherty (Co-Chair of the S&T Committee) represent the IAB on a new interagency working group called the Capabilities Implementation Team (CIT), created by DHS G&T to help coordinate the various programs charged with implementing the TCL and to communicate with stakeholders about the TCLs. The CIT meets biweekly to discuss issues related to the TCL.

An example of the importance of this work was made apparent to some of our SubGroup members who volunteered to assist with DHS's Tactical Interoperability Communications Plan evaluation exercises. During these exercises, members used the aforementioned guides to evaluate the plans drafted by various regions of the country. In doing so, we were able to see real-world examples of what parts of an example guide (communications interoperability) worked and how the guides might be improved. Involvement in the Tactical Interoperability Communications Plan exercises also led to another project: the ICIS SubGroup began efforts to form a national effort to consolidate incident management system–related communications training.

The last several years have shown great technological strides toward making communications more interoperable. The interoperable equipment that is now available ranges from minor, local patching equipment, to infrastructure specific support tools. Equipment is now available to readily patch almost any number and type of communications devices together. What has been lacking is widespread recognition that trained, knowledgeable and qualified individuals are essential to successfully integrate the interoperable hardware solutions. Without the proper individuals to make them work, even technically sound communications systems fail! Entire infrastructures can be crippled and cause extreme safety hazards.

SubGroup Member Accomplishments

Some ICIS members are currently active within project SAFECOM, a communications program within the DHS Office for Interoperability and Compatibility that provides research, development, testing and evaluation, guidance, and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications.

The ICIS SubGroup is also active with the Project 25 steering committee. In recognition of the need for common standards for first responders and homeland security/emergency response professionals, representatives from APCO, the National Association of State Telecommunications Directors, selected federal agencies, and the National Communications System established Project 25, a steering committee for selecting voluntary common system standards for digital public safety radio communications. Work on standing up the Project 25 Compliance Assessment Program is well under way. The first test reports will focus on subscriber units and will test the Common Air Interface. The initial reports are targeted for early spring. The initial ISSI (Inter-RF Subsystem Interface) messaging and protocol standards document has been published. Both the CSSI (Console Subsystem Interface) and FSSI (Fixed/Base Station Subsystem Interface) now have stable messaging and protocol standards documents completed.

Several ICIS members are also active in DHS G&T's Fusion Center ventures. The Fusion Centers are created to form groups that are capable of detailed analysis fusion and dissemination of information to support operations, response, and decision making needs of local responders. Cooperating agencies usually include local, state, and federal law enforcement, emergency management, fire departments, transportation authorities, universities, airports, and criminal justice agencies. DHS has expanded on the initial Terrorism Early Warning work and is now in the process of helping to establish Fusion Centers. SubGroup members continue to assist in these efforts providing examples and expertise.

The ICIS SubGroup continues to screen those communications and information technology–related portions of the RKB and SEL and to work with G&T on the AEL.

It is perhaps in this last role of "go-between" (among DHS's grant guidance section, the first responder community, and the larger communications interoperability groups—SAFECOM, et al.) that we have seen some of our greatest successes. As with most of the IAB SubGroups, the conditional linking of federal grants to standardized equipment and standardized lists has accelerated interoperability throughout the many disciplines within public safety's response to incidents.

Current ICIS Priorities

As the definition of "first responders" grows (fire, police, EMS, military, etc.), so too are their specific needs in terms of interoperable communications, information systems, related equipment, and associated philosophies. Before, during, and after any appreciable incident, the communications needs invariably change in form, magnitude, and content. Individuals and agencies come and go, their roles may wax and wane or change suddenly, and the very structure and content of the communications needs/infrastructure often change. To that end, the ICIS SubGroup has attempted to establish focus groups that are able to report back to the whole SubGroup. Some of the specific focus areas include cybersecurity, communications-related training, and the role of communications within the National Incident Management System.

While all SubGroup members contribute to all of these focus areas, the members use their own experiences, respective agencies, and educational backgrounds in their division(s) of choice.

The standards-making progress is complex and time-consuming. A sample of some of the areas we continue to work on includes the following:

- Development of Cyber Security Requirements to protect information systems and the technology required to support disaster response capabilities at all phases of operations (pre-, trans- and post-incident)
- Development of standards for geospatial intelligence, including visualization and the need for geospatial standards
  - Mapping tools, GIS, symbology, integrating geospatial tools with data-mining results
  - Modeling standards (especially for fate and transport, i.e. plume models, etc.)
- Information/data fusion (including geospatial, data-mining, production, dissemination and distribution)
  - Need for interoperability and "continuity of operations" for use of software agents and development of secure portals/data exchange
  - Need to integrate cybersecurity/surety into all tools
- Adaptive bandwidth management
- Virtual reachback (for data, voice, video, multimedia, etc.) and tactical telemetry (sensor arrays)

Future Trends/Priorities

In addition to the current goals and priorities listed previously, the ICIS SubGroup has been working with the S&T SubGroup and their partners (TSWG, national laboratories, etc.) to further the development of equipment/systems that enhance interoperable communications. Examples of just some of the ideas include the following:

- Dual-channel/intercom-style portable radios—Our respective user communities have stated they could all benefit from a hands-free, voice-activated portable radio that operates as an intercom between a small working group in close proximity to each other. The expectation is that the few members in the group would hear each other at all times, while also being able to hear another frequency/channel (Fire Ground Tactical Channel, Fire Ground Command Channel, etc.). Users would have the option to then talk on the alternative frequency/channel by keying their portable radio microphone.
- Blimp antennas—The ability to quickly set up significant regional communications is lacking (shuttle disaster, Katrina, 9-11, etc.). What is needed is the ability to establish a pseudo communications satellite. An example would be a tethered blimp hovering high enough (>40,000 feet) to provide coverage to entire regions. Devices such as this would theoretically be like setting up a single, temporary, stationary antenna that could be used to establish secure and nonsecure communications over an area spanning 500+ miles. Unmanned Aerial Vehicles also offer important opportunities in this area.
- CAD-to-CAD interface—There is an emerging National Information Exchange Model framework currently being developed as a partnership between DHS and the Department of Justice. NIEM would allow different agencies' CAD software to seamlessly exchange information. As an example: A city police agency is dispatched to a domestic situation that escalates into an assault or

police officer shooting. The responding fire/EMS immediately have, in their own dispatch content, information pertaining to the ongoing incident (initial start time, that X number of police units are assigned, that the call started out as a simple disturbance, which agencies are involved, etc.).

As a SubGroup, we are excited about the distance that interoperable communications has come and the direction it is going. We look forward to our continued work in these efforts.

ICIS Cybersecurity Subgroup Meeting

On February 8-9, 2006, The Interoperable Communications and Information Systems (ICIS) Subgroup of the Interagency Board met at Dartmouth College's Thayer School of Engineering. The purpose of the meeting was to discuss modifications to Section 5 (Cyber-Security Enhancement Equipment) of the Standardized Equipment List and to educate subgroup members in cybersecurity issues related to emergency response.

ICIS attendees:

Amy Donahue, University of Connecticut
Bill Schrier, City of Seattle Chief Technology Officer
Chris Lombard, Seattle Fire Department, State & Local Chair
Don Hewitt, Responder Knowledge Base
Harlan McEwen, IACP
Jeff Rodrigues, City of Chicago
Jessica Russell, Battelle-InterAgency Board Program Office
Joey Booth, Louisiana State Police
John Sullivan, Los Angeles County Sheriff's Department
Luke Klein-Berndt, NIST
Mark Morrison, Louisiana State Police
Ron Burch, Phoenix Fire Department
Susan McGrath, Dartmouth College
Troy Sella, Los Angeles County Sheriff's Department
Walt Kaplan, Battelle

Speakers:

Dennis McGrath, Dartmouth College
Mark Stanovich, Dartmouth College
Bill Stearns, Dartmouth College
George Bakos, Dartmouth College
Chris Goggans, SDI, Inc
Matt Devost, Terrorism Research Center

Workshop Summary: The workshop was divided into three parts: the first consisted of talks provided by cybersecurity experts to inform the attendees about the fundamentals and prevention techniques of cybersecurity; the second phase provided the attendees with various cyber threat scenarios to illustrate the critical role that diligent security protocols play in protecting information systems; the final part of the workshop involved an interactive exercise in which the attendees and cybersecurity experts worked together to attack and defend prototypical information infrastructures.

The cybersecurity seminars were presented in an instruction-discussion format that encouraged participation by the ICIS Subgroup members. Dennis McGrath presented an Introduction to Computer Security. Dennis is a Principal Investigator at the Thayer School of Engineering and has been a primary exercise designer for several cyber security exercises. Dennis's presentation included definition of the four most common examples of network attacks, and the general taxonomy of computer attacks as defined by CERT (DHS – United States Computer Emergency Readiness Team). The presentation also included a glossary of terms common to computer security, and a brief description of how hackers might perform reconnaissance and gain access to a network. Some important points made during this presentation included:

- Network attack examples include interruption (denial of service), interception (credit card/identity theft), modification (vandalism of web sites), and fabrication (creation of bogus web sites for illicit purposes).

- The taxonomy of computer attacks examined the attackers, tools, how access was gained, results of attacks, and the attackers' objectives for an attack. Attackers' characteristics range from "script kiddies" who disrupt networks and websites for thrills, to highly-skilled professionals who are "hired" by hostile entities and nation-states who are capable of serious damage to critical infrastructure.

- Hacker objectives can be defined using the "CIA Model", meaning the attacker is looking to disrupt the confidentiality, integrity, or availability of the targeted network. An attack may be designed and launched to achieve a single objective, a combination of those objectives, or all three concurrently.

- The relationship between vulnerability and exploit was defined as the following: vulnerability is a weakness in hardware, and an exploit takes advantage of that vulnerability. Sometimes web servers can run without the knowledge of a network manager, which potentially creates a vulnerability, which can then be exploited.

- "Security through obscurity" is a method of attempting to hide critical functions and processes that a network performs among many other functions. Though this is prudent as a secondary measure, it is insufficient as a primary means of security. An adversary that knows how to recon your network will find what he wants to find.

- Spoofing is a term describing a person or entity who is masquerading as someone or something else. Some of the things that are spoofed are web sites, IP addresses, and e-mail addresses.

- Social Engineering is a form of spoofing in which the perpetrator attempts through misleading or false pretense to convince people to give up information they would not normally divulge, such as banking or credit card information, other personal data.

- Authentication is the verification of identity using passwords, tokens, and/or biometrics. Encryption is a mathematical algorithm that obscures information. The receiver must have the same algorithm to decode and read information.

- A virus is a malicious code that attaches to or replaces existing code, usually requiring human intervention to spread to other computers (downloading, opening e-mail attachments, etc.).

- A worm is executable code that is capable of replicating itself and spreading without human intervention.

- A “backdoor” is a program that gives an attacker alternative access to a machine.

- A Trojan (horse) is a malicious program that arrives disguised as something innocuous.

- Rootkits are applications that alter or replace existing system components, creating the illusion of normal operations, and covering the tracks of attackers.

- Bots, zombies and drones are compromised machines that await attack commands from their masters. They can be used to launch DDoS attacks, and can be obtained by trojans, direct exploits, worms, or trading information.

- A buffer overflow exploit is the use of cleverly crafted over overflow data can be used to place executable code in a data buffer. There used to be only one way to attack computers, but buffer overflow exploits changed everything. Input buffers should be checked for size, as unchecked large input can overwrite other buffers

- A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. Basically, a firewall, working closely with a router program, filters all network packets to determine whether to forward them toward their destination.

- A Demilitarized Zone (DMZ) is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

- Intrusion Detection Systems may be signature based— a format that looks for specific attack, or anomaly based— where the system is looking for something outside of normal network activity.

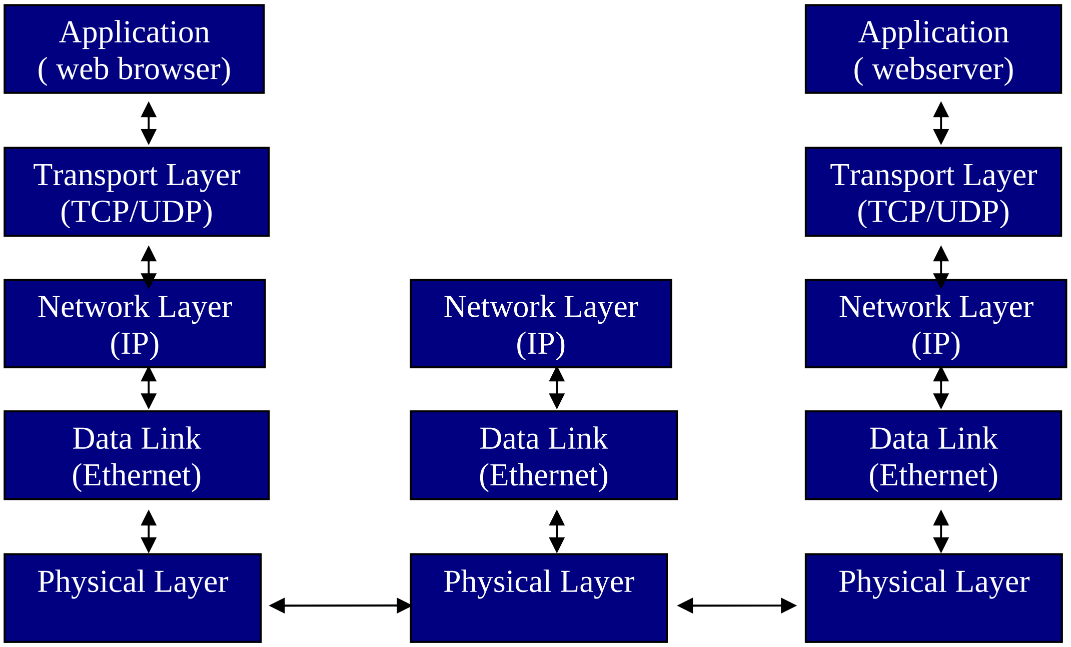
- Phishing is a scam that consists of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

- Spyware is a general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use spyware to gather data about customers. The practice is generally frowned upon.

- Network Protocols include
  - IP - Internet Protocol
  - ICMP - Internet Control and Messaging Protocol
  - TCP - Transmission control protocol
  - UDP - User datagram protocol
  - HTTP - Hypertext Transfer Protocol

- Data Encapsulation can be thought of as a set of Russian nesting dolls, in that each protocol is contained inside another protocol, with the data to be encapsulated being in the smallest and most protected protocol.

- Network Communications is a communication between a workstation, router, and server, with data traveling the opposite path for return communications. The diagram below illustrates the passage of data between workstation, router and server.



- When establishing Virtual Private Networks (VPNs) it is important to remember that all VPNs aren't equal, and they aren't necessarily private. If you are relying on VPN for critical secure communication then you need to have a continuous threat assessment; you may need to have additional security on top of VPNs. It is important that you make sure the security is inherent in a VPN.

- Port numbers allow multiple applications to share network access. The Well Known Ports are those from 0 through 1023 (managed by IANA). The Registered Ports are those from 1024 through 49151, and the Dynamic and/or Private Ports are those from 49152 through 65535.

- Hacker Modus Operandi - The MO for a hacker is to perform reconnaissance on the target network or system, scan that system, utilize an exploit to gain access, maintain and expand that access, upload tools for extracting data, downloading information, and cover his tracks so that the network manager could not detect the hacker's presence.

- Reconnaissance consists of finding out as much as you can about a computer or network. This can be done by network footprinting, accessing websites, running a "whois?" query, or a variety of low-tech methods.

- Scanning is the equivalent to rattling doorknobs, and can be accomplished by a number of different methods. War dialing is the process of dialing a series of numbers looking for an active dial-in connection. Ping sweeping and port scanning are methods of determining what ports and IP addresses are actively used by the network. Traceroute is the mapping of data paths into and out of networks, determining which hardware and software devices data passes through to reach into and out of the targeted network or workstation.

- Gaining Access to a network can be accomplished in a variety of ways, many of which are detailed above. Passwords and usernames can be compromised, security information can be obtained via spoofing, individual machines can be hijacked (zombies!), and software vulnerabilities can be exploited. Access can be maintained by manipulation of event logs, or via a backdoor, or a root kit can be installed that will allow access and manipulation of the system to occur undetected.

Bill Stearns from Dartmouth’s Thayer School of Engineering and SANS Instructor, presented an instructional seminar concerning User-Level Security. This seminar introduced and explained the common tools and processes that a user can employ to assist in overall network security, with some basic recommendations as to the employment of those tools. Key points included:

- Passwords are a simple and effective way of authenticating access to networks. In order to remain effective, users and administrators must pay attention to password length and complexity, along with minimum/maximum password age.

- Physical tokens are another method of authenticating users on a network. They plug into a computer and contain verification of permission for access. Some examples of tokens are SecurID and CryptoKey.

- Certificates are “soft” keys that verify ID of holder. A certificate holds cryptographic key which vouches for the holder’s identity. Server certificates authenticate the web server.

- One-Time Passwords (OTP) are a very effective method of providing security. With a one-time password, a cclient and server agree to change password for each and every exchange. This process can be time based, or a function of selection from a list of passwords. The concept is that a password from one minute ago won't work now. Software is available that creates a new password with every log-in.

- Proximity Locks are devices that will close access to networks and clear screens should the user move more than a specified distance from the workstation. There are two types of proximity locks. One type plugs into a USB port on your computer that the user removes when leaving the workstation. The second type clips on to a belt and locks out if the user moves a few feet away from his/her computer.

- Administrative vs. User permissions are a major source of security problems. Administrators have no restrictions on their access, where users are limited in what they can do based upon job requirements. Users can only view certain files unless given specific permission for others. Ideally, user accounts are used for almost everything but practically that is tough to accomplish.

- File and printer sharing can be a little-known vulnerability. Most of us don't need to share the printers on our laptops in order to be able to use a printer somewhere else in the building.

- Password Settings are extremely important to maintaining security. Below are some suggestions for guidelines in assigning and updating passwords:
    - Minimum length (6-8 characters for user, longer for administrator account)
    - Mix of digits, punctuation, lowercase letters and uppercase letters
    - Maximum age 90-180 days
    - Minimum age 2 days

  These are guidelines, but you must decide for yourself and consider your location and the relative damage that could be done to your system

- Personal firewalls are software that runs on a computer and looks at what kind of conversation is running in and out of a machine. There are problems with these, as sometimes they can't tell what is malicious and what isn't. The solution to this problem lies with establishing a basic level of common user education.

- A choice in security posture is the one between software and employing a SOHO (small office/home office) router. A SOHO router is convenient and effective for multiple machines, whereas a software installation is good for portable systems. Some of the other considerations in that choice are outlined below.

- Routers do need to be patched from time to time to get the most updated features. Security managers have to take care that all parts of the network interact and work well together.

- There are standards that can help solve the issues that may come from network interactivity, however interoperability is a major factor as well. Some of the questions that must be asked are:
    - How do you protect your system from being disrupted?
    - How important is it to protect the information you are sharing on your network?
    - You have to assess the risk of the information getting out.

  - What training curricula are available that can be put in academies to educate users?
  - What about software that requests that you disable your firewall? Perhaps the firewall just doesn't understand that you have a legitimate use of the software. Some people may open themselves up to vulnerabilities by installing such software.

- Another choice for user-level security is that of managed vs. standalone Firewalls. A standalone firewall is less expensive to buy, easier to set up, but a managed firewall may be less expensive in the long run because you can check to see if people are running their antivirus software, you can update their software, etc. www.firewallguide.com/software.htm provides a useful firewall guide.

- Antivirus software is a required piece of any system at this point. There is a need to scan entire drive weekly. This is necessary to make sure all systems are safe. Regular signature updates are necessary, as well.

- Anti spyware software is a critical element to network security. Spyware consists of applications that send back information about the Web sites you visit, which can be a privacy issue. Spyware can show up in an e-mail, from a Web site you visit, or pop-ups of online offers, etc. It is prudent to employ two types of this software on every machine. Some commercial examples of anti-spyware programs are AdAware, Seek and Destroy, Hijack This.

- Encryption is a system that is visible to protect your information. Encryption hides text in an unreadable form. Once the recipient decrypts the information, it becomes readable again.

- E-mail Protection is important, as a means of protecting information as it travels. IMAPS encrypt the messages in transit; however, encryption doesn't apply to the messages at either end. They are read and stored in plain text.

- PGP and GPG are two methods of encrypting and signing e-mail files. What is required is to have someone's public key to ensure you received an e-mail from them.

- Sensitive data can also be stored off-system, such as on USB tokens or external drives.

- Security for web browsers include using HTTPS, the SSL browser was designed to protect secure information.

- Personal certificates are another method of securing access to sensitive data. Pay $15-50 for a file you save (on your hard drive or USB drive), and that is your way of authenticating yourself to someone else.

- File encryption can encrypt one file or can encrypt an entire drive if necessary.

- Physical security is an often overlooked aspect of user level security. There are usually common sense solutions such as locks for desktops/laptops, and controlled access to rooms and equipment.

- Backup security is another relatively easy step. A good place to start is to answer two easy questions. Do you have backups? If you do, who has access to those backups?

George Bakos, also from the Thayer School of Engineering and a SANS Instructor, presented the next instructional seminar on the principles of network defense. Mr. Bakos provided common definitions of network defense tools, the capabilities and limitations of those tools, as well as a basic approach to network defense for network administrators. He also discussed the need for enforcement of sound network security policies, and the four basic elements of a well-thought network security plan were also discussed. Key discussion points included:

- The question that a network administrator must answer is: What are we defending? We are defending information that makes us a value to the community, and network communications are what we are depending upon. We put a lot of faith into these systems. These systems can be easily accessible, and if the bad people out there get into our network—they can make a lot of money from this, and disrupt our abilities to operate.

- Over-The-Wire attacks are attacks that come from remote locations into a network. They include resource exhaustion/denial of Service (DOS) attacks. Others include attacks exploiting buffer overflows, and user-facilitated compromises such as e-mail viruses, worms, trojans, or phishing. Man-in-the-middle attacks such as eavesdropping or modification or gaining unauthorized access (where encryption may not help) are also over-the-wire attacks.

- Defense in Depth is the concept of having many layers of protection such that if one layer falls away, the other layers will still protect your network. If one layer fails all may not be lost. It's not a true defense in depth if any one of the layers is critical to your mission. The systems that comprise perimeter defense include firewalls, intrusion detection, intrusion prevention, and deception systems (e.g., honeypots).

- Firewalls are policy enforcement engines. They do both ingress and egress filtering, and provide an audit trail of activity going in and out of the firewall. False alarms are common with employing firewalls. Most events are false alarms, but one has to be careful not to ignore alarms, as they may be alerting you to a real threat.

- Not all proxies are firewalls and not all proxies do policy-based filtering. A proxy acts on your behalf to make sure everything is correct on both ends. Proxy activity requires another program to be running and may use a lot of resources.

- There are limits to the protection that IDS provides. There are ways to compromise an IDS. An IDS can show you that there is something happening, but it doesn't tell you why. An IDS can give you false positives or, if not configured right, can produce false negatives.

- Honeypots are decoy networks set up to distract adversaries from more valuable machines on a network. Honeypots can provide early warning about new attack and exploitation trends and they allow in-depth examination of adversaries during and after exploitation. Honeypots can tell you the attacker's intent with a good analysis of the information. Honeypots can be either exposed or interleaved.   It is important to note that Honeypots are risky for tactical and technical reasons.

Don Hewitt, ICIS member and cybersecurity expert provided a presentation on the Risk Knowledge Base. He discussed in more detail some of the vulnerabilities common to networks and what evaluation a network manager has to make to mitigate those threats.

- A network administrator needs to decide which is most important—confidentiality, integrity or accessibility—but should keep all 3 in mind when building network security.   One has to increase awareness and understanding of information security issues but it's not a solvable problem as there isn't a person anywhere who can understand everything about an operating system.

- Security is often the enemy of efficiency. The easier it is for authorized users to access information, the easier it is for an attacker. Attackers have the advantage because it's difficult to defend yourself against any single possible attack

- TCP and IP are the protocols that enable the Internet, but TCP/IP has vulnerabilities—there are superfluous services that start by default. There are over 65,000 ports that exist and only the first 1024 are reserved.

- Everything that an attacker does is connected
  - Ping—see if host is on network
  - Port scan—see which ports are responding on hosts
  - War-dialing—searching for a carrier tone
  - War-driving—searching for wireless account points via car, you can discover that about 60% of points are unsecured

- Buffer overflow vulnerabilities are the result of pathetic programming. Major software companies are working to close those holes but it will take time. Many haven't been announced and won't be until exploited.

- The biggest security problems today are the same as they were in 1971—password discipline and dialup connections.

- A network administrator or user must not assume:
  - It's only a workstation—if it's connected to your network, it's a potential attack platform.
  - No one will "see" a dial-up connection—if you have a telephone, you can see a dial-up connection.
  - The manufacturer's default settings will be fine—this is almost never true.
  - It will be ok to connect this one machine across multiple networks for ease of use—all it takes is one connection between the 2 networks and they're connected.
  - The threat is from the outside—threats are largely from the inside.

- On the inside users and administrators must stay away from a "perimeter mentality". This can lead to poor discipline and password protection. It is also a misperception of the threat. It is vital to have an internal permission scheme and internal segmentation. Any penetration turns internal vulnerabilities into external vulnerabilities.

- There are several countermeasures, but there isn't a silver bullet. Scanning tools are useful but won't fix your entire network. Firewalls, intrusion detection, virtual private networks, and encryption are all parts of an internal security scheme.

- One of the most underrated tools in computer security is putting a system in place that tracks the versions of the software on your computers, printers, etc.—anything on your network. Patching is a big step toward getting control of and protecting your network.

- Paper is not an adequate countermeasure for network security. It has to be an ongoing effort. You can't have perfect security. The goal is to do due diligence.

- There are four main components to a security program
  - Policy—where management makes its stand on what is necessary
  - Risk Assessment—critical to have a 3rd party assessment
  - Training—mandatory awareness training for everyone who touches the organization's network
  - Technology Deployment—needs to be done in response to the identified threat

Matt Devost from the Terrorism Research Center presented information on the importance of having a third-party assessment of network vulnerabilities. Some of the highlights of Devost's discussion included:

- Certification and accreditation is not the same thing. Certification is objective; it is a test or series of tests against known variables. Accreditation is a subjective decision-making process, looking at risks and deciding which risks we can live with.

- Risk assessment parameters must include the disruption of social integrity. We must consider the context of threats, concerns at the impact level and the likelihood of an attack. This assessment will drive what actions need to be taken.

- Threat Agents to consider include both external and internal threats, e.g., terrorist attackers and disgruntled employees.

- Risk assessment is a somewhat subjective process that includes vulnerability assessment, which can be more objective. Vulnerability assessments take the attacker's perspective. They include internal and external attacks. Such an assessment should validate your existing security methods to see how well the real world matches up with the policies you have in place. It should also have a detailed analysis of the networked devices and services you currently have, and include an audit of best practices. It is critical to have a baseline assessment which will allow serious problems to be addressed quickly, and provide a means to address real problems and discuss future best practices.

- There is a widespread perception that the Internet poses the greatest threat to networks. The reality is that the Internet is a pretty well-controlled threat. The internal connections as well as dial-up and wireless connections are the larger threats.

In part two of the workshop, Chris Goggans from SDI Inc. moderated a discussion of real-world examples of IT security breaches. The discussion included observations from Matt Devost and Don Hewitt.

Examples provided illustrations of how organizational information technology policy and procedures often contribute directly to breaches in security:

- An Insurance company had employees posting to USENET groups and mailing lists. These usernames could be used to access internal network providing unauthorized access.

- A telephone company utilized dial-up modems with un-password protected PCAnywhere. The PCAnywhere system was used primarily for internal camera monitoring, and coincidentally provided full access to its internal network.

- A defense contractor had a compromised printer on a telnet interface that provided access to routers. The system administrator used the same password on the router as he did on his personal account.

- A power company had a workstation on its internal network with an unpatched web server. The password file was pulled from that workstation and used to get access to the domain controller. The attackers could then act as system administrators and give themselves domain administration permissions. Using this strategy, the attackers were able compromise a power grid engineering and management workstation which allowed control of the grid system.

- A county government in the Midwest had poor password policies which allowed easy access to administrative privileges. This allowed attackers to view court dockets, tax documents, etc. The county also had a server that was vulnerable to a UNICODE attack and discovered the server had already been attacked at 2 different times 6 months apart.

- An organization was responsible for state-wide EMS and had dedicated lines to other state-run networks. The firewall rules allowed certain hosts into the EMS network using unsecured protocols. The network access was leveraged to compromise of about 98% of all IP addresses on the network.

- A government agency that maintained its own police force had an unpatched machine as its web server, allowing access to password files on another machine on the network. The passwords were then used to compromise machines used for investigation purposes.

Some observations regarding these examples:

- The Internet is very easy to secure, but modems don’t get the attention they deserve.

- Patch and configuration management are consistently neglected if not outright ignored.

- Partner connectivity is a big problem. Just because they're your partner doesn't mean they are as secure as you are or adhere to the same baseline level of security as you.

- Poor passwords are the primary mechanism to gain host-level access.

- Wireless usage continues to explode, and unless that is properly managed, there will be problems. Requisite security is not keeping up with growing usage.

- About 20% of security actions taken will replace ~80% of network vulnerabilities. As a Network Manager, you can't solve security and then walk away from it. You have to fix your vulnerabilities and then stay diligent. Due diligence requires a security program as well as a security attitude.

The third phase of the workshop began with a discussion-based exercise moderated by Bill Stearns and George Bakos. The attendees were split into 2 groups (Attackers and Defenders) to discuss a fictional, but prototypical information infrastructure ("West Dakosha Department of Public Service"). The players were given a sample network design for the fictional public service network. The goal of the exercise was to critique the network and propose software to be used, network design changes, and system security improvements. As a team, members were to come up with suggestions for defending and attacking the network.

Additional network details included:

- The network was running mostly Microsoft operating systems and Cisco routers.
- The perimeter network used Microsoft Sharepoint for email, instant messaging, and collaboration between client MS Office applications.
- Firewalls and their policies were maintained internally.
- Additional software used on the network included Symantec Antivirus, iBase, Analyst Notebook, Arcview, Cognos, and Crossflow.

Defenders were to consider how well the network was configured and to make recommendations for cyber security policies and procedures. The defense team was asked to consider the following:

- Choice of software
- Network layout
- Ease of maintenance

- How many layers of security protect a resource
- Redundancy issues
- Potentially vulnerable services and how they're protected

The questions below were for consideration in the context of the exercise.

- What strengths do you see in this network design?
- What weaknesses do you see in this network design?
- Are there any missing components?
- What potential threats do you see against this network?
- What steps could we take to reduce the risk to the network?
- What are your impressions about the pieces of software used?
- How could we improve reliability and uptime for critical services?

Attackers were to consider an attacker's mindset and determine approaches for breaking in to the network. The attack team was asked to consider:

- Choice of software
- Network layout
- How many layers of security protect a resource
- Potentially vulnerable services and how they're protected
- Ability to detect intrusions on the network

The questions below were for consideration in the context of the exercise.

- What servers can you reach from the Internet?
- What publicly visible services are they likely to be running?
- If you could get physical access to the computers on this network, what could you do to get confidential information?
- If you couldn't get Internet or physical access, what other approaches are available to you?
- You find a laptop at a conference that has a VPN connection back to this network. How could you use this to attack the network?
- What methods could you employ to avoid detection during the attack?

Actions of the attackers and defenders were discussed, as were participants' responses to the questions posited. Several participants commented on the value of such exercises to put the security concepts into real-world context.

ICIS Chairs

Christopher Lombard

Communications Special Operations
Seattle (WA) Fire Department

Christopher Lombard works for the Seattle Fire Department, where, in addition to working both in the operations division and as a dispatcher, he manages a variety of projects, including communications coordination for the department's specialty teams, liaison for the department's interoperability with other jurisdictions, and project manager/coordinator for the department's mobile computing. His current responsibilities include the coordination, management, and maintenance of communications equipment and policies for special operations teams (including Urban Search and Rescue, Metropolitan Medical Response Systems, EMS, etc.). Recent projects he has helped coordinate within the department include a wireless data project (mobile computing), interoperability initiatives, and CAD/records management system upgrades. Mr. Lombard has been in the Fire Service for about 15 years and a member of the IAB and the ICIS SubGroup from their onset. He is also involved in active communications-related roles on NFPA 1221 (the standards committee for Public Emergency Service Communication), Project SAFECOM's Advisory Group, FEMA, and as a public safety communications instructor at Texas A&M University/Texas Engineering Extension Service.

William Snelson

Chief, Office of Emergency Management
United States Marshals Service

Bill Snelson has over 24 years of experience in law enforcement, beginning with the Buncombe County (NC) Sheriff's Department. In 1991, he went to work for the U.S. Marshals Service. Since then, he has risen through the ranks to his present position as the Chief of the Office of Emergency Management. Chief Snelson oversees numerous programs, including the Strategic National Stockpile Security Operations, the Canine Program, the Incident Management Teams, the Peer Support Team, the Missile Escort Program, the Communications Center, the Emergency Operations Center, Continuity of Operations, and Continuity of Government. Chief Snelson became a member of the IAB in 2003.

Mission

The D&D SubGroup provides input, direction, standards, and information to first responders on equipment for sampling, detecting, identifying, quantifying, monitoring, and decontaminating WMD agent (CBRNE) contamination throughout designated areas or at specific points, and items that support detection activities.

Functions

The D&D SubGroup is responsible for addressing equipment identification, interoperability, and standardization in complex areas of D&D: chemical warfare agents, TICs, biological warfare agents, radiological/nuclear materials, and explosives. This work is accomplished by articulating user requirements for D&D equipment; identifying existing equipment guidelines or performance standards that address user requirements; and developing, maintaining, and updating the D&D portion of the SEL which provides the responder a reference to the type of equipment required to prepare for, respond to, mitigate, and recover from a CBRN incident.

Goals

- Facilitate the exchange of information between the first responder community, government agencies, and the private sector, including the sharing of knowledge, expertise, and technology regarding the detection, identification, warning, and decontamination of CBRNE incidents.
- Participate in the development and implementation of performance criteria, standards, and test protocols for D&D response equipment and identify additional equipment and standards requirements.
- Facilitate and promote the standardization and interoperability of D&D capabilities to optimize response team integration and operations at the local, state, and national levels.

Detection & Decontamination (D&D) SubGroup

CO-CHAIR

James Schwartz
Arlington County (VA) Fire Department

FEDERAL CO-CHAIR

Elaine Stewart-Craig
Department of Defense, Research, Development and Engineering Command, Edgewood Chemical and Biological Center

Membership

Ed Bergamini
Fire Department, City of New York (NY)

Thomas Brandon
Suffolk County (NY) Police Department

Charlie Brannon
National Naval Medical Center

Steve Clendenin
Massachusetts Department of Fire Services

John Eversole
International Association of Fire Chiefs

Alim Fatah
National Institute of Standards and Technology

Mark Gutke
Jefferson County (CO) Sheriff's Office Bomb Squad

- Facilitate and promote the proper selection and use of the best available D&D equipment and procedures to optimize safety, interoperability, and efficiency.
- To encourage governmental, military, and private agencies, as well as manufacturers, to sponsor priority R&D projects to satisfy local, state, and federal CBRN incident response equipment requirements.
- To encourage the development of detection capabilities for an all hazard approach.

Current Projects

Decontamination

Chemical Warfare and Toxic Industrial Chemical Contamination Levels Study

Chemical warfare contamination level studies, using simulants, are being conducted at ECBC in support of the DHS/NIST Standards Development Program. The studies are being conducted as a testing program to provide real-life levels of contamination that may be experienced by victims or emergency response personnel. A report entitled “Experimental Methodology for Assessing Hazardous Materials Deposition on Personnel and Interior Facilities from Diverse Dissemination Devices” was published in 2006. This report and the experiments performed to complete it are being used to verify the levels of contamination that are currently used to evaluate respirators and protective ensembles as well as personnel decontamination equipment. A final report regarding explosive contamination tests using simulants of semipersistent chemical warfare agents is due in 2007. Explosive contamination tests using simulants of persistent chemical warfare agents are in progress using the same methodology and protocols.

Decontamination Equipment Testing Needs

The D&D SubGroup has been concerned that there no performance standards are currently being used by manufacturers of decontamination equipment that state the efficacy and the casualty flow-through rates for particular pieces of equipment. There is also concern over the variation from vendor to vendor and product to product from the same manufacturer. Until there is a testing and certification program for the decontamination equipment, such as water pumps, decontamination showers, and

Roger Hatfield
Nashua (NH) Fire Department

Gene Ryan
Chicago (IL) Fire Department

Peter Stevenson
Environmental Protection Agency

Wes Thomas
Downers Grove (IL) Fire Department

Michael Walter
Department of Defense, Joint Program Executive Office for Chemical and Biological Defense

Subject Matter Expert

Ed Bailor
United States Capitol Police (Retired)

James Stewart
National Institute of Standards and Technology Support Contractor

entire decontamination systems, all responders have to perform their own evaluation of each piece of equipment they buy to ensure it meets their needs.

To address these concerns the DHS S&T Directorate's First Responder Chemical, Biological, Radiological, Nuclear and Explosives Protective and Operational Equipment Standards Development Program has prioritized the development of these standards to address these shortcomings based on the IAB's priorities. Standards for performance criteria for water pumps intended to be used in decontamination systems are in development based on the needs of the responder community.

Decontamination Equipment and Methods Database

This database, developed last year from a decontamination literature study performed by ECBC under the DHS/NIST Standards Development Program, will continue to be updated as new information becomes available. This information will be provided to the RKB for incorporation with the SEL.

Detection

Biological Sampling

In September of 2001 five letters contaminated with anthrax were mailed, and fatalities resulted from those letters. After that incident, response agencies from across the country at all levels were inundated with calls from the public to sample powders of all types. Since that time and based on increasing experience and a lot of opportunity for discussion within the responder community, many active response agencies have worked with their laboratories in the national Laboratory Response Network (LRN) to agree on how samples should be collected and submitted. These processes have since become locally standardized.

In 2006 ASTM Committee E54, Homeland Security Applications, released ASTM E2458-06, "Standard Practices for Bulk Sample Collection and Swab Sample Collection of Visible Powders Suspected of Being Biological Agents from Nonporous Surfaces." The group of individuals who wrote and reviewed the document came from diverse backgrounds and included members of the IAB. However, the release of the document has raised many issues from the users in the field as to how this document could or should be implemented. With the issuance of a national standard such as E2458-06, it became unclear how the protocols already in place with the LRNs might be affected. The community is extremely concerned that the new document will undo the hard work that has taken place between the local communities and the LRNs to come to agreement on the sampling and packing of suspected biological samples. The D&D SubGroup is heading an effort to consolidate responders' concerns with the sampling standard, which will then be presented to the ASTM committee with a request to make the changes immediately as opposed to waiting for the normal revision cycle.

Biological Detection

There continues to be a need within the response community for detection capability that will allow for informed tactical (not medical) decisions when faced with an unknown but possible biological agent. The initial study sponsored by DHS for the "Evaluation of Pre-Screening Technologies" for possible biological agents/threats was completed in 2005.

Additional work has been sponsored by DHS to continue to evaluate the needs of the emergency responder in relationship to handheld assays (HHAs) for anthrax and ricin. The additional work will include a survey for HHA users to garner insightful information on the performance expectations of HHAs from the people using them. Members of the IAB will be included in those being surveyed. Information from the survey will aid in developing performance criteria and study designs with the HHA user in mind.

Chemical Detection

The Chemical Warfare Vapor Detector Standard CWVD has been approved by ASTM and will be available shortly. A certification program associated with this standard is not in place yet.

The Standards Development Program has begun groundwork for a TIC detector. The current efforts include working with the medical community to determine the appropriate detection levels required for various TICs and toxic industrial materials based on their respiratory or dermal toxicity. There currently exists an Underwriters Lab (UL) Gas Detection Standard 2075, which may be very useful but does not require specific detection levels for specific chemicals. Discussions with UL will be required to determine whether and how this standard can be used for the emergency response community.

Radiological Detection

All of the ANSI N42 series of standards and their testing and evaluation protocols were revised in 2006. In addition, a new National Voluntary Laboratory Accreditation Program (NVLAP) was established for the accreditation of laboratories testing radiological equipment used in DHS applications in 2006.

D&D Chairs

James Schwartz

Chief, Arlington County (VA) Fire Department

James Schwartz is Chief of Arlington County (VA) Fire Department, where he has worked for 22 years. He served in a variety of positions before his appointment as Chief, including Assistant Chief of Operations, overseeing all response-related activities—fire, EMS, hazardous materials and technical rescue response, incident management, and operational training. The Arlington County Fire Department's 300+ personnel serve a community of nearly 200,000 residents in a 26–square mile area. It was the lead agency for the response to the September 11 attack at the Pentagon. Chief Schwartz has a B.S. in Fire Administration from the University of Maryland. He chairs the sustainment committee for Arlington County's Metropolitan Medical Response System, a federally funded program that focuses on the integration of a community's response capabilities for a terrorism event. He is also currently Vice Chair for the Washington Area Council of Governments Fire Chiefs Committee. Chief Schwartz is a member of the International Association of Fire Chiefs' Committee on Terrorism and Homeland Security and serves on the Senior Advisory Board for the Responder Knowledge Base.

Elaine Stewart-Craig

Chemical Engineer; Research, Development and Engineering Command
Edgewood Chemical and Biological Center

Elaine Stewart-Craig, a chemical engineer who has worked for ECBC for more than 20 years, is currently Special Projects Group Leader. Her primary duties include the development of chemical and biological standards for commercial equipment to be used by the emergency response community in the event of a terrorist attack. This program, funded by DHS, is a joint effort between ECBC, NIOSH, and NISH. Ms. Stewart-Craig has a B.S. in chemical engineering from the University of Virginia and an M.B.A. from Loyola College. She began her career in personnel protection equipment, designing and producing CB-protective masks and filters for the military, and has been involved with quality assurance, strategic planning, and future business development for ECBC. Ms. Stewart-Craig is a member of ASTM Committee E54, Homeland Security Applications, and has been involved in the area of homeland security/defense since 1995.

Mission

The mission of the Medical SubGroup (MSG) is to provide guidance to the IAB on medical, public health, and incident health and safety equipment, supplies, and pharmaceuticals needed to respond to CBRNE events. This guidance is developed from member experience and discussion of relevant material. In addition, the MSG reviews and makes recommendations to the IAB on needs for new or modified equipment performance and operational standards. The MSG strives to understand and document in the SEL and RKB the generic medical, public health, and incident health and safety equipment, supply, and pharmaceutical capabilities to support responders, first receivers, and volunteers as they prepare for, respond to, and recover from CBRNE events.

Membership

MSG members represent local, state, and federal organizations and academic institutions. They are familiar with local, state, and federal plans, procedures, programs, guidance, functions, systems, and capabilities for public health and medical response. Current members have operational experience with emergency medical systems, primary and emergency medical care, hospital systems and operations, the National Disaster Medical System, disaster medicine and response, public health, law enforcement and special events operations, and emergency management. The MSG attempts to maintain active members who are involved in the public health and medical aspects of incident response and the use of and operational considerations for equipment, supplies, and pharmaceuticals during incident response. The MSG also supports the other IAB SubGroups with public health and medical representatives. The MSG maintains contact with SMEs for assistance with specific topics or areas of interest. SMEs occasionally participate in MSG meetings to expand the breadth of knowledge and resources available to the IAB as a whole.

Role and Functions

The MSG participates in all aspects of the IAB. Due to the diversity of the mission, which includes

Medical SubGroup (MSG)

CO-CHAIR

Tom Walsh
Seattle (WA) Fire Department

FEDERAL CO-CHAIR

Stephen Skowronski
Centers for Disease Control and Prevention

Membership

Knox Andress
Christus Schumpert Health System

Sandy Bogucki
Yale University Emergency Medicine

Kelly Burkholder-Allen
University of Toledo

Richard Burton
Placer County (CA) Health and Human Services

Christian Callsen
Austin-Travis County (TX) Emergency Medical Services

Joshua Creighton
Wake County (NC) Emergency Management

Earl Hall
University of Montana, College of Health Professions and Bio-Medical Science

consideration for and understanding of the care of casualties as well as the health and safety needs of personnel participating in the management of the incident, information exchange with each of the other IAB SubGroups is essential. Specifically, the functions and roles of the MSG include the following:

- Participating in SCC meetings to represent medical, public health, and incident health and safety interests.
- Participating in S&T Committee meetings to promote inclusion of medical, public health, and incident health and safety interests.
- Reviewing, improving, and updating the medical section of the SEL and RKB.
- Reviewing, improving, and updating other sections of the SEL and RKB for integration of medical, public health, and incident health and safety needs.
- Understanding and documenting current and potential gaps and needs in medical, public health, and incident health and safety equipment and supplies.
- Supporting the development of new standards or modification and integration of existing standards that are needed for the medical, public health, and incident health and safety aspects of the response.

The majority of the equipment and pharmaceuticals used in the medical management of victims of a CBRNE event are regulated by the U.S. Food and Drug Administration. Consequently, the compilation of equipment and pharmaceuticals in the medical portion of the SEL is commonly found in today's prehospital and clinical environments. However, the MSG also reviews and recommends for reference, formal adoption, or change other available performance standards, technical specifications, and standard guidance for SEL items.

Accomplishments in 2006

Equipment/Supplies/Pharmaceuticals

In 2006 the MSG considered equipment, supplies, pharmaceuticals, and operational concerns for

Susan Jones-Hard
Mid-America Regional Council

Keith Holtermann
United States Department of Health and Human Services

Paul Maniscalco
National Association of Emergency Medical Technicians

Tim McAndrew
City of Las Vegas (NV) Office of Emergency Management

Kenneth Miller
Orange County (CA) Fire Authority

Peggy Shapiro
Washington State Hospital Association

Tom Skowronski
Phoenix (AZ) Fire Department

Lawrence Tan
New Castle County (DE) Police Department, Emergency Medical Services

Subject Matter Experts

John Ferris
United States Occupational Safety and Health Administration

Stephan Graham
United States Army Center for Health Promotion and Preventive Medicine

Paul Kim
Department of Veterans Affairs

CDR Michael Penny
Chemical Biological Incident Response Force

John Piacentino
United States Occupational Safety and Health Administration

special-needs and vulnerable populations, shelter operations, and medical and public health surge capacity. The following list (grouped by topic) illustrates several publications released in 2006 that include some information on equipment, supplies, and pharmaceuticals.

- Special-Needs and Vulnerable Populations
  - Annotated Bibliography on Emergency Preparedness and Response for People with Disabilities, American Association on Health and Disability, 2006.
  - We Can Do Better: Lessons Learned for Protecting Older Persons in Disaster, American Association of Retired Persons, 2006.
  - "Availability of Pediatric Services and Equipment in Emergency Departments: United States, 2002–03," Advanced Data from Vital and Health Statistics, Number 367, CDC, February 28, 2006.
  - A Disaster Preparedness Plan for Pediatricians, Scott Needle, MD, FAAP, American Academy of Pediatrics, June 2006.
  - Future of Emergency Care Series: Emergency Care for Children, Growing Pains, Institute of Medicine, June 2006.
  - Testimony of Steven Krug, MD, FAAP, on behalf of the American Academy of Pediatrics before the Homeland Security Subcommittee on Emergency Preparedness, Science and Technology regarding "Emergency Care Crisis: A Nation Unprepared for Public Health Disasters", July 26, 2006.
  - Nursing Home Emergency Preparedness and Response During Recent Hurricanes, DHHS Office of the Inspector General, OEI-06-06-00020, August 2006.
  - "Prophylaxis and Treatment of Pregnant Women for Emerging Infections and Bioterrorism Emergencies," Emerging Infectious Diseases, Vol. 12, No. 11, November 2006.
- Shelter Operations
  - Shelter from the Storm: Local Public Health Faces Katrina, Five Hurricane Stories, National Association of County and City Health Official, February 2006.
  - Mega-Shelters Planning and Activation, A Best Practices Guide, Preliminary Release, Phase 1 Document, International Association of Assembly Managers, Inc., May 2006.
- Medical and Public Health Surge Capacity
  - Model Trauma System Planning and Evaluation, Health Resources and Services Administration, February 2006.
  - Guide for Interfacility Patient Transfer, National Highway Traffic Safety Administration, April 2006.
  - Future of Emergency Care Series: Hospital-Based Emergency Care at the Breaking Point, Institute of Medicine, June 2006.
  - Future of Emergency Care Series: Emergency Medical Services at the Crossroads, Institute of Medicine, June 2006.
  - After Katrina, Hospitals in Hurricane Katrina, Challenges Facing Custodian Institutions in a Disaster, The Urban Institute, July 2006.
  - Disaster Preparedness: Limitations in Federal Evacuation Assistance for Health Facilities Should be Addressed, GAO-06-826, July 2006.
  - States of Preparedness: Health Agency Progress 2006, Association of State and Territorial Health Officials.
  - Providing Mass Medical Care with Scarce Resources: A Community Planning Guide, Agency for

Healthcare Research and Quality, AHRQ Publication No. 07-0001, November 2006.

- Pandemic Influenza; Preparedness, Response and Recovery, Guide for Critical Infrastructure and Key Resources, Department of Homeland Security, September 19, 2006.
- The Canadian Pandemic Influenza Plan for the Health Sector, Public Health Agency of Canada, ISBN 0-662-44409-4, 2006

(Note: The MSG is not endorsing or validating the content of any of these publications.)

The MSG sent a representative to the Emergency Preparedness and Response Conference (for People with Disabilities, the Elderly, Pediatrics, and Animals), December 13–14, 2006, Washington, DC.

Training

MSG members took advantage of opportunities to review draft Exercise Evaluation Guides and Target Capabilities provided by DHS.

Operations

MSG members are participating in the review of the OSHA publication Best Practices for Emergency Medical Technicians involved with Homeland Security and WMD.

Initiatives and Progress (2006 and beyond)

After the fall meeting, the MSG began testing the use of a Web-based computer and teleconferencing technology provided by the Health Officers Association of California to provide monthly member updates. The MSG hopes to continue the use of this technology in 2007 to improve communications and accomplishments.

The MSG will continue to focus on the topics listed in the "Accomplishments" section above and will review new publications and other references to improve the SEL.

The first meeting in 2007 will be held in Arlington, Virginia. An extra work day has been approved to meet with representatives from the U.S. Department of Health and Human Services and other agencies to discuss and develop work plans related to the following topics:

- Special-needs and vulnerable populations
- Food and Drug Administration approval process for countermeasures, both biologicals (vaccines) and chemicals
- Health Resources and Services Administration Cooperative Agreement Programs
- National Disaster Medical System transition
- Agricultural terrorism prevention, response, and mitigation equipment

The MSG recommends and supports efforts to provide equipment procurement guidance to public health and medical authorities that is compatible and interoperable with the DHS AEL, RKB, and the IAB SEL.

Medical Chairs

Thomas Walsh

Seattle (WA) Fire Department

Thomas Walsh is currently assigned as Medical Services Officer in the Seattle Fire Department's EMS Division. He has served the citizens of Seattle for 35 years with assignments on engines and ladders and as a firefighter paramedic. He joined the MSG in 1998 shortly after its inception.

Stephen Skowronski

Exercise and Preparedness Coordinator
Centers for Disease Control and Prevention

Steve Skowronski's first career was in the U.S. Army, where he served as a chemical decontamination officer; an aeromedical evacuation rotary wing pilot; a medical plans, operations, and training officer; and a DoD medical liaison to federal health and medical support. He participated in numerous domestic and overseas exercises and operations, including military support to Cuban refugee relocations in 1980 and the response to Hurricane Bertha. Following his military career, Mr. Skowronski worked as the Department of Health and Human Services' Regional Emergency Coordinator in New York City and Boston. In 2000, he began working for the CDC National Pharmaceutical Stockpile Program (currently Strategic National Stockpile) before his current assignment with the National Center for Environmental Health, Environmental Public Health Readiness Branch. Mr. Skowronski has been a member of the MSG since 1999.

Mission

The mission of the Training SubGroup is to improve responder mission performance by conducting a cross-disciplinary review of, and providing end user input on, training doctrine and guidance developed for the responder community.

Membership

The Training SubGroup consists of representatives from local, state, and federal responder agencies and institutions engaged in responder training. A goal of the SubGroup is to engage all of the response disciplines as defined by DHS's Office of G&T. The Training SubGroup also draws upon a wide range of SMEs, both within and outside the IAB.

Roles and Functions

- Focus on the operational applicability of the DHS training doctrine and programs.
- Provide end user guidance and input on training program improvements.
- Facilitate the implementation of training programs that support a capability-based response system.
- Review training requirements for safe and effective operation of grant funded responder equipment.

Initiatives and Progress

The IAB membership and federal partners recognize that, in addition to the core mission of recommending appropriate responder equipment as well as appropriate performance standards for their equipment, a crucial need exists to provide guidance on the training required to effectively and

Training SubGroup (TSG)

CO-CHAIR

Alan "A.D." Vickery
Seattle (WA) Fire Department

FEDERAL CO-CHAIR

Barbara T. Wisniewski Biehn
Department of Homeland Security, Office of Grants and Training

Membership

Ed Allen
Seminole County (FL) Sheriff's Office

Christina Baxter
Douglas County (GA) Fire Department

Richard Callis
Department of Homeland Security, Federal Emergency Management Agency

Terry Cloonan
Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health

Teresa Embrey
Technical Support Working Group

John Ferris
United States Occupational Safety and Health Administration

safely use the equipment. The basis for this guidance is enhancing preparedness capabilities and improving responder performance and safety.

- Reviewed critical tasks and subtasks for applicability to the first responder community.
- Reviewed and provided input to capability-based exercise evaluation guides (EEGs) designed to assist with exercise evaluation by providing evaluators with consistent, operationally valid standards and guidelines for observation, data collection, analysis, and report writing.
- Provided responder input into identifying the training required (federal, state, local, and tribal) to successfully tie performance of tasks to overall capability.
- Provided responder input on how best to achieve improved performance.
- Reviewed and provided input on improvements to capability-based training programs.
- Reviewed and provided input on training programs that strengthen the links between strategies, capabilities, and tasks.
- Initiated a program to link training requirements with equipment recommendations contained in the RKB.
- Initiated a study of minimum core curriculum applicable across response disciplines.
- Provided input to the SCC in the development, adoption, and implementation of appropriate and relevant training standards.

Ongoing Commitments

The Training SubGroup continues to be a "sounding board" for training doctrine and programs. This task is essential in focusing funds and resources on relevant, operationally sound training programs. The Training SubGroup provided valuable feedback for refining the DHS Universal Task List and Target Capabilities List and also provided recommendations for improvements in the development of operationally valid Exercise Evaluation Guides. As these efforts evolve, the Training SubGroup will remain engaged to provide input on training implications for the operational community.

Paul Hauptman
Sacramento (CA) Sheriff's Office

Gregory Noll
South Central Pennsylvania Counter-Terrorism Task Force

Ronald Olin
Lawrence (KS) Police Department

Steve Souder
Montgomery County (MD) Communications Center

Jamie D. Turner, III
Delaware Emergency Management Agency

Roy Waugh
University of Washington

Subject Matter Expert

Kevin Johnson
Federal Bureau of Investigation, Hazardous Materials Response Unit

Ted Miller
National Guard Bureau, Operations

John Piacentino
United States Occupational Safety and Health Administration

Priorities of 2007–2008

- Review and provide input on improvements to existing DHS training doctrine and programs.
- Review existing training programs for relevance to Homeland Security Presidential Directive-8.
- Match training requirements to responder equipment.
- Provide input on the development, adoption, and implementation of appropriate and relevant training standards and requirements.

Future Initiatives

The process of providing advice on relevant and successful responder-focused training programs is an ongoing process, driven by technology, threat, capability, and personnel. The Training SubGroup will identify and prioritize training requirements based on these factors.

In future editions of the SEL, the Training Subgroup will work with the respective SubGroups to identify each individual item as having a minimal, moderate, or extensive training requirement based on initial and sustainment training required to operate the equipment. As part of this effort, the Training Subgroup will work to identify recommended training baselines by equipment category.

The Training SubGroup will work closely with the SCC to identify standards where they exist and identify their application to capability-based training. Where standards do not exist, the SubGroup will advocate, through the IAB, for their establishment.

Summary

Equipment is only as good as those trained to use it effectively and safely. The IAB has tasked the Training SubGroup with providing input on a national level on how best to train the responder community to address their daily responsibilities as well as catastrophic events.

Training Considerations for Equipment Purchases

The IAB Training Subgroup strongly recommends that any equipment purchased include identification of initial and sustainment requirements for competency-based training on the calibration, operation, and maintenance of the equipment.

In considering the total cost for equipment purchases, responders should evaluate:

1. the initial cost of the equipment itself and yearly maintenance costs
2. the cost for providing responders initial training on operational use and maintenance of the equipment
3. life-cycle costs associated with sustainment training for the expected life of the equipment

Initial training is defined as the training required for a responder competent in a specialization to achieve competency-based knowledge, skills, and abilities beyond day-to-day duties (e.g. competency based training for new detection equipment reflects operation of that detector by a certified HazMat technician, similarly use of a laser range finder reflects its employment by a certified law enforcement officer just as use of a specialized robot to disable a potential improvised explosive device is based on employment by certified bomb squad technician).

Sustainment training is defined as training required to maintain competency-based knowledge, skills, and abilities.

In future editions of the SEL, the Training Subgroup will work with the respective subgroups to identify each individual item as having a minimal, moderate, or extensive training requirement based on initial and sustainment training required to operate the equipment.

The IAB Training Subgroup recommends that organizations purchasing or developing training require that it adhere to the principles of instructional systems design and best practices for adult learning. Instructional systems design, also called a systems approach to training, applies a series of logical steps to ensure the development and delivery of consistent, quality training to meet operational needs. It consists of:

- Analysis to determine what knowledge, skills, and or abilities (KSA) are required in the operational environment
- Design of curriculum into a program of instruction using terminal and enabling objectives to provide those KSA
- Development of curriculum using various educational approaches and delivery methods appropriate for different audiences and circumstances
- Implementation of training using one or more delivery methods appropriate to the audience
- Evaluation of the effectiveness of the training in developing the desired KSA.

Training Chairs

Alan Dennis Vickery

Assistant Chief of Operations
Seattle (WA) Fire Department

A.D. Vickery, a 39-year veteran of the Seattle Fire Department, is currently the Assistant Chief of Operations, dealing with all aspects of the department in regards to fires, hazardous materials, emergency medical services, special operations, and homeland security. He was previously Deputy Chief of Special Operations, responsible for all operational issues for the department's specialty teams—the Hazardous Materials Unit, the Marine Firefighting Unit, the Technical Rescue Unit, Emergency Preparedness, Metropolitan Medical Strike Team, Urban Search and Rescue, and Homeland Security Planning. Assistant Chief Vickery has served as a Firefighter/Paramedic, the head of the Fire Investigation Unit, and on both Engine and Ladder Companies. He is recognized for his proactive role in preparing firefighters to safely perform their jobs using the latest technology available.

Barbara T. Wisniewski Biehn

Deputy Director, Exercise and Training Division
Department of Homeland Security,
Office of Grants and Training

Barbara Biehn has been an advocate for consistent, high-quality training for operational communities throughout her tenure with the federal government. She began her career as an intelligence officer in the U.S. Air Force preparing fighter pilots against likely threats and completed multiple deployments in southwest Asia. Ms. Biehn also served as a training project director in support of the DoD National Guard Civil Support Teams. For the past six years, as part of G&T before and after its incorporation into DHS from the Department of Justice, she has held various training and management positions including Deputy Director of the Training and Exercise Division. Ms. Biehn's background includes an M.S. in strategic intelligence studies from the Joint Military Intelligence College, where her thesis focused on Algerian political terrorism and terrorist decision-making models.

Strategic Plan

The "Strategic Plan for Developing a Suite of Chemical, Biological, Radiological, Nuclear, and Explosives Protective Equipment Standards" is currently being revised to reflect the all-hazards scope of the IAB and to incorporate other changes, as well. The revised version of the Strategic Plan will be available on the IAB website after approval by the IAB membership, and will be published in the 2007 Annual Report.

Executive Summary

A common suite of first responder equipment standards is needed to establish minimum performance and interoperability requirements for chemical, biological, radiological, nuclear, and explosives (CBRNE) equipment utilized by local, state, and federal first responders to acts of terrorism and CBRNE incidents. Such standards, and the associated requirements and test protocols, serve multiple purposes, including (1) establishing baseline capabilities and limitations for currently available equipment, (2) guiding production and technological developments by manufacturers and designers, and (3) guiding equipment procurement decisions by the public safety and health communities. This document presents the strategy and process within the InterAgency Board (IAB) for Equipment Standardization and Interoperability for identifying, adopting, modifying, and developing CBRNE equipment standards. The priorities for developing standards will be established and periodically reviewed by the IAB Standards Coordination Committee (SCC). It does not address the specifics of schedules, resources, or those standardization processes that are agency and organization specific. It is relevant to note that no such suite of CBRNE equipment standards exists today, and it is a goal of the IAB to remedy this shortcoming.

This CBRNE Equipment Standards process will be accomplished through two phases a "Preparation Phase" and an "Implementation Phase." During the Preparation Phase, requirements for standards will be identified from local, state, and federal first responder functional and operational equipment requirements. These equipment requirements will be compared with existing standards to determine whether existing standards can be adopted into the CBRNE Equipment Standards Suite, modifications are required, or gaps exist requiring new standards to be developed. During the Implementation Phase, the recommendations of the equipment SubGroups will be coordinated with appropriate standards organizations to facilitate adoption, modification, and development of standards for incorporation into the CBRNE Equipment Standards Suite. Gaps in standards will be presented to sponsoring agencies and organizations for new standards development. A review process will be established and managed by the SCC to periodically validate the suite and all incorporated standards.

The National Institute of Standards and Technology, Office of Law Enforcement Standards (NIST/OLES), as the executive agent for the SCC, will implement and administer the CBRNE Equipment Standards Suite repository, to include promulgation where appropriate. Implementation of this suite of standards is expected to be a multi-year process. In the interim, to address the user communities' needs for CBRNE equipment information, NIST/OLES, on behalf of the SCC, will publish and administer a first responder equipment set of guides to assist first responder agencies in making informed procurement decisions.

The Strategic Plan for Developing a Suite of CBRNE Protective Equipment Standards

1.0 Purpose

A common suite of CBRNE equipment standards is necessary to ensure compliance with minimum requirements for performance, commonality, and interoperability of equipment utilized by local, state, and federal first responders in the public safety and health communities. Such standards, as well as the specifications and test protocols that evolve from them, are needed to guide the efforts of the manufacturers and equipment developers and to serve as a guide for informed procurement decisions by criminal justice, medical/public health, and public safety agencies. The phrase "public safety and health communities" includes law enforcement, fire fighter, HAZMAT, emergency medical, and other related agencies that consist of the first elements to respond to public safety CBRNE incidents or attacks and also pertains to organizations that are involved in the mitigation and recovery phases of such attacks. This document describes the strategy and process that the CBRNE Equipment Standards Project will take to develop that common CBRNE Equipment Standards Suite. This document further serves as the action plan for the CBRNE Equipment Standards Project and identifies the tasks that must be undertaken, and the organizations responsible for undertaking them, to implement a CBRNE Equipment Standards Suite. It does not address the specifics of schedules, resources, or those standardization processes that are agency specific. Those remain to be developed within the context of this strategic plan. The IAB SCC will establish the prioritized order for developing or adopting standards and will periodically review and revise the prioritization as requirements change or as standards are implemented.

2.0 Goals and Objective

2.1 ***Goal of the CBRNE Equipment Standards Project*** -The goal is to enhance public safety and health by defining and promulgating a set of standards for CBRNE equipment that ensures minimum performance, quality, and reliability and that are accepted by public safety and health communities. This suite of standards will be disseminated to the local, state, and federal public safety and health communities to facilitate informed equipment procurement and to guide manufacturers, developers, and the test-and-evaluation community to ensure product compliance.

2.2 ***Objective of the CBRNE Equipment Standards Project*** - The objective is to facilitate the adoption of standards that can be used by local, state, and federal public safety and health communities. To accomplish this, strong working relationships must be established with the public safety and health communities, to the point where the communities' representatives play a key and integral role in all facets of the standards process. Further, the project must be oriented, to the maximum extent possible, toward using the approaches, standards, specifications, etc., that already exist within standards development organizations (SDOs), standards-related organizations (SROs), and standards enforcement organizations (SEOs). This project will not reinvent work previously done or provide redundant products, but rather will take advantage of all available information and standards that may be applicable. This project will conform to the regulatory statutes and guidance governing the SDOs, SROs, and SEOs, as applicable.

3.0 Overview of the CBRNE Equipment Standards Suite Development Process

The standards development process consists of two distinct phases - the "Preparation Phase" and the "Implementation Phase." During the Preparation Phase, functional requirements are defined and existing standards are surveyed to determine whether they address these requirements. During the Implementation Phase, gaps in the existing standards will be addressed. Additionally, because the implementation of this suite of standards is necessarily a time-consuming process, some interim steps will need to be taken to provide manufacturers, developers, and procurement officials guidance upon which they can act now.

3.1 ***Preparation*** - During the Preparation Phase, requirements for standards will be identified by determining the first responder functional equipment requirements and comparing those requirements against existing standards to see (1) if existing standards can be adopted into the CBRNE Equipment Standards Suite (2) if they need to be modified before being adopted, or (3) if new standards need to be developed. Functional requirements are derived in equal measure from an assessment of the threat(s) with which first responders will have to deal and the operational practices and procedures (i.e., how they do business) that they will bring to bear to deal with that threat. Users will be involved in every stage of this process, providing initial input and feedback on final products.

3.1.1 *Identification of the Threat* - The first step in the standards development process will be to do a threat assessment to identify the particular agents that are likely to be encountered in a CBRNE terrorism situation, the scenarios in which these agents are likely to be used by terrorists, and the likely methods of agent delivery in a civilian environment. Since the best information is likely to be held by national security organizations and will most likely be classified, it will, of necessity, be restricted to a limited number of people who have the proper security clearances. The second step of the threat assessment will involve situations where simulated releases can be conducted, using simulants, to develop the appropriate "models" and response methods, while working with trained public safety and medical teams.

3.1.2 *Identification of Operational Requirements* - This step involves collection of detailed information regarding the functional and operational requirements of CBRNE equipment based on user needs, practices, and procedures (i.e., how they go about their business). While identification of the threat defines the nature of the agent(s) and the design parameters for a self-contained breathing apparatus, for example, practices and procedures will define the size and weight of that apparatus, how long it needs to function, and how (and if) it needs to be decontaminated. The information will be summarized and catalogued by equipment type.

3.1.3 *Survey and Assessment of Existing Standards*

3.1.3.1 Existing standards relevant to CBRNE equipment will be surveyed to identify any that can be used without any modification, as well as those that can be used with some modification. The SCC will develop a review and approval procedure for both adoption and modification of existing standards. That procedure must take into account the agency-specific requirements and procedures of organizations currently involved in the development of standards.

3.1.3.2 In instances where the SCC review of existing standards has determined that a particular standard(s) not be adopted in whole or in part, it shall issue a report to the IAB, documenting the limitations and/or shortcomings of the existing standard(s).

3.1.3.3 Recommendations for adoption, modification and adoption, as well as the identification of new standards to be developed, will be recorded for action during the Implementation Phase.

3.1.3.4 Implementation - During the Implementation Phase, recommendations resulting from the Preparation Phase will be carried out through coordination with appropriate SDOs, SROs, and SEOs to facilitate adoption, modification, and development of standards for incorporation into the CBRNE Equipment Standards Suite. A periodic review process to validate the suite, and the standards incorporated into it, will also be implemented.

3.2 *Adoption of Existing Standards* - Standards that require no modification will be added "as is" to the CBRNE Equipment Standards Suite. The adoption and inclusion of a standard into the suite will follow the review and approval process as developed by the SCC. Cognizant SDOs, SROs, and SEOs will be notified. These standards will be disseminated to the local, state, and federal public safety and health communities and to manufacturers, developers, and the test-and-evaluation community.

3.2.1 *Modification of Existing Standards* - If the SCC determines that an existing standard needs to be modified before it can be used, the review process and a discussion of the limitations shall be documented. Modification to standards will be coordinated with the cognizant SDOs, SROs, and SEOs for implementation. In cases where existing standards are not able to be modified to meet the specific needs of the IAB, a new standard will be developed as discussed in paragraph 3.2.2. These modified standards will be disseminated to the local, state, and federal public safety and health communities and to manufacturers, developers, and the test-and-evaluation community.

3.2.2 *Development of New Standards* - This type of document will need the most time and resources to develop, as well as the most extensive review process to ensure consensus. Where applicable, the need for new standards will be coordinated with the cognizant SDOs, SROs, and SEOs for development. If the appropriate SDOs, SROs, and/or SEOs cannot be convinced to modify a standard, or if no cognizant SDO/SRO/SEO can be found to develop a new standard, the identified requirement will be addressed through the issuance of a voluntary standard(s). These standards will be issued as National Institute of Justice (NIJ) standards. These standards will be disseminated to the local, state, and federal public safety and health communities and to manufacturers, developers, and the test-and-evaluation community.

3.2.3 *Methodology for Reviewing Standards* - A process will be put in place so that, on a biannual, periodic basis, the standards included in the CBRNE Equipment Standards Suite will be reviewed in light of evolving threats, evolving technologies, user practices, and user procedures to:

- Reaffirm still useful standards and disseminate that information to the local, state, and federal public safety and health communities and to manufacturers, developers, and the test and evaluation community.
- Recall obsolete standards once a review finds a document obsolete; and disseminate that information to the local, state, and federal public safety and health communities and to manufacturers, developers, and the test-and-evaluation community.
- Provide notification when any standards incorporated into the CBRNE Equipment Standards Suite are updated, modified, revised, replaced, or superseded by the SDO or SRO and when exceptions or waivers are granted by SEOs.

3.3 *Interim Steps* - A first responder equipment compendium and set of guides will be developed and published to assist first responder agencies in making informed procurement decisions prior to the implementation of a CBRNE Equipment Standards Suite. These documents will catalogue existing CBRNE equipment and their characteristics and contain test data where found. Of necessity, interim voluntary standards and/or comparative evaluation protocols for testing of CBRNE equipment will also be developed and implemented for selected categories of equipment and threats.

4.0 Organization and Responsibilities

4.1 The key organizations within the IAB that facilitate the development of the CBRNE Equipment Standards Suite are the equipment SubGroups and the Standards Coordination Committee. The equipment SubGroups take the lead for developing the functional requirements for equipment in their commodity areas, in close collaboration with the user community. They also identify and recommend to the SCC existing standards for direct incorporation into the CBRNE Equipment Standards Suite, standards that could be incorporated with modification, and new standards that need to be developed. The SCC, which includes the Chairs of the equipment SubGroups, will manage this process and will be principally responsible for implementation and management of the suite.

4.2 *Standards Coordination Committee (SCC)*

4.2.1 The SCC consists of a panel of representatives from various federal and private standards organizations, the Co-Chairs of the equipment SubGroups, and the Co-Chairs of the Science and Technology Committee. The SCC is responsible for coordinating CBRNE equipment standards projects of the IAB SubGroups with other organizations and enforcing authorities including, but not limited to, National Institute for Occupational Safety and Health (NIOSH), National Fire Protection Association (NFPA), Occupational Safety and Health Administration (OSHA), NIJ, Department of Energy (DOE), Federal Emergency Management Agency (FEMA), Environmental Protection Agency (EPA), and the NIST/OLES. As the various equipment SubGroups of the IAB determine minimum performance, quality, reliability, and other qualification requirements for their respective commodities, the SCC, representing regulatory, consensus, and voluntary standards organizations, will endeavor to create national harmonization by incorporating the requirements into its standards. The SCC will also serve as a reviewer during the development of qualification requirements by other SubGroups to:

- Alert SubGroups and request reconciliation when contradictory requirements for complementary equipment are proposed.
- Alert SubGroups when proposed requirements are contradictory to federal or state regulations.
- Raise attention to similar or additional qualification requirements under internal development within the regulatory, consensus, and voluntary standards organizations.
- Provide technical and non-technical advice for improvements.

4.2.2 In the absence of appropriate standards for equipment deployed by emergency responders, the SubGroup members will serve as liaisons to their respective organizations to encourage development and harmonization of standards. NIST/OLES, as the executive agent for the SCC, will implement and administer the CBRNE Equipment Standards Suite, to include promulgation.

4.3 ***Equipment SubGroup*** - There are four equipment SubGroups established by the IAB. These SubGroups are composed of subject matter experts who address domestic preparedness equipment, systems, and protection issues related to a specific commodity area. The four equipment SubGroups are (1) the Medical SubGroup, (2) the Personal Protective and Operational Equipment SubGroup, (3) the Detection and Decontamination SubGroup, and (4) the Interoperable Communications and Information Systems SubGroup. Each SubGroup has two Co-Chairs, one from the ranks of the SubGroup's local and state ranks and the second from federal or private ranks. The role of each SubGroup is to maintain and update its portion of the Standardized Equipment List and to address the ways and means by which technology can support CBRNE response concerns. Additionally, the SubGroups take the lead for developing the functional requirements for equipment, and identify and develop priorities for standards development within their respective commodity areas. The SubGroups identify existing standards that may be incorporated into the CBRNE Equipment Standards Suite without change, identify standards that may be incorporated into the suite after modification, and recommend areas for development of standards where none currently exist.

4.4 ***The Science and Technology Committee (S&T)*** - The mission of the S&T is to identify interagency (local, state, and federal) first responder research and development (R&D) requirements and innovative technologies (fieldable in the next 6 months to 5 years) that address CBRNE detection, individual and collective protection, medical support, decontamination, communications systems, information technology, and miscellaneous operational support. The S&T consists of subject matter experts in the R&D field, the Co-Chairs of the equipment SubGroups, and the Co-Chairs of the SCC.

5.0 Execution

5.1 The CBRNE Equipment Standards Suite will be developed, promulgated, and administered as outlined above. The work will be conducted during regularly scheduled meetings of the IAB, and specially convened SubGroup sessions and by members of the SubGroups as directed by the SubGroup Chairs.

5.2 ***Standards Coordination Committee*** - The SCC will solicit input from the equipment SubGroup(s), consolidate input, and develop priorities for subsequent efforts, as outline in section 3.0. The SCC will develop, maintain, and publish the list of IAB adopted CBRNE protective equipment standards and develop a schedule for periodic review of these standards.

5.3 ***Equipment SubGroups*** - The equipment SubGroups will perform the steps outlined in section 3.0 according to a schedule developed by the Standards Coordination Committee.

5.4 ***NIST/OLES*** - The NIST/OLES serves as the executive agent for the SCC and implements, administers, and promulgates the CBRNE Equipment Standards Suite repository as appropriate. Additionally, NIST/OLES will publish, administer, and maintain a set of first responder CBRNE equipment guides. These guides will catalogue existing CBRNE equipment and their characteristics and will contain test data where available.

Acronym List

AEL	Authorized Equipment List
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials-International, Inc
ATSD(NCB)	Assistant to the Secretary of Defense (for Nuclear and Chemical and Biological Defense Programs
CAD	Computer-aided Dispatching
CB	Chemical and Biological
CBDP	Chemical Biological Defense Program
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CDC	Centers for Disease Control
CFR	Code of Federal Regulations
CIC	Compatibility and Interoperability Committee
CIT	Capabilities Implementation Team
CWA	Chemical Warfare Agents
D&D	Detection and Decontamination SubGroup
DHS	Department of Homeland Security
ECBC	Edgewood Chemical Biological Center
EEG	Exercise Evaluation Guide
EMS	Emergency Medical Services
FACC	Federal Agency Coordinating Committee
FDNY	New York City Fire Department
FEMA	Federal Emergency Management Agency
G&T	Department of Homeland Security, Preparedness Directorate Office of Grants and Training
HHA	Handheld Assay
IAB	Interagency Board
IACP	International Association of Chiefs of Police
IAFF	International Association of Fire Fighters
ICIS	Interoperable Communications and Information Systems SubGroup
JPEO-CBD	Joint Program Executive Office for Chemical and Biological Defense
KSA	Knowledge, skills, and/or abilities
LRN	Leader in governance, ethics and compliance management
MSG	Medical SubGroup
NFPA	National Fire Protection Association
NIEM	National Information Exchange Model

NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology
NPPTL	National Personal Protective Technology Laboratory
OLES	Office of Law Enforcement Standards
PPE	Personal Protective Equipment
PP&OE	Personal Protective and Operational Equipment SubGroup
PPT	Personal Protective Technology
RDECOM	Research, Development and Engineering Command
RDT&E	Research, Development, Test and Evaluation
RKB	Responder Knowledge Base
RMS	Record Management Systems
SAR	Specific Absorption Rate
SCBA	Self Contained Breathing Apparatus
SCC	Standards Coordination Committee
SEL	Standardized Equipment List
SME	Subject Matter Experts
S&T	Science and Technology Committee
TCL	Target Capability List
TEW	Total Extreme Warfare
TIC	Toxic Industrial Chemical
TSG	Training SubGroup
TSWG	Technical Support Working Group
WMD	Weapons of Mass Destruction

Special Thanks

The InterAgency Board would like to extend special recognition to the National Memorial Institute for the Prevention of Terrorism (MIPT) and the Responder Knowledge Base team. Their work played a key role in the development of the 2007 Standardized Equipment List. Particular accolades go to Don Hewitt and his staff for their dedication and commitment to this project.

The 2007 Standardized Equipment List (SEL)