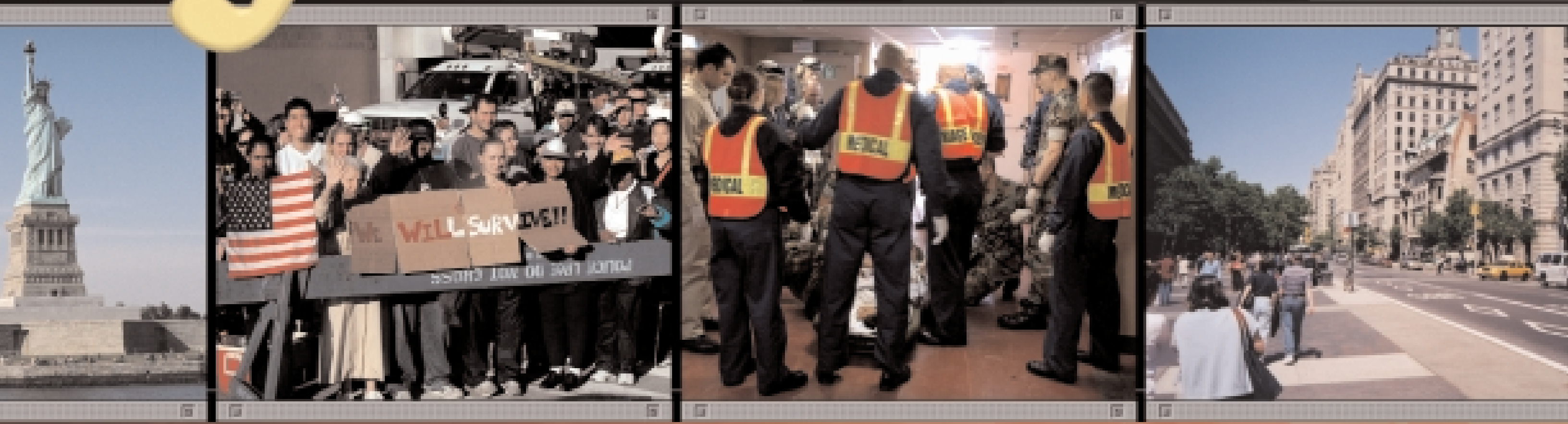
Defense Standardization Program

Journal

July/September 2003



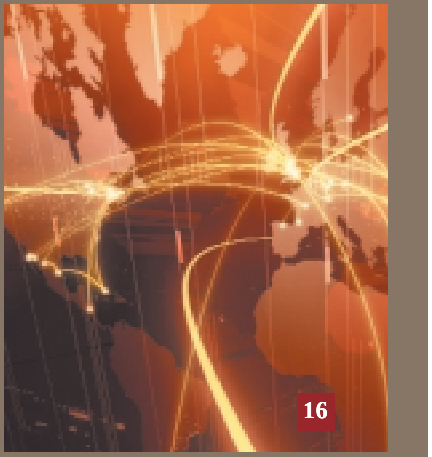
Homeland Security

SEVERE
SEVERE RISK OF TERRORIST ATTACKS
HIGH
HIGH RISK OF TERRORIST ATTACKS
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
GUARDED
GENERAL RISK OF TERRORIST ATTACKS
LOW
LOW RISK OF TERRORIST ATTACKS
THE GREAT SEAL OF THE UNITED STATES OF AMERICA

Defense Standardization Program
Journal

Contents *July/September 2003*

Departments



16

20

Front cover: New Yorkers on 9/14/01, White House photo by Paul Morse; medical personnel on USNS Comfort *courtesy Department of Defense. Back cover: Tactical Operations monitoring surface and aerial contacts courtesy Department of Defense.*

Gregory E. Saunders
Director, Defense Standardization Program Office

Sharon Strickland
Editor, Defense Standardization Program Journal
sharon.strickland@dla.mil

Defense Standardization Program Office
8725 John J. Kingman Road
Stop 6233
Fort Belvoir, VA 22060-6221

703-767-6874
Fax 703-767-6876

dsp.dla.mil

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published three times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to *DSP Journal*, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to sharon.strickland@dla.mil
floppy disk (Windows format) to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Homeland Security… A National Imperative That Involves Us All

Where were you when our world changed? December 7, 1941, and September 11, 2001, are two days of infamy marked by surprise attacks, loss of American lives, and a fundamental shift in how we viewed national security and America's role in the world. The dramatic events on those two days transformed America from a nation at peace to a nation at war. On both occasions, we responded by carrying the fight to the enemy and by strengthening our security at home. Those alive and old enough to remember will never forget.

During the post-Cold War period, joint and coalition operations are increasingly important in the defense of freedom and protection of our national interests. Throughout its 50-year history, the Defense Standardization Program has played a vital role in containing acquisition and logistics costs and improving the interoperability of America's military forces and those of our allies. Yet, in every new conflict, we encounter new areas where standardization can help solve interoperability problems.

September 11, 2001, added an entirely new dimension to our understanding of the need for interoperability and the role of standardization in securing our homeland. Before September 11, we thought about interoperability almost exclusively in terms of joint and coalition warfare. The DSP was committed to serving our military forces with the highest quality standardization products and services. Standardization for interoperability within our homeland infrastructure was not even on the radar screen.

Just as the attack on Pearl Harbor and the subsequent war led to the birth of the DSP and the long march of standardization in the military domain, the September 11 attacks on the World Trade Center towers and on the Pentagon gave birth to the Department of Homeland Security

Gregory E. Saunders
Director, Defense Standardization Program Office

(DHS) and the start of standardization for interoperability within the homeland domain. The task is huge, affecting almost every aspect of our national infrastructure from the federal to the local level.

The United States already spends roughly $100 billion per year on homeland security. This includes the services of federal, state, and local law enforcement and emergency services but excludes most spending for the armed forces. Homeland security is an enormous undertaking that will involve thousands of government, private-sector, and international standards, spanning myriad disciplines. The task of developing, understanding, coordinating, maintaining, and distributing those standards may be equal to or even greater than that of the Defense Standardization Program.

Development and production of the devices and systems needed for homeland security will require standards for homeland security technology. Standardization is a critical element in ensuring compatibility between and among systems and equipment. Information and materiel technologies must be compatible and interoperable if we are to operate on a national or global scale to prevent or respond to terrorism or to a catastrophic event.

It's sometimes said that in the modern world, the parents of standards are war and catastrophe, meaning that it often takes a disaster before the public demands solutions, which typically take the form of standards, to prevent or lessen similar disasters in the future. Fire safety codes, the boiler and pressure vessel code, environmental standards, and many others were all born from disasters. The events of September 11 no doubt will prove to be the parents of many new standards. Our challenge in the standards community is to ensure that those new standards are the "right" standards that will best address our most critical needs. It's a daunting task to address different needs at the local, state, national, and even global level, and there is no single path to follow. The one thing that is certain, though, is that we will succeed only if we communicate about needs, priorities, and ongoing efforts, which is why we dedicate this issue to homeland security, a topic that is, and will continue to be, an integral part of our contribution to national security.

Interoperability and Standardization for National Homeland Security

Four Keys to Success

By Richard Jackson and Brian Mansir

Interoperability and standardization will be integral to the success of the homeland security process.

Workers at World Trade Center site chanting their support in September 2001.

White House photo by Paul Morse

Where should we focus our efforts to improve the national homeland security posture? The threats are many, our challenge is large, and our needs to improve are widespread. The nation must simultaneously control its borders, protect its national infrastructure, gather and share intelligence about potential adversaries, strengthen its capabilities to prevent hostile events, and improve its ability to respond to events when they happen. Each of these responsibilities requires a unified effort from multiple federal, state, and local governmental organizations. In some cases, assistance from nongovernmental organizations and private industry is critical. To succeed, these diverse organizations must be able to effectively share information and services, and this will not occur automatically or "by magic." An effective national homeland security program requires a well-thought-out approach to interoperability and standardization to make sure that we make the best use of our resources and provide the best possible protection for our citizens. This article outlines the importance of interoperability and standardization to our homeland security capability, and it identifies four keys to success for an effective homeland security interoperability and standardization program.

The Importance of Interoperability and Standardization

The nation will face many challenges in the months and years ahead as we strengthen our homeland security capabilities. The new Department of Homeland Security (DHS) must simultaneously lead the national effort to improve homeland security preparedness and create a single agency of more than 170,000 personnel capable of efficiently managing and executing its homeland security missions. Integrating the people and functions drawn from 22 different federal organizations into a single cohesive unit will require a major standardization effort just to enable internal interoperability, seamless communications, and efficient data sharing.

The interoperability challenge is not limited to DHS. Homeland security involves us all, from our national government, to state and local governments, to private-sector organizations and individuals. Homeland security will also involve our international allies. Interoperability and standardization will play an important role at every level in this vast homeland security network.

The day after the Pentagon attack, firefighters drape an American flag on the building.

White House photo by Paul Morse

We must carefully choose our priorities and focus our efforts to quickly, effectively, and efficiently close the gaps in our capabilities and in our abilities to work together in our common purpose. Interoperability and standardization are key enablers for many critical homeland security actions. As such, the establishment of an effective, comprehensive interoperability and standardization program should be an early priority for DHS.

Why is interoperability and standardization so important to homeland security? We do not have the resources to provide every possible capability to every level of jurisdiction throughout the nation. Instead, our strategy is, of necessity, one of focused reinforcement. Our communities have a cadre of first responders and other "on-the-ground" personnel with the training and equipment necessary to meet day-to-day requirements and common contingencies. During times of increased threat and in response to incidents, the "in-place" organizations are augmented by additional personnel and capabilities. This doctrine of reinforcement requires that certain levels of training and equipment be standardized and uniform among our first responders. The ultimate goal should be a national "plug-and-play" capability that allows us to increase preparedness and response levels seamlessly and effectively.

The character of the homeland security threat also requires us to achieve interoperability. Those who would attack our nation are clever adversaries who will study our capabilities and look for weaknesses and gaps. Terrorists will exploit our lack of communications, our gaps in information sharing, and similar vulnerabilities. Effective interoperability will reduce our vulnerabilities and maximize our capability to deter, detect, prevent, and respond to threats.

Interoperability is not solely an equipment issue. Interoperability and standardization for homeland security includes the capabilities needed to share both information and services, when needed and where needed. It certainly involves critical equipment and infrastructure issues, like communications and detection devices, but it goes far beyond those critical components. Interoperability must be built in to the process, rather than trying to add it on later. This will require a common language and a certain level of common operating concepts. Interoperability and standardization do not mean that everyone must have the same equipment and same procedures. "One size" clearly does not fit all in this business. The challenge will be to set meaningful high-level policies and standards that provide the needed capabilities—and not to seek "lowest common denominator" solutions that further burden already overtaxed state and local governments.

> **"Smart containers"... provide assurance about their contents and integrity from point of origin to point of destination. Such a capability requires international standards...**

One example of the broad interoperability challenge is in border and transportation security. Tens of thousands of shipping containers arrive on our shores every day from every port around the world. For the most part, we have little real intelligence about what is in those containers. Although significant progress has been made, the lack of specific, verifiable information about the contents of containers presents our nation with a significant vulnerability. Gaining information about the contents requires the cooperation of multiple governments and commercial entities. The end-to-end shipping process can involve up to 20 commercial and governmental parties, use more than 200 data elements, and require some 30 documents or messages. One possible solution may be to use "smart containers" that provide assurance about their contents and integrity from point of origin to point of destination. Such a capability will require international standards for the technology, the processes and procedures, and the relationships among the participating nations and commercial shippers. And this solution must apply to each location in the world where containers may be loaded. Clearly, the solution is not trivial, but standardization is essential.

The Homeland Security Coalition

DHS, which combines 22 federal agencies, will play a lead role in defining the interoperability and standardization requirements needed to move the nation toward a national plug-and-play capability. However, DHS cannot achieve the goal on its own. Achieving the needed levels of interoperability will require a coalition effort. The coalition must include some 20 other federal agencies that still have significant homeland security responsibilities (such as DoD and the National Institute of Standards and Technology).[1]

The homeland security coalition must also include state and local governments, industry, and other nongovernmental organizations (for example, professional associations and private volunteer organizations such as the American Red Cross). State and local governments have a large role in preparing for and recovering from emergencies. And they have the primary responsibility for responding to emergencies with police, firefighting, and emergency medical personnel. In fact, as specified in The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-228), federal assistance during emergencies may be provided only when conditions are beyond the state and local capability to respond.

The roles of industry and other nongovernmental organizations also are important. Industry, for example, produces the equipment used when responding to an emergency, so is an important partner in realizing interoperability and standardization. The federal government and industry must work together. The federal government can have a significant influence on products for which it is the primary customer. Equipment to protect against biological or chemical weapons is an example of such products. The government may have less influence in other areas. In the segments of the communications industry that are dominated by nongovernmental customers, for example, the government will need to leverage industry standards and protocols.

Each coalition member can contribute to or provide standards, training, and in some cases, operational capabilities within their areas of expertise. Existing capabilities may be leveraged and expanded to meet homeland security needs. For example, within DoD, the Defense Standardization Program (DSP), the major provider of defense-related standards and specifications, has much to contribute toward achieving the national requirement for homeland security interoperability and standardization. DSP maintains an Acquisition Streamlining and Standardization Information System (ASSIST) database of more than 30,000 standardization documents, including the international standardization agreements that form the heart of our ability to interoperate with our allies. Many of these DSP standardization documents may be solutions to homeland security interoperability requirements. ASSIST is a national ready resource capable of holding, managing, and making available to all authorized users the standards that will enable and define the homeland security capability. The ASSIST capability is online now. It stands ready to contribute to accomplishing the homeland security mission.

New Yorkers offer their own words of determination on 9/14/01.

White House photo by Paul Morse

Four Keys to Success

Interoperability and standardization will be an important element of the homeland security coalition's success. Achieving interoperability and standardization will require a top-down process, led by DHS and involving all key stakeholders. Four actions will be key:

- Establish a common language among all of the stakeholders

- Develop a common operational architecture for preparedness and response capabilities
- Provide a comprehensive set of national training standards
- Implement a centralized program to develop, manage, and maintain equipment and technical standards, including testing protocols.

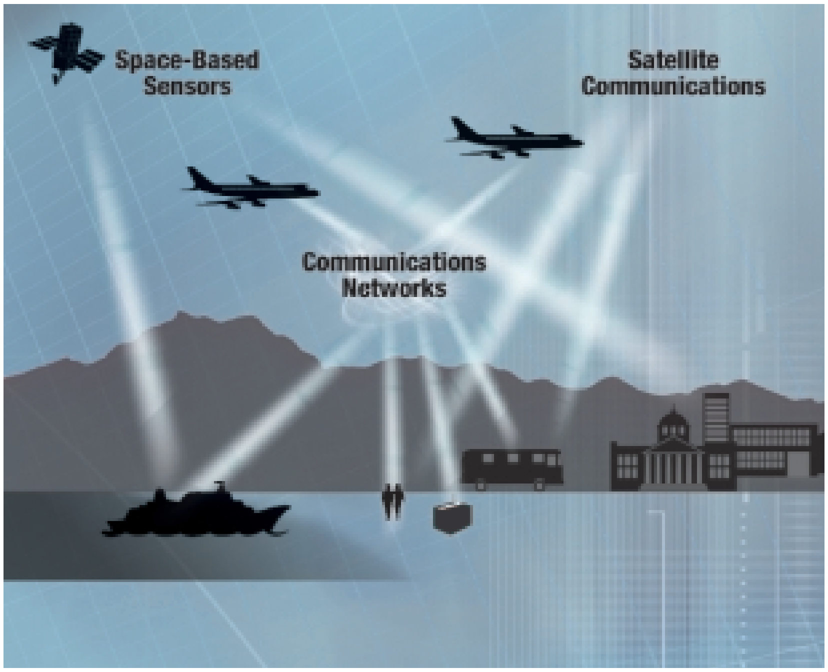
A COMMON LANGUAGE

A common language may seem like a trivial matter, but it is a crucial foundation for other interoperability and standardization measures. The homeland security coalition consists of many communities, and each speaks its own "language." Different groups may use different terms and definitions for procedures and equipment that are essentially the same. We need to use operational and technical terms consistently to ensure clarity and precision during operations involving different organizations. The use of common terminology also will support other efforts, such as planning and architecture development.

THE "WHY" AND "WHAT" OF OPERATIONAL ARCHITECTURES

The national homeland security capability will take decades to build. And because we must build this capability a piece at a time, we must have a plan. An operational architecture plan or "blueprint" is the enabler for a national plug-and-play capability. This top-down framework will give structure to the rest of this complex process.

An operational architecture can be defined as a standards-based "picture" that describes the capabilities in a complex process and the interrelationships among capabilities.[2] An operational architecture can be



- designed to reflect doctrine and assigned tasks and activities,
- designed to represent activities that cross organizational boundaries,
- written in non-system-specific terms,
- independent of specific organizations or organizational structures,
- easily incorporated into communications and information technology planning, and
- time phased to represent current and future capabilities.

Architectures can describe large and complex processes, be developed incrementally, and answer key questions: who needs to be interoperable with whom, what information or services must be shared, and what standards are needed to make it all work? Interoperability and standardization tasks are much easier with a blueprint in place. Trying to implement an interoperability and standardization program without a master plan is impossible.

NATIONAL TRAINING STANDARDS FOR HOMELAND SECURITY

Training for homeland security professionals offers a large near-term return on investment for improving national readiness. Yet the current menu of training opportunities consists of multiple, nonstandard, overlapping federal courses and a dizzying array of nonfederal programs of varying scope and quality. Congress has recognized the need for coordinating this effort; in Section 430 of the Homeland Security Act of 2002 (Public Law 107-296), Congress tasked DHS with coordinating "preparedness efforts at the federal level, and with working with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support."

Establishing clear national training standards will

- improve the focus and quality of the training programs,
- enable the consolidation and streamlining of the multiple similar training programs that the federal government offers to assist state and local governments, and
- facilitate the development of a streamlined, standards-based DHS training system.

DHS will take a leadership role in developing standards and certification processes for non-DHS homeland security training. DHS must work with the state and local governments and professional associations to establish a collaborative process for developing and maintaining a comprehensive set of national standards for first responders and other functional personnel.

We must place a high priority on training standards for those leaders who have to integrate different functional capabilities at the local, state, and federal levels. With standardized training, senior leaders will be able to effectively orchestrate and employ teams and capabilities from multiple diverse functional areas.

A SINGLE, COMPREHENSIVE HOMELAND SECURITY STANDARDIZATION PROGRAM

The effective management of equipment interoperability, technical standards, and testing protocols is required. We need a Homeland Security Standardization Program as a central management and information resource for all standardization and testing-related issues. Such a program would involve many different organizations. The Interagency Board for Equipment Standardization and Interoperability (IAB), for example, is cochaired by DHS's Office of Domestic Preparedness (formerly part of the Department of Justice) and the Department of Defense. In its 2000 annual report, the IAB stated that it works with selected federal, state, local, and association groups "to develop, maintain, and update a nationalized standardized equipment list for use by the interagency community in preparing for and responding to weapons of mass destruction terrorism."

The DSP has a 50-year history of developing coordinating, maintaining, and making defense-related standardization documents available to all who need them. The DSP, IAB, and many other organizations must work together to shape the Homeland Security Standardization Program. Only together can we transcend the often fuzzy boundaries of standardization and provide a meaningful capability across the spectrum of the homeland security program.

The coalition must create an integrated standards and testing program that embraces all of the functional areas within the homeland security domain. The functional experts within each standardization area must remain responsible for technical content and collaboration with stakeholders, but at the same time, must function as part of a single seamless and comprehensive program.

Conclusions

A comprehensive interoperability and standardization program can ensure the effective coordination of homeland security preparedness and response capabilities. A collaborative, top-down approach can make this program a reality. Establishing a common language and building a blueprint for capabilities in the form of an operational architecture can provide the necessary framework for other needed interoperability initiatives.

We can consolidate training and equipment standards into a well-managed, focused program that will help first responders and other homeland security professionals maximize the capability of available resources, share information and services, and provide the nation with a trained and ready coalition of federal, state, local, and nongovernmental professionals for this vital mission. Achieving these objectives will require DHS leadership and involve many different organizations in government, the private sector, and our friends around the world. Among these many and diverse players, the DSP stands ready to contribute its skills, knowledge, and resources to make us all more secure.

About the Authors

Richard Jackson has worked on nuclear, biological, and chemical defense; homeland security; and interoperability issues in both government and commercial programs for the past 27 years. A retired Army colonel, he is currently a research fellow at the Logistics Management Institute, McLean, VA.

Brian Mansir has worked at the Logistics Management Institute for the past 25 years. He leads research and analysis projects and provides counsel to senior leaders of the nation's national security and other public-sector organizations.

[1] General Accounting Office, *Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness*, GAO-02-473T, March 1, 2002, states that "More than 40 federal entities have a role in combating and responding to terrorism, and more than 20 federal entities in bioterrorism alone." An early chart on homeland security showed 44 federal agencies with significant homeland security responsibilities.

[2] Our definition of an operational architecture is adapted from the definition in *C4ISR Architecture Framework Version 2.0*, published by the Department of Defense C4ISR Architectures Working Group, December 18, 1997.

Dick Tracy Comes of Age

Digital Radio Technology for the First Responders

By Gerald Doempke

"Breaker, Breaker, Smokey in a plain wrapper coming your way!" How did that truck driver spot the unmarked police cruiser? Easy, it was a late model sedan, with antennas on the trunk. Lots of antennas! Each antenna, of course, is connected to a different radio and data system. The problem is that as public-service units move to more data-intensive operations, especially with the post-9/11 homeland security initiatives, reliance on separate data and communications systems must give way to a new model: shared data traveling over interoperable wireless networks.

Police departments were among the first users of mobile radios, which enabled them to respond to emergencies and coordinate with other units. In April 1928, the Detroit, MI, police department began regular one-way radio communications with its patrol cars. In March 1933, the first two-way mobile radio was installed by the Bayonne, NJ, police department. Soon, after realizing that close communications could be used to marshal emergency units beyond the artificial limits of precinct and district boundaries, fire departments and ambulance units began using two-way radios.

Over time, emergency units added data communications, on-scene injury diagnostics, national criminal databases, global positioning, and other systems. Each system requires another radio and another antenna. However,

despite the proliferation of various systems, emergency units still cannot communicate with emergency responders from different jurisdictions—as the nation has discovered during major catastrophes.

Communication among emergency units across jurisdictional boundaries will not improve by adding new radios, even with miniaturization. There is simply not enough room in emergency vehicles for all of the systems needed to cover the breadth and diversity of communications when responding to an emergency. And space is not the only issue. The limitations of the existing systems cause unexpected hazards, as illustrated by the inability of homeland defense fighter aircraft to communicate with public and commercial aircraft.

The answer is not more radios, but a radio system that can enable any kind of communications—much like computer systems that can perform many functions. Like radios, digital desktop systems were initially designed to carry out specific functions, for example, word processing, accounting, or graphics. Then the personal computer was developed as a multipurpose data system that could perform many functions as controlled by one of several software programs, each designed to make the computer do a specific job. As with radios, each system was unique and had unique software and data formats. Interoperability did not exist until the PC system architecture evolved to become an open standard. Now, although many manufacturers build systems and myriad software houses write programs, they all use the same industry standard. This allows all hardware and software to work together and makes it possible to share files among systems. Networking technologies have taken these capabilities to new levels, enabling national and international sharing of data and making ubiquitous communications seamless to the user. Digital technologies have become part of the very fabric of our lives, and the application of digital communications is readily apparent to anyone who uses a cell phone or personal digital assistant.

Digital communications systems work because there is a vast, fixed, commercial network infrastructure to handle incompatibilities, but no such infrastructure exists for homeland security and public-service units. Although their many radios can operate in multiple systems, emergency units need networks that can be formed ad hoc to support a changing emergency environment—one in which units arrive, leave, or redeploy around the area. The solution to such a requirement is a software-defined radio (SDR), which can be programmed to operate in many modes and can be reprogrammed quickly to meet necessary operational requirements. SDRs that operate in one mode within a district can be changed to adapt to the communications of another district or to a special interoperable mode during a crisis.

DoD's Work on Digital Radio Technology

The largest single user of radio technology is DoD, which is addressing the interoperability problem through the development of the Joint Tactical Radio System (JTRS) based on software communications architecture (SCA) standards.

The use of DoD radio-based communications and data systems has grown; the ability to conduct joint service operations involving sea, air, land, and space elements has become essential. The various high-technology systems did their mission, but joint forces could not share information without relying on the lowest common denominator of radio communications—plain voice. To solve that problem, and address future communications, the Office of the Secretary of Defense initiated JTRS in 1997. The JTRS concept involves SDRs running SCA-compliant waveform application software. The result is a single family of waveform application software to be maintained. The current diverse radios will be replaced by a few types of SDRs, each type, called a "cluster" (because it is intended to meet a cluster of joint requirements), defined by size, power, and operating environments.

Establishment and maintenance of the JTRS SCA standards and development and maintenance of the standard waveform application software are the responsibility of the JTRS Joint Program Office (JPO). To optimize the effectiveness and industry acceptance of the SCA, the JPO developed the SCA through a two-step process over a 3-year period. The JPO began by soliciting initial architecture definitions from three different industry consortia and selecting desired features from the definitions they provided. Then, the JPO developed the SCA from the definitions and validated (through prototyping efforts) that the SCA could be implemented in products that meet program requirements. The JPO led an industry consortium in developing the SCA specification and building four prototypes. In addition, the JPO led seven separate efforts to address particular concerns and verify that independent developers could build SCA-compliant products.

Throughout the development process, the JPO SCA team sought to maximize industry input from a range of sources to ensure that industry can, and will, use the SCA, while establishing a single standard that will meet government goals. The JPO works closely with the SDR Forum (SDRF), an association of more than 130 commercial and military industries, to ensure that the SCA meets the SDRF members' needs. The SDRF Working Group incorporated commercial industry concerns, endorsed the SCA, and forwarded it to the Object Management Group, an international commercial standards body of more than 300 member companies, for endorsement. The JPO also held a series of open workshops to promote the SCA, educate developers on technical aspects of the SCA, inform academia, and solicit comments. Finally, the JPO developed an open-source implementation of the core framework (the primary middleware component defined in the SCA) to facilitate vendor SCA use. The JPO is now developing a set of industry test tools to assess SCA compliance.

The JPO's purpose in involving commercial and international organizations in the development of the SCA was twofold: utilize the best of the commercial technologies, and ensure that it developed an open architecture that could be adapted by industry for commercial use, thus allowing the momentum of industry to keep the architecture consistent with digital technology developments.

Defense Applications

For defense applications, the joint services are initially developing four JTRS clusters:

- Cluster 1—Ground, Vehicular, and Rotary Wing, led by the Army
- Cluster 2—Handheld and Back-

pack, led by the Special Operations Command

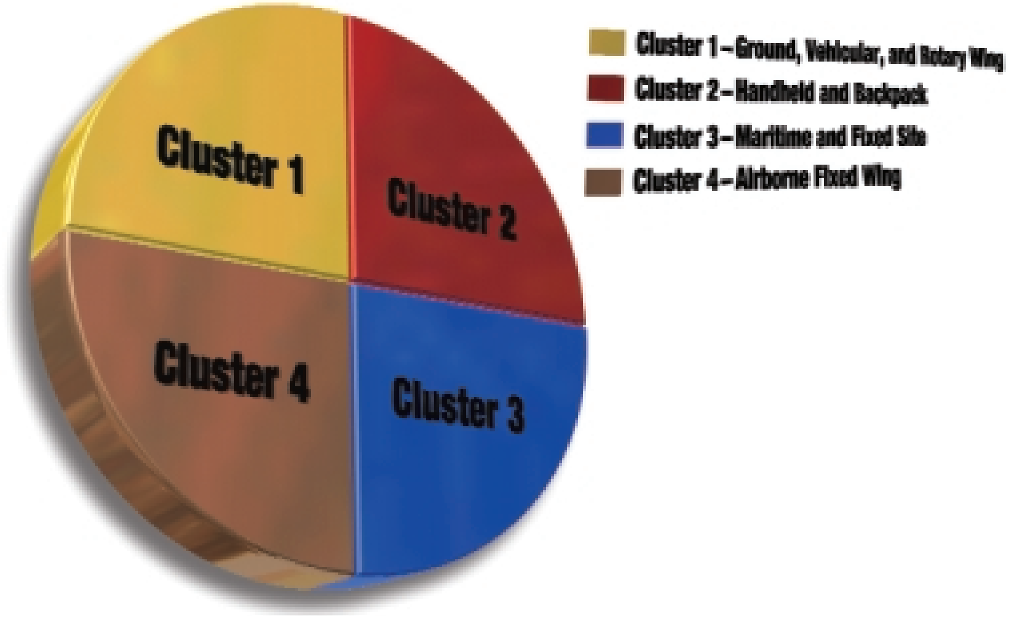
- Cluster 3—Maritime and Fixed Site, led by the Navy
- Cluster 4—Airborne Fixed Wing, led by the Air Force.

Additional clusters for embedded small form factor, command and control, and space-based communications systems are envisioned.

The payoff for defense will be huge. The successful development of standardized software architecture for communications systems will result in significant cost savings, for several reasons:

- The use of standard waveform application software, shared among all SDRs, will reduce the need (and cost) for major development and modification efforts.
- Waveform-related efforts can move toward standardization independently of their radio hardware.
- Multiple vendors can produce myriad combinations of radio features, designed around a standard open architecture and capable of using the same standard waveform application software.
- The channels of a multichannel SDR can be configured to operate in whatever mode is necessary, and they can be changed as the local situation changes, thus reducing the need for multiple same-type radios.

JTRS Clusters



- Common hardware and software components will increase logistics efficiencies and decrease life-cycle costs.
- International and commercial standardization will leverage a number of commercial hardware and software technologies.

Homeland Security Applications

The application of the SCA to homeland security and public-service use is obvious. DoD has invested in an open software communications architecture, enabling the use of a new class of radio network communications, much like the investment in Macintosh and PC architectures led to the widespread use of computer networks. With SDRs, a fire unit could roll up to a large emergency and tune to a common public-service channel to receive instructions on the communications settings to use. In fact, these settings could be transmitted to set up the SDR automatically. Responders without an SDR could participate by having one SDR unit serve as a cross-band relay system, passing communications from one communications system to another. In the short term, a Federal Emergency Management Agency or National Guard translator-relay van could tie in all responders, regardless of their legacy communications systems.

Some federal and local agencies have already begun to develop wireless network data communications systems, generally using established commercial systems and technologies. However, although these systems and technologies will provide multiple functions, incompatibilities across networks will still be a problem. Solving that problem will require radio frequency translators and bridges to pass data and communications across disparate systems.

The Vision—An Ad Hoc Digital Network

While the immediate requirements for new SDRs to be compatible with current communications systems is important, it is the future vision that changes the model completely. Rather than transmitting voice, video, or text, communications systems will simply send data packets on whatever channel is available, much like the Internet finds the path to send packets of information from one computer to another. Just as a message can now be sent to a specific user, emergency communications will allow individuals to communicate directly with each other on the same wireless network as other responders, yet still be able to receive networkwide communications, such as from the area coordinator.

The envisioned network is not unlike what is currently available from commercial wireless networks. However, a public-service mobile wireless network needs the capability to form ad hoc to support all units responding to a particular emergency, and to change as the situation and units change. Adaptable interoperability would even enable the use of existing cellular communications where available.

One key customer for SDRs operating over an ad hoc digital network is the Coast Guard. Its vessels need to interoperate with various communications systems around the world, so a radio that can adapt to local systems would be invaluable. It would eliminate the need for multiple communications systems, enabling vessels to operate where needed, without refitting new communications equipment when they move to a different area of operations. An adaptable radio could interoperate with both domestic and foreign systems. Furthermore, as the expanding use of commercial wireless applications encroaches on or interferes with current public radio bands, an adaptable SDR system can utilize available bandwidth, depending on the local conditions. Eventually, national radio frequency area maps can enable units with a global positioning system to determine the best local frequency operating bands.

With an ad hoc digital network, radio and processing capabilities can be developed independently. Rather than using multiple data systems, homeland security and public-service units can operate with portable computers in multiple modes, linking the units to various data and image sources. By connecting the data systems to a separate radio network, data systems can become multipurpose, and emergency units can be equipped with new software as new capabilities are needed or new functions are developed. Furthermore, ad hoc mobile networks based on a standard SDR architecture can overcome the vulnerabilities to damage, or overload in emergencies, of fixed commercial infrastructure.

Parallel with the development of SDRs is the exploration of new switching and antenna technologies. The vision is to have antennas that do not need to be attached to vehicles, but rather conform to, or are part of, a vehicle's structure. So the truck driver won't be able to spot the "County Mounty," because the police car's roof itself will be the antenna for multiple communications, and the radio, computer, and display will be embedded, rather than fill the front seat.

First responders will really value the ability to communicate with other responders, regardless of the situation. That is the true vision of the SDR.

About the Author

Gerald Doempke is a senior research analyst for Analytic Services, Inc., an independent, not-for-profit public-service research institute and home of the ANSER Institute for Homeland Security. He has extensive experience as a project manager and consulting engineer to various DoD components and NASA. He currently supports the JTRS program.

Information Technology Standards and Interoperability

The Challenge of Homeland Security

By Russell Richards

In 1995, the National Research Council published a report stating:

> Many facets of our daily lives depend on standards….Standards may function to inform, to facilitate, to control, or to interconnect—frequently, a combination of such elements….They also serve societal aims, such as protecting health, safety and the environment.[1]

The Council could not have known the extent of the challenge that would occur 6 years later, after the terrorist attacks on September 11, 2001, in "protecting health, safety and the environment." It is now more important than ever to use standards to step up and meet those "societal aims."

Standards for information technology (IT) are key to meeting societal aims because we depend more and more on technology to provide the tools we need to protect health, safety, and the environment:

> Ensuring homeland security necessitates linking many disparate government computer systems together. Security depends on finding ways of tying information together that is held and managed at the federal, state and local government level as well as the private sector, to ensure that the right people have the right information at the time when they require it.[2]

The Congressional Research Service (CRS) addressed some of the standards issues in *Homeland Security: Standards for State and Local Preparedness* (released on January 2, 2003).[3] This article describes some of the actions taken in direct response to the needs identified in the CRS report and describes some initiatives to implement preparedness standards.

A key player in standardization efforts in the United States is the American National Standards Institute (ANSI). ANSI's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and by safeguarding their integrity. As part of fulfilling that mission as it applies to homeland security, ANSI, on February 5, 2003, established a Homeland Security Standards Panel. ANSI tasked the panel to

- promote a positive, cooperative partnership between the public and private sectors and
- identify and communicate to governmental units the existence of current standards that can meet urgent needs.[4]

The panel's initial tasks will be to catalog, promote, accelerate, and coordinate the development

Interoperability is key to the use of information technology in homeland security. Linking many government computer systems ensures access and management of data across traditional boundaries.

of standards in homeland security areas. Those areas include transportation, biometrics, cybersecurity, and interoperability of emergency-response equipment.

Congress will play an important role in promoting national interoperability through standards. According to *National Strategy for Homeland Security*, the United States has more than 87,000 different jurisdictions. Achieving interoperability across all these jurisdictions is a daunting task. In considering the legislative options, the CRS report noted the following:

> The 107th Congress addressed the issue of preparedness standards, particularly in its debate on the Department of Homeland Security (DHS). Initial versions of the DHS bill (H.R. 5005 and S. 2452) took broad approaches, authorizing the new department to coordinate and develop standards for first responders. The Administration appeared to support such an approach in its *National Strategy for Homeland Security*. Ultimately, however, the enacted version (P.L. 107-296) took a narrower approach, instructing the department to develop standards for a limited number of functions, mostly related to emergency response equipment and technology.[5]

Congress considered a number of approaches it could take to address preparedness standards:[6]

- Congress could mandate that states and localities meet set standards. That approach arguably could ensure adherence to set standards, but would likely raise a number of federalism issues, including unfunded mandates, preemption, and enforcement.
- Congress could make federal assistance conditional on meeting set standards. That approach could prompt states and localities to satisfy standards, but could limit recipients' flexibility with federal funds.
- Congress could encourage the development and implementation of standards. That approach could give states and localities dis-

cretion in adapting standards to their unique preparedness needs, but may not lead to nationwide adoption.

- Congress could take no action. Many observers believe that defining a baseline level of preparedness is a daunting challenge with questionable benefits. Also, some believe that current nongovernmental and federal efforts to develop preparedness standards are sufficient to meet public safety needs.

The specific approach to deploying preparedness standards remains undetermined. However, regardless of the approach chosen, IT will play a role. We must call upon technology and supporting standards to

- ensure that public safety elements can communicate and exchange information effectively, not only across neighboring jurisdictional boundaries but also nationwide;
- provide information on demand, in near real time, to support heightened protection of major bridges and tunnels and key pieces of infrastructure such as nuclear power plants, railroad lines, and ports;
- enhance capabilities to sense the threat of "militarized" diseases using unexpected vectors like the postal system, prevailing winds, water supplies, and sewer systems; and
- improve the nation's methods of screening people and baggage at airports, train and bus depots, and passenger ports for weapons (as small as pocket knives) and explosive devices (including methods for using the transportation fuel system as the actual source of a massive explosion).

Many initiatives required to help fortify America's security had already been envisioned and pursued when the Office of Homeland Security was formed shortly after September 11, 2001. The following are some of the key initiatives:

- *Supporting first responders.* "First responders" are the personnel typically required immediately at the scene of an emergency. Communicating with and mobilizing first responders quickly—through standardized communications equipment and infrastructure—can save valuable time and, potentially, lives and have a profound impact on crisis management.
- *Securing America's borders.* Standardized technology plays an increasing roll as a means of detecting, analyzing, and tracking the movement of people and goods into and throughout the United States. The thousands of miles of coastline (Atlantic Ocean, Gulf of Mexico, and Pacific Ocean) and our common borders with Mexico and Canada make this task a daunting one. Everywhere along our borders, not just ports of entry, are potential entry points for terrorists (on foot or aboard vehicles on the ground, in the air, or on or under the water).
- *Defending against bioterrorism.* The fight against bioterrorism requires detection and intervention technology, as well as standards-based communications technology and infrastructure. This extends from communicating with the personnel who remotely monitor and inspect the nation's food and water sources, to providing citizens and agencies with information or emergency notification systems, to using multichannel customer relationship management solutions for tracking, collecting, and providing critical information.
- *Leveraging 21st century technologies.* Established and emerging technology, standard-

ized to reduce cost and increase dependability, must be used widely in a practical way to implement solutions and accomplish our security goals. Leveraging technology may be the differentiating factor as we strive to anticipate, detect, and act upon accurate, secure, and dependable information that has never been more important.

- *Undertaking government-to-government federal initiatives*. These Office of Management and Budget initiatives (for example, wireless public safety interoperable communications, or Project SAFECOM) will enable sharing and integration of federal, state, and local data to facilitate better leveraging of investments in IT systems (for example, geographical information) and to provide better integration of key government operations, such as disaster response.[7] These initiatives will also support intergovernmental integration requirements for homeland security.

Technology and appropriate standardization to achieve the objectives of the initiatives have been at the forefront, and improvements in the communications infrastructure have been perceived as playing a major role in the transformation of our homeland security infrastructure.

Each of the initiatives deserves a great deal of discussion for a full understanding of the implications of how the landscape of national security has changed and how standardization has and must change to focus on security actions to protect our homeland as well as to support defense and military actions in other parts of the world. To the extent possible, we should leverage the experience of our defense community (DoD, U.S. defense industry, and other stakeholders), as well as the "homeland security" efforts of other nations and NATO, to capitalize on solutions and approaches already devised. At the same time, we must be able to define how the challenges of homeland security and defense are different from the challenges in our leveraging models. And we must find ways to rapidly fill the gaps with standardized, repeatable, extensible solutions that will work to provide fast, cost-effective, and leading-edge advantages to the leaders and managers of homeland security and to those who are on the front lines responding to threats to our security.

About the Author

Russell Richards is the lead engineer for the Center for Joint and Coalition Interoperability in the Interoperability Directorate, Defense Information Systems Agency. He has served in military or civilian capacities for more than 20 years, including several years as the DoD Information Architect, supporting DoD as well as other national defense ministries, U.S. federal organizations, and industry leaders in matters related to information technology and affiliated standards.✺

[1] National Research Council, *Standards, Conformity Assessment, and Trade—Into the 21st Century* (Washington, DC: National Academy Press, 1995), p. 9.

[2] Open GIS Consortium, Inc., *The Importance of Open Interoperability Standards in Homeland Security*.

[3] Library of Congress, Congressional Research Service, *Homeland Security: Standards for State and Local Preparedness*, January 2, 2003.

[4] American National Standards Institute, "ANSI Forms Homeland Security Standards Panel as Coordination Body for Private and Public Sectors" [online article], February 5, 2003. Available from http://www.ansi.org/news_publications.

[5] See Note 3.

[6] See Note 3.

[7] The eGov Task Force specified that public safety personnel must be able to communicate with local, state, and federal agencies in the event of an emergency or other public safety response event. The task force indicated that the efforts of the Project SAFECOM partners will be focused on specific results, including effective, interoperable communications throughout government; integration across levels of governments; saved lives through quicker response and coordination; and realized cost savings through standardization and sharing. See http://snad.ncsl.nist.gov/fwuf/may02slides/wiesner.pdf.

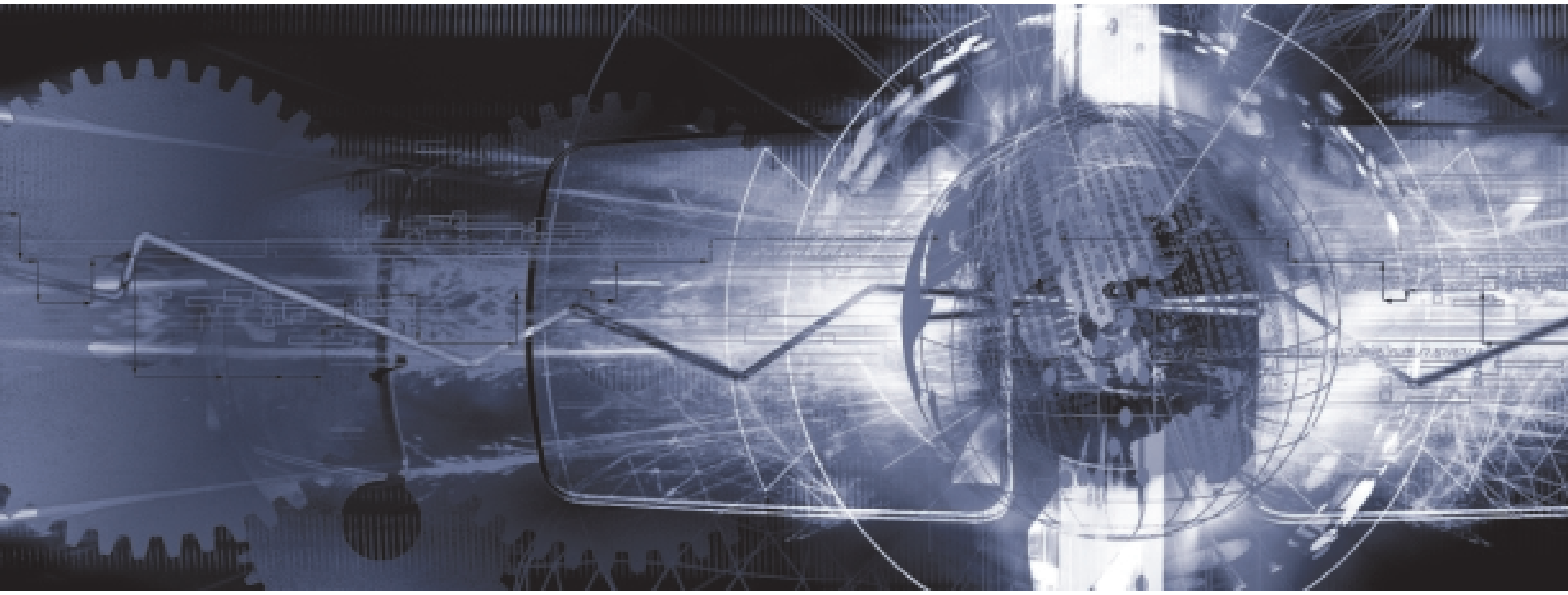
Inter-Enterprise Architectures

Using a Collaborative Approach to Standardizing Enterprise Architecture Components

By Joel Henson, Kristina Olanders, and Didier Perdu

Introduction and Summary

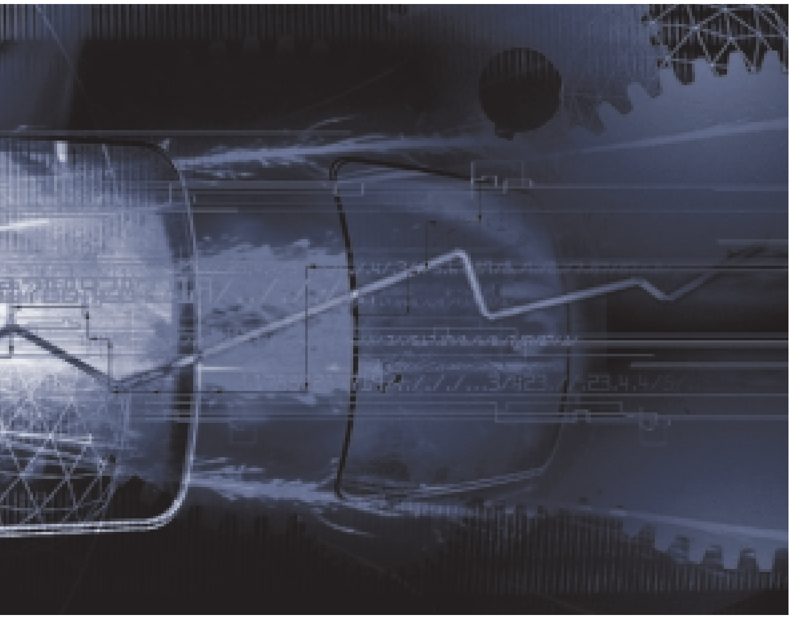
One of the questions facing the new Department of Homeland Security (DHS) is how to address the need for government and private-sector organizations at all levels to collaborate effectively to secure the nation against a terrorist attack and, should an attack occur, respond effectively. The key to effective collaboration is sharing information efficiently across organizational and geographic boundaries: all organizations involved in homeland security must have quality information readily available at the right place and at the right time. For example, they need to disseminate information about individuals who are under surveillance, and during an emergency, they need to coordinate information about available resources, such as the location of personnel with medical experience or specialized equipment.



Among the organizations that must share information are DHS, some 20 other federal agencies with responsibilities for homeland security (notably, the Department of Defense and the National Institute of Standards and Technology), state and local governments, and various nongovernmental organizations (associations, industry, volunteer organizations). So establishing a practicable approach for knowledge dissemination is not a trivial exercise. The approach must accommodate the business needs of each organization while enabling each organization to share information with other organizations and, at the same time, ensuring the security and privacy of America's citizens.

DHS faces two major challenges in coordinating the efforts of the myriad external organizations involved in homeland security:

- The organizations have different functions, processes, procedures, and assets—all designed to meet their particular business needs—that together enable them to fulfill their stated missions.
- DHS does not have the authority to specify how organizations outside of DHS do their jobs. Funding is limited for those external organizations to purchase new equipment or to change their procedures to carry out necessary changes.



Our solution? An approach that leverages resources already deployed. Specifically, DHS can leverage basic information about each organization—its functions and processes, pieces of information critical to performing those functions, software used to manage that information, and the technology in place—to establish interrelationships. In other words, it can define where connections among organizations must occur—what information must be shared—to achieve seamless interoperability as an "inter-enterprise." We recommend using an enterprise architecture framework to define and categorize those connections.

There are many stakeholder "communities of interest"—law enforcement, emergency medical service providers, and so on. Each of these communities has standard practices and established technology standards that are readily available to be used or augmented. DHS can leverage the work of existing standards-making bodies, encouraging them to develop additional standard practices (based on best practices) and augment existing technology standards, where necessary, and to promulgate those standards within their respective communities of interest. DHS's key role is to maintain a constant presence, exerting its influence by helping to shape the standards, such as pointing out best practices. Its goal should be to ensure that standards are applied nationwide so that seamless interoperability is feasible. From a technical standpoint, making those connections requires the establishment of standards so that all organizations use common points of reference.

What Do We Mean by "Inter-Enterprise"?

An inter-enterprise is an alliance of stakeholder organizations working as one to secure the nation against terrorism and to respond effectively if an attack occurs. Numerous inter-enterprises can exist at any time, but all would have the same common mission—secure the homeland. And one organization can contribute to more than one inter-enterprise.

An inter-enterprise has the following fundamental characteristics:

- The organizations participating in a particular inter-enterprise vary, depending on the specific need. For example, state motor vehicle departments and the Immigration and Naturalization Service maintain data about individuals. Their sharing of that information—as an inter-enterprise—may help identify individuals who have entered the country illegally but have established U.S. credentials.
- The life span is variable; a particular inter-enterprise exists only as long as necessary to address the need. In other words, organizations participating in an inter-enterprise interact solely to the extent required by the specific purpose or need that unites them. For example, a city's hospitals, fire and police departments, the American Red Cross, and the Federal Emergency Management Agency share information and resources (personnel, equipment) when responding to an earthquake. When the crisis is over, the resources are given back to the owning organizations and the inter-enterprise ceases to exist. Other inter-enterprises may be permanent. For example, law enforcement organizations at all levels can continually share information about suspects.

In sum, an inter-enterprise unites any number of organizations—at as many levels as necessary and as long as necessary—so that they can collaborate effectively on some aspect of homeland security.

How Can Disparate Organizations Work Together Seamlessly?

For an inter-enterprise to be successful, all of the organizations involved must understand each other's capabilities, skills, assets, knowledge, and authority so that they can augment and draw on those resources as necessary. For example, a state knows whether a tractor trailer is properly licensed and inspected, a shipping company knows the contents and location, and various federal entities may have an interest in certain cargos. By sharing data from the licensing process, the shipping manifest process, and information captured for regulatory processes, stakeholder organizations can have a comprehensive view of a given cargo.

Gaining that understanding requires identifying common points of reference at different levels. We suggest that virtually all organizations—no matter what their size—have four things in common: each has a mission and specific business functions and processes that it must complete to fulfill that mission, each uses information in its processes, each has applications and communications systems that it uses to manage its information, and each uses information technology (IT) to support its applications. What is needed is a national strategy to coordinate those common components across all organizations involved in homeland security so that they can readily exchange information. We recommend an enterprise architecture framework.

What Is an Enterprise Architecture?

According to the Federal Chief Information Officers (CIO) Council,

> An enterprise architecture…defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing needs of business.[1]

Typically, an organization captures its enterprise architecture information in an automated repository or database. The organization can then run queries to identify the interrelationships of the different types of information. That information aids decision making within the organization. For example, it can readily identify which technologies support which applications and thus determine the practicability of eliminating an outdated technology. And it can determine whether the applications it is using effectively support its business processes. The enterprise architecture repository can reflect a particular framework.

Numerous enterprise architecture frameworks have been developed. The most commonly used are Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), developed by DoD; Federal Enterprise Architecture Framework (FEAF), developed by the Federal CIO Council; National Association of State Chief Information Officers (NASCIO) Adaptive Enterprise Architecture; and Zachman (see Figure 1).

FIGURE 1. Potential Architecture Frameworks in the Inter-Enterprise

C4ISR
FEAF
Zachman
NASCIO
Others
?

Each of the architecture frameworks was developed for a specific purpose. The C4ISR framework provides direction on how to describe architectures and is a product-focused method for standardizing architecture descriptions. FEAF was developed to support agencies' IT investment selections and the management of their IT portfolios. The NASCIO Adaptive Enterprise Architecture is a guide to the enterprise architecture evolution process and provides process models and templates.

What Architecture Framework Is Best for an Inter-Enterprise?

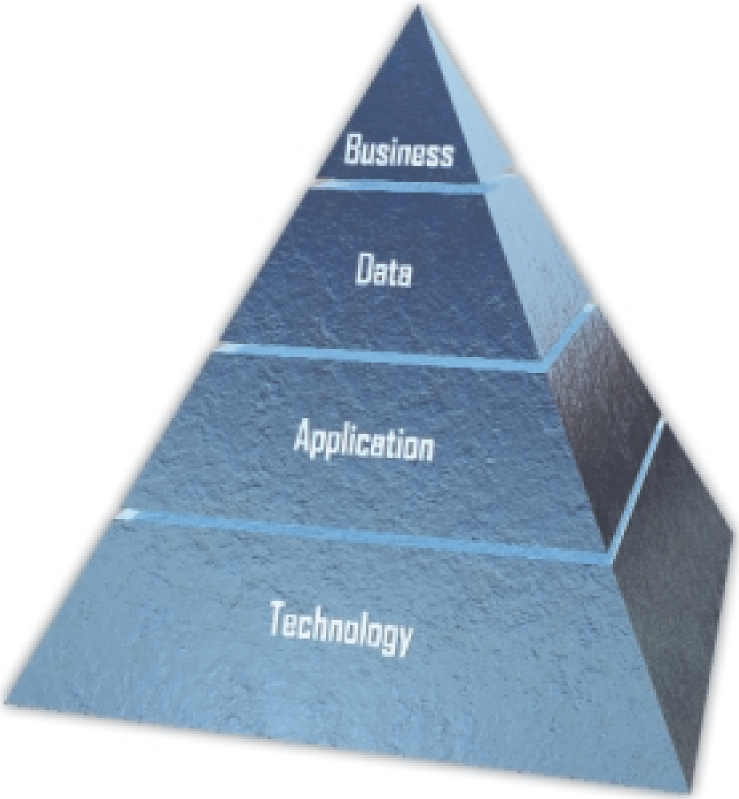
We believe that FEAF would be best for an inter-enterprise:

- It is a simple, basic approach to organizing an inventory of enterprise architecture information.
- It is well established and understood throughout the federal government.
- It is flexible, allowing each organization in the inter-enterprise to continue using the enterprise architecture framework it has already deployed, but enabling them to share command information with other organizations.

FEAF was first developed in 1998 to address the need in the federal government for a common set of terms for a given set of events, actions, organizations, information, and information technology systems. FEAF also serves as a reference point to facilitate the efficient and effective coordination of common business processes, information flows, applications, infrastructure components, and investments among federal agencies. The objective was to enable business processes and systems to operate seamlessly in an enterprise architecture that provides standards that identify and define the information services used throughout the government. As depicted in Figure 2, FEAF has four separately defined, but interrelated layers:

- Business architecture. The business architecture defines the business processes needed to perform the functions that the organization undertakes to achieve its goals and thereby accomplish its mission. This layer

FIGURE 2. Federal Enterprise Architecture Framework



also addresses the sequence in which the business processes occur, the organizational units that perform those functions, and the locations where the processes occur.

- Data architecture. The data architecture defines the pieces of information needed in the business processes and the interrelationships of those pieces of information.
- Application architecture. The application architecture defines the applications needed to manage data and support business functions. This layer also identifies the personnel who have access to those applications.
- Technology architecture. The technology architecture defines the hardware and systems software, including operating systems and middleware. In other words, this layer defines the infrastructure used to support the business.

Detail is added to each layer through the use of reference models. A reference model has the same role for an architectural layer as the architecture framework has for the entire inventory of information about the enterprise. Specifically, it identifies what information will be collected; what syntax or standards will be used to convey the information consistently and systematically; and how the information will be organized. These models organize information to support drilling into additional levels of granularity in a consistent way. Table 1 provides examples of the various reference models and the fundamental questions that they answer.

The use of reference models in information technology—application and technology layers—is a long-standing and generally well-understood concept. The most familiar is the technical reference model, which specifies

TABLE 1. Sample Reference Models

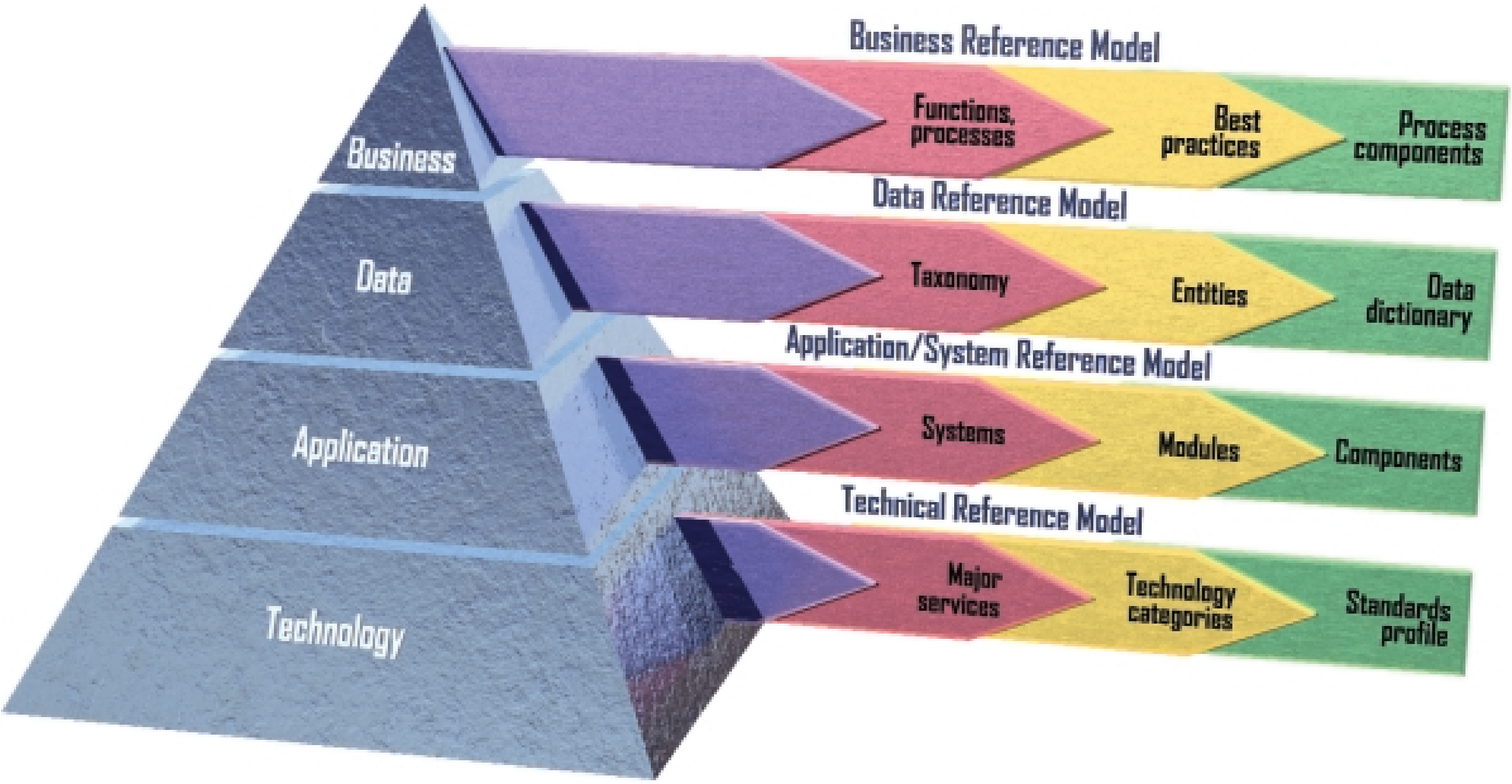
Reference model	How information is organized	What syntax or standards are used	What information is collected
Business	Functions, processes, organization, location	Best practices, standard operating procedures, common practices	Process components that address: Who are you? What do you do? How do you do it? Where are you?
Data	Taxonomy	Entity relationship diagrams, data dictionary, data elements	Data dictionary that defines: What do you know? What do you mean?
Application/ system	Systems	Modules or software and hardware components	Components that address: How are data manipulated? How are data changed? How are data reported? Where are the data?
Technical	Major technology services	Technology categories, standards profile	Standards profile that describes: How can we talk?

technology standards. For example, the technical reference model used by many organizations establishes XML as the standard for sharing information with partner organizations, and some federal agencies use XML for their transactions (such as purchase orders) with industry.

Reference models for the business and data layers exist but often are not as formal or rigorous as those for the application and technology layers. Examples of business and data reference models include the guidance of communities of interest and industry associations for areas as diverse as law enforcement, medicine, environmental sciences, and transportation. The guidance may be documented in standard operating procedures, ISO procedures manuals, and the like, or it may just be a common or generally understood practice.

The federal government is moving toward reference models in its enterprise architecture practices. The Federal Enterprise Architecture Program Management Office (FEAPMO), sponsored by the Office of Management and Budget, has released the first version of the federal government-wide business reference model and will soon release a second, updated version. Figure 3 depicts the conceptual relationship between the enterprise architecture framework and the various reference models.

FIGURE 3. Conceptual Relationship Between Enterprise Architecture and Reference Models



Where Should Organizations Connect Their Enterprise Architectures to Share Information?

To achieve seamless interoperability as an inter-enterprise, organizations must share information at the detail level—the part of the reference model that identifies what information is collected. DHS and the stakeholders in securing the homeland need a national strategy to identify the types of information that must be shared, and that national strategy must address each architectural layer, thereby establishing an inter-enterprise architecture for homeland security.

Information from the business layer that will contribute to interoperability includes the names of the involved organizations, their missions and mission-critical functions, and the needs they are addressing. Also key are details about each organization's authority or mandate and the geographical area where that authority or mandate is exercised (that is, its jurisdiction), as well as details about its capabilities, skills, and assets. Having such business information available will enable participants in an inter-enterprise to learn what organizations perform similar functions and whether the organizations can contribute to a given mission. For example, before exposing a search-and-rescue team to a situation in which there is a potential biohazard, incident managers need assurance that the team has the appropriate training and skills to work in that environment or need to identify the organization that can best provide that expertise to the team.

Information from the data layer that will contribute to interoperability includes the data that the organizations are maintaining. Data required by the inter-enterprise may be maintained by more than one participating organization and for different purposes. If participants know what data are being maintained, they can validate and perhaps augment those data. For example, state motor vehicle departments maintain data that may be useful in tracking and monitoring potentially vulnerable transportation assets and their cargo.

Information from the application layer that will contribute to interoperability includes application components that are available for sharing. Those components include the systems used in support of a particular business process and the system modules associated with processes and information.

Information from the technology layer that will contribute to interoperability includes the technology standards being used to input, transport, and output data and processes.

How Can Organizations Share Necessary Information?

The organizations in the inter-enterprise can share information efficiently, and thus achieve seamless interoperability, only if they use common syntax or standards in their enterprise architectures. To put it another way, they need common points of reference for a given set of events, actions, organizations, information, and IT systems. These reference points would enable an organization to obtain information at an appropriate level of detail. For example, a city manager would know that Fire Station 5 on Main Street has a qualified two-person biohazard team, while an organization at the national level would know only that a qualified team was in the area.

Again, the syntax or standards must be established for each business function or activity. Standards for the business layer include the recommended or best practices that can be applied to given business processes. Information about the mission and capabilities of an organization provides a starting point from which to categorize and assess where an organization fits into the inter-enterprise. This leads to more specific information about what standards and common practices apply to the organization.

The data layer requires a framework for taxonomy about how information in a given context is going to be classified, related, and grouped for the supported business function. This framework supports the lines of business addressed in the business reference model and the information exchange that occurs between the various organizations. The next level of detail for the data architecture is to provide entity relationships for the types of information. A data dictionary, based on the entities, is then developed to facilitate the mapping of the data. The same data managed by different organizations may have different names. Here again, a need for standardization or transformation is required so that participants in the inter-enterprise understand each other.

> **...the collaboration of the communities that represent first responders can assist in establishing common communications practices and standards that can lead to standards in the devices that they depend upon.**

Standards for the application layer identify and classify applications into those that create information, those that share information, and those that depend on others for input. This assists in the identification of applications that are viable sources of record.

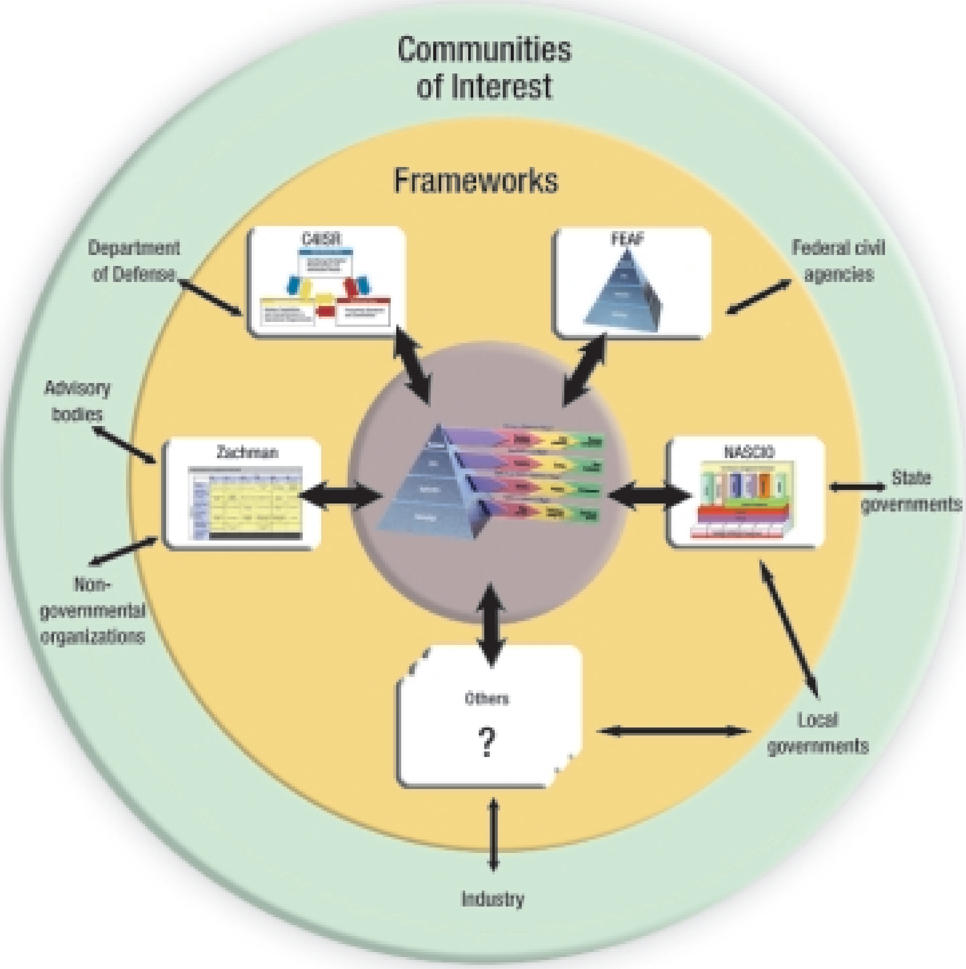
The technology layer requires a hierarchical foundation describing how technology is supporting the delivery of the application capability. It sets and describes the standards used in the software and hardware ultimately supporting the business processes. An example is the establishment of public key infrastructure—PKI—as the standard to enforce privacy and security of data used in a given business process.

How Can Standards Be Developed and Promulgated Nationwide?

DHS does not have any mandate or funding to dictate standards. However, numerous standards-making bodies exist. Their work could be leveraged to assist in the shaping of standards and influence or recommend direction for all participants in a security inter-enterprise. For example, the International Association of Chiefs of Police provides a forum for exchanging law enforcement best practices. That organization and others like it can assist in identifying and sharing common business practices and establishing generally accepted police practices as part of a collaborative process. Similarly, the collaboration of the communities that represent first responders can assist in establishing common communications practices and standards that can lead to standards in the devices that they depend upon. The transportation community can develop standards for identifying and tracking transportation assets. States and local governments can exchange best practices related to task organization and crisis management planning and execution—from setting up a command and control center, to formatting situation reports.

Currently, the many standards bodies are informal stewards of business standards. Their role needs to become more formal and active in order to push the right standards down into common practice. The foundational role of

FIGURE 4. An Inter-Enterprise Enabled by FEAF



DHS will be to encourage those bodies and to foster the collaborative governance necessary to develop additional standards and augment existing standards, where necessary, and to promulgate those standards within their respective communities. DHS must maintain a constant presence, exerting its influence by helping to shape the standards, such as pointing out best practices. Its goal should be to ensure that standards are applied nationwide so that seamless interoperability is feasible.

The long-standing relationship of the Federal CIO Council, FEAPMO, and the Industry Advisory Council—which has assisted in advancing enterprise architectures throughout the federal government—can serve as a model for collaborative governance of the homeland security inter-enterprise. This proven collaborative environment can be extended and its effectiveness enhanced by including representative voices of state and local governments and nongovernmental organizations. Figure 4 depicts the resulting inter-enterprise.

What Is the Next Step?

Once stakeholder organizations have identified the information they need to share and have established a collaborative governance environment for promulgating standards to convey that information consistently and systematically, the logical next step is to enable the sharing of information among disparate communities: federal, state, and local governments; law enforcement groups; emergency medical service providers; volunteer organizations; and so on. The information technology community has identified a variety of solutions to support various functions. For example, there are several viable proposals from the communications industry to establish standards for a common communications protocol for first responders. But other stakeholder organizations in the homeland security inter-enterprise need to decide on their corresponding model for developing, using, and sharing process and data components. Some models are in use. An example is NASCIO's Component Reuse Initiative to encourage the sharing of technology components. Another example is the component reference model recently published by FEAPMO.

A collaboratively developed model of shared components will be a powerful tool to provide consistent, reliable, and cost-effective solutions to securing the homeland. The use of standards-making bodies in this collaborative approach is key to ensuring that the integrated components are cost-effective, are of good quality, and meet the needs of participating organizations.

Conclusion

To realize a national strategy for securing the homeland, DHS can leverage the various communities of interest to guide and shape standard practices supported by common technology standards. Existing architecture frameworks can collaborate using FEAF to map and transform data and information.

FEAF and the reference models associated with each architectural layer are dynamic and powerful tools. By providing descriptions at the finest level of detail of the reference models, we can identify a set of components by layer. The pieces needed for collaborative governance exist in many places. Bringing them into a coherent and useful tool begins with understanding where they fit. The collaborative inter-enterprise architecture framework provides that understanding.

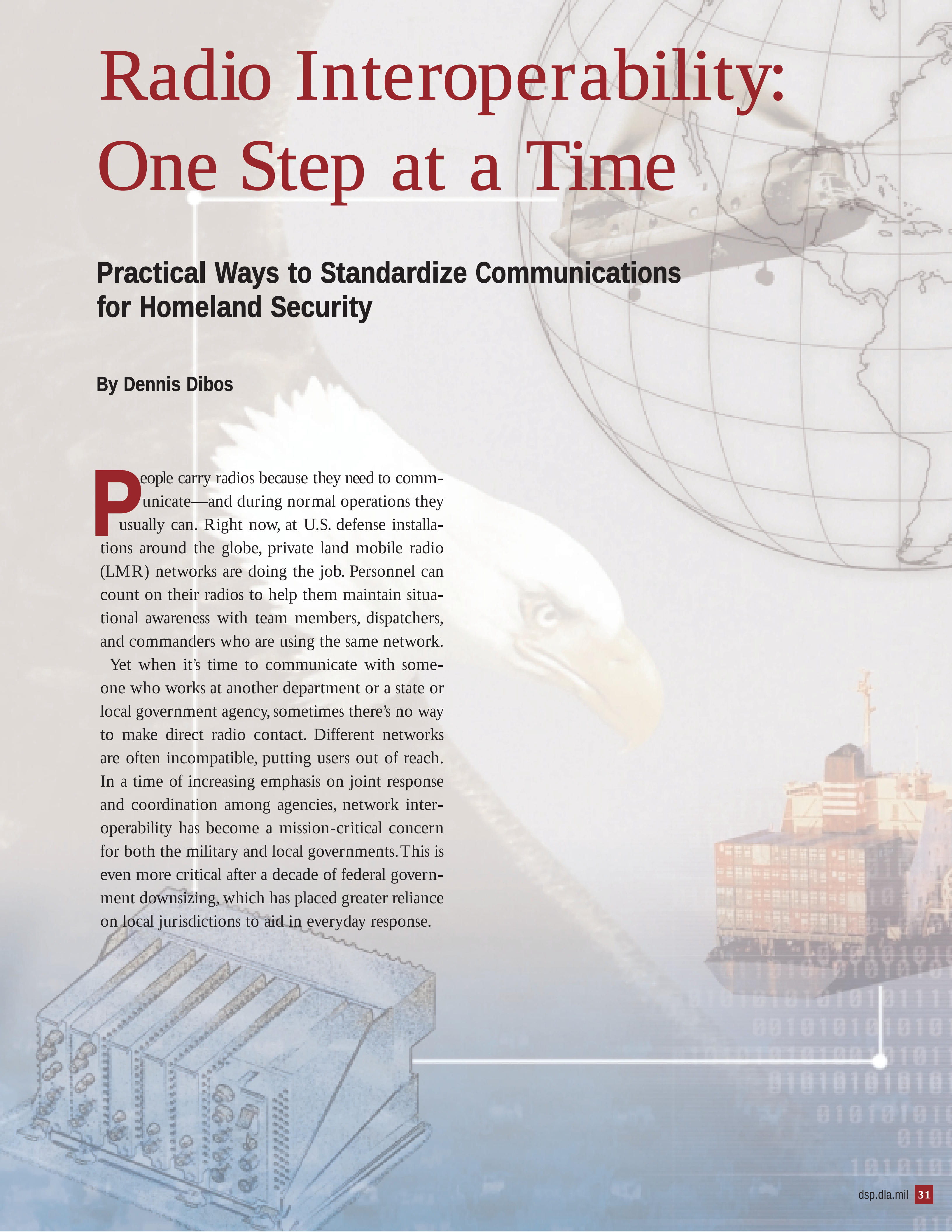
About the Authors

Joel Henson is a program manager with the Information Management program group at the Logistics Management Institute in McLean, VA. The principal author of the LMI Enterprise Architecture Practice™, Mr. Henson's current focus is on using enterprise architectures as a framework to categorize standard practices and align them with technology standards.

Kristina Olanders manages the enterprise architecture program at the Logistics Management Institute. She has participated in the assessment or development of various facets of enterprise information systems architectures for the Department of Defense and numerous civil agencies.

Didier Perdu, Ph.D., is an advisor to the enterprise architecture program at the Logistics Management Institute. He has more than 15 years of experience in the field of enterprise architecture and information systems design, working in both university laboratories and consulting companies.✺

[1] Federal CIO Council, Federal Conceptual Model Subgroup, *Federal Enterprise Architecture Conceptual Framework*, August 1998.



Radio Interoperability: One Step at a Time

Practical Ways to Standardize Communications for Homeland Security

By Dennis Dibos

People carry radios because they need to communicate—and during normal operations they usually can. Right now, at U.S. defense installations around the globe, private land mobile radio (LMR) networks are doing the job. Personnel can count on their radios to help them maintain situational awareness with team members, dispatchers, and commanders who are using the same network.

Yet when it's time to communicate with someone who works at another department or a state or local government agency, sometimes there's no way to make direct radio contact. Different networks are often incompatible, putting users out of reach. In a time of increasing emphasis on joint response and coordination among agencies, network interoperability has become a mission-critical concern for both the military and local governments. This is even more critical after a decade of federal government downsizing, which has placed greater reliance on local jurisdictions to aid in everyday response.

If radio networks are for communicating, how can we get them talking to each other?

Dramatic Changes in the Role of a Communications System

In the 60-plus years since radio first became a vital asset in the defense toolkit, the military's standard mode of operation has changed.

Not so long ago, individual agencies, departments, and installations maintained separate operations with rather limited collaboration across organizational boundaries. Service branches remained separate, and the civilian/military line was rarely breached. Federal, state, and local agencies invested in widely disparate radio systems—analog or digital; conventional or trunking; 800 MHz, VHF, or UHF spectrum bands—that best suited their individual needs at the time of purchase. Different radio networks could not interoperate, but this was not seen as a problem. Even systems purchased from the same vendor might not be compatible.

Today, many of these same networks are still in use, but the mission has changed dramatically. DoD organizations are now expected to mount collaborative efforts with federal, law enforcement, and state and local government entities, sharing both voice and electronic data communications in response to emergencies and ongoing missions. A military base must now be prepared to quickly activate joint communications with

- all departments and functions operating on base;
- other bases, including those operated by other service branches (Army, Navy, Air Force, Marine Corps, Coast Guard);
- civilian and defense agencies at the local, regional, state, and federal levels; and
- local civilian first responders (police, fire, medical services, civil defense).

Radio networks that were originally designed to serve the routine daily needs of their respective users must now adapt to this new environment. Too often, when events require a joint response, personnel from different departments on the same base cannot contact each other. Base-to-base communication is even more problematic. The inability to make direct radio contact can dangerously hinder any force's ability to take coordinated action.

The same concern affects the civilian sector. Often, federal, state, county, and city law enforcement personnel in the same area are unable to talk via radio. When large-scale incidents require mutual assistance from neighboring jurisdictions, radio incompatibilities are a major concern.

Homeland security concerns have highlighted the problem of incompatible networks. Organizations must be prepared to mount an effective joint response to natural and man-made emergencies while, at the same time, continuing to perform their established duties. It is clear that military and civilian organizations at all levels need an interoperable radio solution—a solution that does not compromise an organization's daily activities or its ability to fulfill its mission, but also allows for coordinated interagency response in an emergency.

The Best Solution to System Incompatibility

Standardization is the obvious solution to the problem of system incompatibility. Fortunately, the Association of Public Safety Communications Officials–International, Inc., has developed a suite of LMR standards known as Project 25 (or P25). In the same way that a standard like Microsoft Windows provides a set of agreed-upon rules for computer development, P25 provides a standard for developing radio systems that will be able to work together. P25 has several characteristics that make it widely applicable:

- It supports a variety of radio technologies: conventional or trunked operation, single-site or multisite architecture, analog and digital equipment, and voice and data transmissions. This allows agencies of different sizes to choose a P25 system that fits their needs.
- It allows the use of multiple spectrum bands and supports migration to narrowband

12.5 kHz channels for maximum use of available bandwidth.

- It uses off-the-shelf components that are commonly available and optimized specifically for mission-critical LMR services, giving agencies a wide choice of cost-effective equipment.
- It supports unit-to-unit communication within a limited range (talk-around mode) without the use of a repeater or other network infrastructure. This is a valuable capability in situations where users are outside the range of network transmission sites. It is also a backup in case the infrastructure fails during an emergency, allowing for radio-to-radio communication among personnel at the scene.
- It enables seamless interoperability with other networks and equipment complying with the P25 standard, even if they were built by other manufacturers and use a different frequency range.
- It is scalable to enable additional system capacity to be deployed rapidly at an incident site.

In August 2001, DoD mandated P25 for new LMR equipment purchases. P25 is more than just a standard. It is a process that is constantly evaluated and modified as new technology becomes available. Although it was developed for U.S. civilian public safety, P25 has gained much wider acceptance. It is used in 33 different countries. More than 40 manufacturers have signed on to the P25 Phase I specifications, and compliant products are now available from many vendors.

P25 Advantages

P25 has many advantages that explain why it is now the DoD standard:

- Organizations maintain control over their own separate networks, but can link to other networks as events require.
- "Out-of-the-box" interoperability is quick to implement for a fast emergency response.
- Next-generation equipment is available that is backward compatible, so prior investments are not made obsolete with every new purchase.
- The advanced features being introduced by modern digital systems can be made available to P25 users. P25 defines a minimum feature set, but does not block the introduction of new features (although old equipment might not be able to support some newly introduced or manufacturer-specific features).
- Agencies benefit from all the usual advantages of purchasing standardized equipment: freedom to select from more than one vendor, ability to upgrade or migrate without replacing equipment, and potential to share resources with other organizations to control costs.
- P25 systems can transport voice or data traffic using one network. No special networks or channels are required for data transmissions.

Because P25 is widely accepted in the civilian world, military installations can use it to set up joint voice and data communications with neighboring communities and governmental agencies.

Over the long term, P25 is a great solution for both wireless voice and text messaging. However, if an agency's networks are not yet due for a complete overhaul, its budget may not allow migration to P25 for another few years. During this interim period, military installations require an alternative strategy for radio interoperability.

Interim Solutions

How do you establish a strategy for joint communications? U.S. defense and public safety organizations are employing a variety of interoperability levels chosen to best suit their current needs. Those needs depend on the available budget, current system capabilities, and immediate and long-range requirements.

LEVELS OF RADIO INTEROPERABILITY

Level	Description	Benefits	Pros/cons	Best applications
1—swapping radios	One agency or department provides extra radios to other personnel working a common emergency scene.	Is simple to implement. Has low cost. Works across frequency bands.	Product cross-training is required in advance so people will know how to use the radios. Distributing radios can be a logistical problem.	Immediately following disaster. Small events (two or three agencies). Preplanned events with key players coordinating in advance.
2—talk around	Radios talk to each other directly, in conventional mode, without using network infrastructure.	Is simple to implement. Enables point-to-point direct communication. Is cost efficient. Is simple to initiate calls.	Range is limited. All radios must use same frequency. Radios must have compatible interfaces. No advanced features are available.	Small events (one or two agencies). Tactical coordination. Emergencies only.
3—mutual-aid channels	Multiple radios talk directly to each other using frequencies that are set aside for this purpose. This level is commonly used in civilian public safety.	Is widely available. Most U.S. regions and states have this system in place. Encourages mutual planning. Is cost efficient. Has extended range using dedicated network infrastructure. Is de facto standard.	Preplanning is required. All radios must be capable of operating at specified frequency and have compatible interfaces. Radio is removed from home range (calls on normal channels will not be heard). It has no advanced features. Conventional analog is used as lowest common denominator.	Small- to moderate-scale events (two to four agencies). Unplanned events (agencies must work out a channel plan in advance).
4—gateway	Dedicated hardware and software are installed to build a gateway connecting two systems. Users on both networks can communicate with each other, but only while they are working inside the geographical area in which both systems have overlapping radio coverage.	Connects disparate systems and frequency bands. Can be cost efficient. Has range equal to the overlap area of the two interconnected systems.	Extensive preplanning is required. Operator must manually activate gateway to patch users together when events occur. It has no advanced features; uses audio only. Capacity is limited. Only one channel (or talk group) carries all calls between systems. Capacity of smaller network could be overloaded. Users cannot leave range of home system.	Small- to moderate-scale events (two to four agencies). Preplanned events (concert, sports). Networks with overlapping coverage areas (neighboring communities).
5—system-specific roaming	This level is similar to roaming in a cellular network; a user can maintain communications in areas in which prearranged agreements are in place.	Connects multiple types of systems. Enables instant access. No operator intervention is needed. Has full system features (though limited by the features available in the current location). Has full system range.	Preplanning and investment are required. Depending on configuration, controller can be costly component with infrequent use. Coverage is possible in adjoining areas only. Radios must be compatible with system administrative agreements.	Small to large-scale events. Cross-band. Limited response areas.
6—standards-based systems	Standards-based systems (P25) support full interoperability.	Has robust interoperability. Uses radios built to a common standard. Has full system features. Keeps subscriber operation the same. Enables users to stay in touch with home system.	Deploying a new system is expensive. Strategy is needed for joint communications with agencies that do not yet have a network compatible with P25.	Small to massive events. Urban to rural location. Any spectrum bands.

Starting with level 1 (swapping radios), the strategies become increasingly more sophisticated. Generally, the lower-level strategies (levels 1, 2, and 3) are used as immediate short-term solutions when there are budget and time constraints.

The ultimate solution is level 6, which uses standardized P25 networks for seamless interoperability. After reaching level 6, and until P25 becomes deployed universally, organizations should still have plans to implement lower interoperability levels in case they are required to coordinate communications with an agency that does not have a P25 network of its own.

Agencies must work together to determine which interoperability level is best at striking the correct balance between their joint communications goals and their currently available resources. Over time, that balance will change.

Future Directions

P25 is the military standard for nontactical wireless voice and data communications. In the tactical arena, the military faces a similar communications challenge. But in tactical deployment, the problem is not what type of network infrastructure to build, but rather how to deal with the unpredictability of where personnel will be deployed, what equipment they will have available to them, and whether they can make use of the networks already installed there.

For tactical applications, the military needs radios that can be configured quickly and easily to work with any type of network. Therefore, DoD is developing the Joint Tactical Radio System (JTRS) standard. JTRS will allow one radio to be configured quickly to function in multiple spectrum bands and operational modes using a variety of signaling protocols, such as SINGCARS, Cobra, and P25. Such a radio uses software rather than hardware to configure its capabilities. The JTRS radio would be able to take advantage of any available network infrastructure, or could operate independently when necessary. The objective is a radio that can be quickly and easily configured to operate anywhere.

JTRS is still in development, and compliant systems are not widely available for general procurement. When JTRS radios become available, they will be able to work with P25 networks. Together, P25 and JTRS will go a long way in surmounting the problem of radio incompatibility.

Cooperation Is the Method—and the End Result

Standards are one piece of the puzzle. Interoperability is more than a simple question of buying a new standards-compliant system. It is an ongoing challenge of cooperation among departments, installations, services, agencies, and jurisdictions. Mounting an effective program for joint communications requires

- advance planning with each involved agency to implement one or more levels of interoperability and establish a clear sense of who will perform which tasks under which circumstances;
- preparatory training and joint exercises, including full-scale disaster simulations that give personnel the opportunity to test their communications capabilities before lives are on the line; and
- collaboration that goes beyond the mechanics of radio operation to address the wider context of communicating effectively across organizational boundaries.

As part of an overall planning effort, LMR interoperability standards such as P25 are invaluable tools for building an effective joint communications capability for homeland security and emergency preparedness. By working together, agencies can be confident in their ability to craft an interoperability strategy that fits their needs both today and in the future.

About the Author

Dennis Dibos, a vice president at Motorola, Inc., directs North American Group Safety and Security Solutions, headquartered in Washington, DC, which is focusing on homeland defense. During his career at Motorola, Mr. Dibos has worked in the Commercial, Government and Industrial Solutions Sector as operations manager for the State and Local Government Markets Division, general manager of the Federal Government Division, and distribution manager for the North America Group. He also is president of Motorola Spectrum LLC.

The following is the text of the keynote address given by Allen Beckett, Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness, at the 2003 Defense Standardization Symposium.

Keynote Address at the 2003 Defense Standardization Symposium

It is a pleasure to be here today and have the honor of presenting this symposium's keynote address. Our theme, "Standardization Enabling Coalition Interoperability," is particularly relevant as we deploy over 200,000 coalition forces into the Middle East. The current deployment highlights some of the challenges the Secretary is attempting to address through Force Transformation, particularly our goal to "project and sustain the force with minimal footprint." To achieve that goal, the DoD embarked upon the Future Logistics Enterprise to address all aspects of power projection and sustainment.

Standardization has been and continues to be critical to logistics and coalition operations. Within 30 days after the terrorist attack on the World Trade Center, coalition forces were actively engaged in Operation Enduring Freedom. What made such a phenomenal response possible was the foresight shown by the services and our allies in collectively developing common standards for fuel, munitions, information exchange, and many other areas that logistically enabled rapid coalition action. Standards will be no less important to the success of the current and future operations.

A few weeks ago, we celebrated the birthday of one of our greatest presidents, Abraham Lincoln, whose words and ideas still speak to us today. In the midst of a war that threatened the very existence of the United States, President Lincoln said, "The dogmas of the quiet past are inadequate to the stormy present….As our case is new, so we must think anew, and act anew. We must disenthrall ourselves, and then we shall save our country."

Today, we are engaged in a new kind of war—a war on terrorism. In the future, we are likely to face new asymmetrical warfare situations that will tax our military capabilities in ways we have yet to imagine. If we are to succeed, then we must heed the words of President Lincoln and begin thinking anew and acting anew because no matter what situation arises, our warfighters depend on us for the food, ammunition, fuel, and other items they need to sustain operations. This is really what the goal of the Future Logistics Enterprise is all about: ensuring that wherever we deploy our forces, we have the capabilities to deliver the right resources in the right quantities to the right place at the right time.

While the goal of the Future Logistics Enterprise is simple, making it happen is not. We have six initiatives underway to make the Future Logistics Enterprise vision a reality, and of these six, the four where I believe standardization has an important role are (1) condition-based maintenance plus, (2) total life-cycle systems management, (3) end-to-end distribution, and (4) enterprise integration.

Allen Beckett
Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness

Let's first talk about condition-based maintenance plus. Today, the DoD does not adequately predict failure on equipment. The inability to predict failure adequately has produced a large maintenance work force; diagnostic equipment that is cumbersome, time consuming, and often unreliable; and long repair cycle times that result in expensive supply pipelines. The goal of condition-based maintenance plus is to use an array of prognostic and diagnostic tools in order to reduce maintenance and logistics costs, improve equipment availability, and protect against failure of mission-critical equipment.

The implementation of this condition-based maintenance plus initiative requires the integration of a variety of hardware and software components. From a hardware standpoint, we must have sensors that can automatically track fuel, water, food, and ammunition consumption and embedded diagnostic and prognostic equipment that can detect or predict when a part is failing and requires replacement. From a software standpoint, we need to have the means of reporting this information and sharing it with the many affected stakeholders to ensure maintenance procedures are performed when necessary, and to ensure that the right tools and supplies are available at the right time and place to perform those procedures.

To do all of these things in a way that is consistent across the services and across platforms is going to require a common set of standards, preferably international, commercial standards to ensure interoperability with our allies. Having a common set of standards among the maintenance community for condition-based maintenance will drive the supplier base to producing hardware and software components that are interoperable, make it easier to upgrade system components in the future, and result in a broader supply base, which should offer more choices in technology and reduce costs.

The second Future Logistics Enterprise initiative where standardization will make a difference is total life-cycle systems management. This is a multifaceted initiative, but at the heart of it is the need for a fully integrated life-cycle development process that considers lifetime sustainment up front in the development process. That means developing and deploying systems in a manner that consciously addresses supportability, sustainment, and a reduced logistics footprint from the start and not as an afterthought. With the DoD spending about $62 billion a year on weapon system sustainment, program managers can no longer concentrate on acquisition cost, schedule, and performance at the expense of reliability, maintainability, and logistics footprint.

It's easy to see how standards and standardization can help with total life-cycle system management. To a large extent, logistics is about the management of parts—making sure parts are readily available, are of good quality, and are affordable. Every part, no matter how small, carries significant overhead costs generated by such activities as ordering, delivering, and receiving. To determine the total cost of a part, multiply these overhead cost activities by the number of times they will be performed over the entire life of a system. When you consider that the C-17 transport has 9 million parts, the F/A-18 has 750,000 parts, and the Apache helicopter has 30,000 parts, you can appreciate the magnitude of trying to supply and pay for all of these parts. The greater use we are able to make of standard parts in design of systems up front, the easier it will be to sustain that system in the future at more affordable costs.

An area where we are enjoying success in reducing our logistics footprint by careful design considerations up front is batteries. Every piece of equipment needs power to operate, and batteries are an important source of power. But batteries can come in an almost infinite number of shapes, sizes, and power outputs. It is sometimes said that when contractors design equipment, the very last part they design is the battery. Whatever space is left over after all of the other parts have been designed is the configuration the battery will assume.

But such variety makes it more complicated to anticipate the logistics needs of the operational forces. It can slow down acquisition of supplies since you are forced to deal with many more suppliers, some of which may be sole-source providers of nonstandard items. It makes the transportation system more inefficient since you have to take up precious cargo space transporting large varieties of many different items instead of fewer, standard items. The Army has taken steps to address this proliferation problem in the battery area by directing its program managers to use a limited number of standard batteries in the design of future systems and equipment.

Of course, one of the challenges that every program faces is to identify standard parts and interfaces that might meet their performance requirements. To assist both the government and contractor program offices in this task, efforts under the Joint Materiel Standards Roadmap will result in an automated program manager tool to give guidance in the selection of standard parts and interfaces. This program manager tool will give us an opportunity not only to avoid logistics support problems downstream, but also avoid a range of serious interoperability problems from the outset of deployment. It is somewhat embarrassing when in Afghanistan today, U.S. Navy fighters must be refueled in flight by Royal Air Force tankers because the U.S. Air Force tankers do not have refueling nozzles compatible with Navy aircraft. Where is the common interface standard?

Total life-cycle system management also addresses our legacy systems, which make up most of our inventory. A major source of concern today with our legacy systems is the problem of diminishing manufacturing sources, especially in the electronics area. Traditionally, military electronic systems have been largely platform unique. Because of the rapid pace of technology in electronics today and the ever-shrinking DoD share of the electronics market, we increasingly face difficulties in supporting our electronic equipment.

We need to adopt an open systems approach to supporting legacy systems, and by open systems, I mean systems that are supported by widely used industry standards that define requirements in terms of performance and interfaces. Only by using the open systems standards approach will we be able to upgrade, expand, or replace our electronic systems in an affordable way.

The third Future Logistics Enterprise initiative where standardization will have an important role is end-to-end distribution. The purpose of distribution is to provide the warfighter the right materiel at the right time and right place to support continuous combat operations. Today, the DoD distribution system comprises multiple, unsynchronized distribution points that are not harmonized at the enterprise level. The distribution environment places the tracking burden on the customer, who lacks complete information and end-to-end visibility. Such a process not only creates unnecessary work for the customer, but also a degree of uncertainty as to where an item is in the supply chain and whether it will arrive when and where needed. And if conditions change that require a rerouting of an item, that creates its own special problems.

One example of enterprise-wide effort we have underway to provide greater end-to-end distribution visibility is the Automatic Identification Technology, or AIT, program. AIT integrates a wide variety of technologies, including bar codes, magnetic strips, integrated circuit cards, optical memory, and radio frequency identification tags, and then links this identification information to satellites to track and, if necessary, redirect shipments. AIT will provide commanders information on where their assets are located so they can act with confidence in planning future operations.

The successful implementation of AIT, however, depends on standards, and this program is a classic example of how standards development and application should work throughout government and industry. Under the auspices of such major standards-developing organizations as the American National Standards Institute and the Electronic Industries Association, the DoD participates with the automotive, aerospace, telecommunications, and health industries to develop standards that are being used across industries, across government agencies, and across national boundaries, creating a level of synergy that one seldom sees.

The final Future Logistics Enterprise initiative where standardization will have an important role is enterprise integration. Within the DoD, we currently have over 600 logistics information systems that involve over 400 million lines of code. It's estimated that the DoD spends between $1.5 billion and $2.5 billion annually to support these disparate logistics systems. Many of the systems are batch processed with little or no network capability. Thus, these systems cannot provide the real-time situation awareness envisioned by Joint Vision 2020.

To achieve enterprise integration of all of the logistics information is a daunting task because of the breadth. Enterprise integration requires full integration of all of our logistics business processes, such as acquisition, maintenance, supply, contracting, financial management, and human resource management. It means moving our thinking from a narrowly focused dimension, such as supply chain management, to a more broadly focused perspective of logistics chain management, which ties together all of our logistics enterprises.

This may be the most difficult initiative we are working on today under the Future Logistics Enterprise, but this effort is vital to our overall transformation and is the enabler of all other logistics efforts. If we don't get this right, there will be no transformation, and to make sure we do get it right, we are depending on logistics business systems built to commercial standards that will cut through stovepipes to deliver common business solutions.

I'm not sure how many of you are aware that today is a very special day in U.S. history, for it was on March 4, 1789, that the United States Constitution went into effect. Perhaps one of the lesser known aspects of this remarkable document is that it contains this nation's first requirement for standards.

Article 1 of the Constitution states that the Congress shall have power to fix the standard of weights and measures. Given how important a standard set of weights and measures would seem to commerce, you would think this would have been an easy task, but it wasn't until 47 years later that Congress approved a standard set of weights and measures for the nation. And you thought it was difficult developing consensus standards across the services and with our allies.

I began my talk today by quoting a president whose birthday we celebrated last month, so let me end by quoting another birthday president from last month, George Washington. In a letter sent to the governors of the 13 states in 1783 as the Continental Army was being disbanded, George Washington wrote: "It is essential [to the defense of the Republic] that the same species of arms, accoutrements, and military apparatus should be introduced in every part of the United States. No one, who has not learned it from experience, can conceive the difficulty, expense, and confusion, which result from a contrary system."

More than 200 years ago, we appreciated how necessary and valuable standardization is for our armed forces. Yet even then, it took exceptional people with the dedication, conviction, and talent to make it happen. I know from my experience with the Future Logistics Enterprise how tough it can be to sell an idea, so I can appreciate your uphill battles in selling the standardization vision. But on behalf of the men and women in our armed forces who we send in harm's way to defend our freedom, security, and way of life, I want to thank you for the job you do. Your work is vitally important to their success, and you should be proud of what you have accomplished and what you will accomplish. Thank you.

2003 Defense Standardization Symposium Photo Gallery

Allen Beckett, Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness, was the keynote speaker at the 2003 Defense Standardization Symposium.

Stephen Gibson, Head of Standardization, Defense Standardization, United Kingdom, spoke as a member of the International Standardization Panel about the *European Standardization Handbook for Defense Procurement*.

Christopher J. Denham III (Vice President, Standards and Technology, GEIA) and Gregory Saunders (Director, Defense Standardization Program Office) partnered to produce the 2003 symposium.

Dr. Holly Dockery, Department of Homeland Security, was a member of the Homeland Security panel. Her presentation, "Homeland Security: A Progress Report," provided much information and better insight into how our nation is protecting its citizens.

Rear Admiral Jan Eriksen, Norwegian Navy, and Director, NATO Standardization Agency, NATO Headquarters, Belgium, gave a much anticipated talk—"Standardization: NATO's Force Multiplier." It was well received and very informative.

Darrell Hill, Defense Supply Center Columbus, and Joe Chapman, President, Chapman Consulting, are two key contributors to the Defense Standardization Program.

Gregory Saunders, DSPO Director, and Stephen Lowell, DSPO Deputy Director, enjoy a symposium luncheon. Mr. Saunders and Mr. Lowell are very involved with organizations that support standardization in the United States.

Our exhibitors always bring products of interest. NAVSEA's exhibit—Harnessing the Power of Technology for the Warfighter—was well represented by Gerry Thomas and Dan Quearry, Navy, Crane, IN.

Dennis Dibos, Vice President, Motorola North American Group Safety and Security Solutions, spoke on enabling coalition interoperability through standardization.

Laura Hitchcock, The Boeing Company, and Jane Schweiker, an independent consultant (formerly with ANSI headquarters) are industry partners and key contributors to the Defense Standardization Program.

Pictured above enjoying a break at the 2003 symposium are Han Lo, Defense Supply Center Philadelphia; Terence Chin, NAVAIR (Lakehurst); John Heliotis, Air Force Departmental Standardization Officer; and Frank Yelinek, NAVAIR.

Louis Kratz (Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness), Elaine Babcock (Defense Information Systems Agency's Departmental Standardization Officer), and Gregory Saunders had key roles presenting panelists and topic speakers at the 2003 Defense Standardization Symposium.

2002 Defense Standardization Program Awards

The 2002 DSP award winners demonstrated that concerted standardization efforts can result in substantial savings as well as improved readiness.

On March 4–6, 2003, **Allen Beckett**, Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness, and **Gregory Saunders**, Director, Defense Standardization Program Office, presented seven awards to recognize individuals or teams whose standardization efforts demonstrably promoted interoperability, reduced total ownership costs, or improved readiness. ▮ The 2002 Distinguished Achievement Award, which includes an engraved crystal Pentagon and a check for $5,000, went to **Martin L. Snyder**, Department of the Army, Tank-Automotive Command, Warren, MI. Mr. Snyder led the development of a new, multivolt IR-secure blackout drive lamp that puts enough light in front of military vehicles, while minimizing the chance of detection. Based on light-emitting diode technology, the new lamp meets all requirements of NATO Standardization Agreement 4381, enabling interoperability with NATO forces. The lamp will fit all tactical vehicles, all commercial construction equipment with drive lamps, and some major combat vehicles. ▮ Not only can the new lamp be used on many different platforms—standardization was a key project goal—but it is safer, less expensive, and more reliable than the old drive lamps. It is safer because it gives the soldier/driver enough light, reducing the chance of accidents and, therefore, the number of injuries, both in peacetime and times of conflict. It costs only $50, compared with about $90 for the old lamps. And, the new lamp has an estimated operating life of 100,000 hours—a significant feature, considering that old lamps sometimes fail during the first week of operation. All of those benefits add to a significantly reduced logistics footprint and, most important, improved readiness.

’02 Defense Standardization Program Awards

Martin Snyder, winner of the 2002 Distinguished Achievement Award, receives a check for $5,000 from presenter Gregory Saunders.

The six other winners were as follows:

- A team from the ARMY’S COMMUNICATIONS AND ELECTRONICS COMMAND (Gerard Boyan, ARINC; Kenneth Capolongo, Army; John Klubnick Sr., Aspen Consulting; John Lippert Sr., Aspen Consulting; Lisa Russo, Army) developed a tool to test and diagnose data buses built to MIL-STD-1553. The tool, known as the Advanced Multiplex Test System (AMTS), is faster and more accurate than existing 1553-based test sets and can be used by all U.S. services and allies on any assets with 1553 data buses. Deploying a single standardized tool for testing all 1553-based electronics systems will significantly reduce the logistics footprint; no longer will the services need multiple 1553 test systems. Enhanced readiness also is a key benefit. Because AMTS permits onboard testing, maintainers can diagnose problems, make repairs, and get assets back into action faster. AMTS’s economic payoff is huge—potentially several hundred million dollars. In the pilot program, the AMTS was fielded to the Army’s Apache Longbow helicopter fleet at a cost of less than $3 million, and the 6-year projected payoff is more than $10 million.
- Stephen Daniel, Navy, and George Halak, BAE Systems, were instrumental in the success of a NATO SPECIALIST TEAM formed to produce an architectural standard for tactical unmanned air vehicles. The standard—*NATO Standardization Agreement (STANAG) 4586 Standard Interfaces of the Unmanned Control System (UCS) for NATO UAV Interoperability*—identifies the protocols, message formats, and other parameters that must be used in ground control systems so that they can operate multiple types of unmanned air vehicles. Use of a standardized control system to operate UAVs not only promotes joint service, multinational UAV interoperability, but facilitates shared development of components, among other things. Mr. Daniel and Mr. Halak coordinated and ensured government and industry support and participation. Their work resulted in multinational consensus about the new standard—10 nations intend to ratify it. In addition, they obtained buy-in from a broad industrial base—21 companies from 8 nations.
- A JOINT TEAM (Bob Billmyre, Army; R. David Curfman, Navy; Richard Paradis, Navy; Larry Spangler, Air Force; Maria Swift, Navy) developed a contract that enables Army, Navy, and Air Force architects and engineers to use the Internet to view, print, and download non-government standards (NGS) established by organizations such as the American Society for Testing and Materials and the American Society of Heating, Refrigerating, and Air-Conditioning Engineers. The task involved identifying organizations whose standards are referenced in the criteria, standards, and specifications developed by the military services for facilities planning, design, construction, operation, and maintenance. The team also took the opportunity to

Pictured above are members of the team that developed the Advanced Multiplex Test System. The team members are Gerard Boyan, Kenneth Capolongo, John Klubnick Sr., John Lippert Sr., and Lisa Russo. They are shown with Louis Kratz, DoD Standardization Executive; Richard Pribyl, Chief, Airborne NAVCOM Division; Edward Wuyscik, CECOM Software Engineering Center Supervisor; Stephen Kovacs, Deputy Director, CECOM Software Engineering Center; and Anthony LaPlaca, Director of the Logistics and Readiness Center (CECOM). Also accompanying the team are Karim Abdian, Army Departmental Standardization Officer, and Harold Barnett, Army Standardization Executive.

George Halak and Stephen Daniel show their plaques for the work they did on NATO STANAG 4586. Also shown are Captain Dennis Sorenson, PMA 263 Program Manager; Greg Catrambone, PEO Deputy for UAVs; Jeff Allen, NAVAIR Command Standardization Executive; and Allen Beckett, Principal Assistant Deputy Under Secretary of Defense for Logistics and Materiel Readiness.

Bob Billmyre, R. David Curfman, Richard Paradis, Larry Spangler, and Maria Swift are members of the joint team that developed a contract enabling military architects and engineers to use the Internet to view, print, and download non-government standards. They are accompanied by Dr. James Wright, NAVFAC, and Richard Brittingham, Senior Accounts Manager for IHS, Inc. The group is flanked by Louis Kratz and Allen Beckett.

Pictured above are the winners of the joint Air Force and Navy team that developed and published *Airworthiness Certification Criteria*. The team members are Susan Breslin, Fernando Falasca, Robert FitzHarris, Susan DeGuzman, and Robert Hanley. They were accompanied by John Heliotis, Air Force Departmental Standardization Officer; Scott Kuhnen, Air Force Command Standardization Officer; James Engle, Air Force Standardization Executive; Commander Scott Howe, Navy; Carlotta White, Navy Standardization Office; and Jeff Allen, NAVAIR Command Standardization Executive. The group is flanked by Louis Kratz and Allen Beckett.

Pictured above are members of the joint Air Force and Navy team that developed CMBRE. The team members are William Cannington, Rick Foulk, Margaret Villagran, Raymond Holden, and MSgt G.B. Thomas (not at ceremony). Also shown are Louis Kratz; Allen Beckett; Carlotta White, Navy Standardization Office; James Engle, Air Force Standardization Executive; John Heliotis, Air Force Departmental Standardization Officer; and Scott Kuhnen, Air Force Command Standardization Officer.

Abdonasser Abdouni displays his plaque. With Mr. Abdouni are Bill Lee, DLA Departmental Standardization Officer; Darrell Hill, Chief, Sourcing and Qualification Unit; Samuel Merritt, Chief, Standardization Division; Dave Moore, Chief, Document Standardization Unit; Ronald Bayless, Director, Operations Support Group; Frank Lotts, then Deputy Director, HQ DLA Logistics Operations; and Christine Metz, DLA Standardization Executive. The group is flanked by Louis Kratz and Allen Beckett.

unify the military specifications, continuing the process of eliminating single-service specifications and contributing to DoD's goal to maximize the use of NGS. Easy access to up-to-date facilities-related NGS significantly increases productivity, resulting in direct savings of $800,000 annually. In addition, DoD expects substantial savings that are difficult to quantify, such as reduced construction, acquisition, and engineering costs.

- AN AIR FORCE AND NAVY TEAM (Susan Breslin, Air Force; Susan DeGuzman, Navy; Fernando Falasca, Air Force; Robert FitzHarris, Air Force; Robert Hanley, Navy) developed and published *Airworthiness Certification Criteria* (MIL-HDBK-516)—a concise, consensus-based set of assessment criteria that apply to all fixed-wing aircraft systems. MIL-HDBK-516 addresses 15 key technical areas and contains more than 700 criteria that must be addressed to ensure safety. In addition, MIL-HDBK-516 cross-references the airworthiness criteria to the technical performance requirements contained in the joint service specification guides and Federal Aviation Administration documentation. Standardizing the airworthiness certification criteria eliminates the need for each military service to recertify the airworthiness of an aircraft, which in turn eliminates the needless consumption of limited resources (manpower, financial, schedule). Certifying the airworthiness of a single aircraft can easily exceed $1 million. Eliminating the need for recertification results in substantial savings. It also reduces response times, which translates directly to increased readiness.

- AN AIR FORCE AND NAVY TEAM (William Cannington, Air Force; Rick Foulk, Air Force; Raymond Holden, Navy; MSgt G.B. Thomas, Air Force; Margaret Villagran, Air Force) developed equipment that can test and reprogram the latest generation of smart weapons defined by MIL-STD-1760. The equipment—Common Munitions Built-In Test Reprogramming Equipment, or CMBRE—is small, lightweight, computer-controlled, and easy to use. With CMBRE, warfighters can ensure that the smart munitions loaded on combat aircraft are mission ready. The equipment is highly reliable, enhancing readiness. In Kosovo, the mean time between failures for CMBRE was 8,892 hours, exceeding contract requirements by some 4,000 hours. The standard tester eliminates the need to have weapon-unique support equipment, reducing the logistics footprint and saving DoD several million dollars through, for example, reductions in training and spares, as well as the elimination of weapon-unique support equipment. Also, CMBRE increases interoperability. Initially, the equipment is being used with three munitions, but CMBRE can be used on numerous other MIL-STD-1760 munitions. It also can be adapted for use on some non-MIL-STD-1760 munitions.

- Abdonasser Abdouni, Defense Logistics Agency, Defense Supply Center, Columbus, contributed significantly to improving MIL-DTL-38999, the specification on circular electrical connectors. In one effort, he worked closely with a Society of Automotive Engineers committee to solve a connector vibration problem that resulted in jet engine shutdown. Mr. Abdouni also led a major effort to overhaul MIL-DTL-38999 and its specifications sheets. That effort required completing 59 DoD standardization projects, upgrading technical requirements, and streamlining qualification and conformance testing, among other things. The result is an up-to-date circular connector specification that reflects DoD's requirements for state-of-the-art connectors. MIL-DTL-38999 applies to more than 10,000 standard connectors in the DoD inventory system and affects 130 critical military weapons systems. The updated specification also allows connector manufacturers to use best practices. Mr. Abdouni's work improves the performance and availability of standard connectors and directly supports interoperability and readiness of existing military systems.

August 10–14, 2003, New Orleans, LA

SES Holds Its 52nd Annual Conference—Standards Trends: Emerging, Converging, and Diverging

The Standards Engineering Society is holding its 52nd Annual SES Conference at the Royal Sonesta Hotel in New Orleans, LA, August 10–14, 2003. The event features complimentary tutorials on Standards 101 and the SES Certification Program on Sunday, August 10. On Monday at 9:15 A.M., William H. Lash III, Assistant Secretary for Market Access and Compliance, International Trade Association, will give the keynote address, "Setting the Standard: The Department of Commerce Plan to Improve Market Access by Fighting International Standards Barriers," followed by Gregory Saunders, Director, Defense Standardization Program Office, speaking on "Homeland Security Standards—What's At Stake." On Tuesday, Stephen Lowell, Deputy Director, Defense Standardization Program Office, will be introduced as the incoming SES President. For more information, please visit www.ses-standards.org/content/conference.html.

September 1–3, 2003, Canberra and Sydney, Australia

EIA Presents the Ninth Annual World Electronics Forum

EIA is holding the Ninth Annual World Electronics Forum on September 1–3, 2003, in Canberra and Sydney, Australia. The World Electronics Forum (WEF) is a voluntary gathering of electronics industries association leaders to which the EIA is secretariat. Founded in 1995, the forum meets annually to discuss topics of interest, exchange information on services and data, and strengthen relations between associations to benefit the high-technology industry worldwide. For more information, please visit www.eia.org/events.

People in the Standardization Community

New Standards Executive, Aeronautical Systems Center, Air Force Materiel Command

With the recent departure of Gary Adams, Mark Wilson, a senior-level executive, is now the Technical Adviser, Systems Engineering, Engineering Directorate, Aeronautical Systems Center (ASC). Mr. Wilson provides senior technical leadership for all engineering personnel and represents the U.S. Air Force on the Aviation Engineering Board for the Joint Aeronautical Commanders' Group. He also serves as the engineering representative on acquisition strategy panels at the Headquarters, U.S. Air Force, and ASC levels. In his new position, Mr. Wilson now serves as Center Standardization Executive for ASC.

Mr. Wilson earned a master of science degree in management (Sloan Fellowship) from Stanford University and a master of science degree in management science from the University of Dayton. He received his bachelor of science degree in 1971 (aerospace engineering) from Purdue University.

Mr. Wilson is the recipient of the Secretary of the Air Force Lightning Bolt Award, the John J. Welch Jr. award for excellence in acquisition management, and, in 2001, the Exemplary Achievement Award.

Mr. Wilson is an Associate Fellow, American Institute of Aeronautics and Astronautics; a member of the National Defense Industries Association; a member of the Executive Government Steering Group for NDIA Systems Engineering Division; Cochair, NDIA Systems Engineering Division, Systems Engineering Effectiveness Committee; and a member of the International Council on Systems Engineering Airlift and Tanker Association.

We welcome his active participation in the standardization community. He has championed the Air Force's move to reinvigorate Systems Engineering and is helping to formulate the Systems Engineering Center.

Honoring Oliver Smoot

Recently, Oliver (Ollie) Smoot, newly elected president of the International Standards Organization (ISO), was honored with a reception on Capitol Hill. The Honorable Ralph M. Hall of Texas, in the House of Representatives, recognized Mr. Smoot by saying, "Mr. Speaker, I rise today for myself and for Chairman Boehlert of the House Committee on Science to recognize Oliver R. Smoot, vice-president for external voluntary standards relations at the Information Technology Industry Council, as he begins his term as the President of the ISO. It is a high honor and a major achievement to be asked to be the leader of the world's standards community but it is not surprising that Ollie Smoot is the one chosen. Mr. Smoot has long been a pillar of the standards community, most recently as President-elect of the ISO and as Chairman of the American National Standards Institute, the organization which represents the United States in international standards matters and oversees the establishment of U. S. national standards."

Representative Hall continued to praise Mr. Smoot and ended his remarks by saying, "Oliver Smoot is a great American who has labored long for the betterment of science and the global economy and I am pleased that this week he is getting long-deserved recognition of this service."

The defense standardization community joins Congress in wishing Ollie all the best and hopes for a great term as the newly elected president of the ISO.

Reassignments

Stephen Lowell has been appointed as the new Deputy Director, Defense Standardization Program Office, replacing Andy Certo, who recently retired. Steve has been a staff member of the Defense Standardization Program Office since the early 1980s and is considered a valuable asset to the office. Congratulations, Steve!

Al Stanley, Air Force Metrology Calibration Program, Warner-Robins Air Force Base, recently retired, and we wish him well. Taking his place is Stephen Hooper. We look forward to working with Mr. Hooper.

Dave Britton, former chief of the ASC Information Management Branch (which contained the

ASC/Air Force Research Laboratory Engineering Standards Office, Air Force Code 11), was reassigned to the C-17 System Program Office as the Mission Planning integrated process team lead. Dave had served as the chief of the function since August 1997 and was recognized with a team of standardization personnel within the Air Force Materiel Command to receive the Defense Standardization Program Outstanding Achievement Award in 1998. Good luck Dave!

Edward C. "Pete" Aldridge Jr. retired May 23, after serving the Defense Department in various assignments over 18 years of a 42-year career in the defense arena. We will remember Mr. Aldridge for his work in championing acquisition reform at DoD. Until a permanent replacement is named, Mr. Aldridge's principal deputy, Michael W. Wynne, will serve as the Acting Under Secretary.

Fond Farewell

Karin Allen, a 34-year civil servant, has retired. She had more than 23 years with the Army Materiel Systems Analysis Agency (AMSAA) at Aberdeen Proving Ground. Karin began her career at the Bainbridge Naval Training Center, MD, as a GS-02 file clerk, and had the good fortune to work 4 years for the Army Dependent School in Hanau, Germany. After returning stateside, she went to Fort Hood, TX, where she worked for the Training and Doctrine Command's Combined Arms Test Activity. During her tenure with AMSAA, she was given challenging opportunities and was able to earn a bachelor of science degree in computer science and a master of business administration degree. Her career highlights include serving as the head of the U.S. delegation to the NATO Battlefield Maintenance Working Party; managing AMSAA's computer facilities; working on efforts in the Defense Standardization Program, including leading a team for Army specifications and standards reform initiatives; and working on reliability issues for the Future Combat Systems.

Karin has always been a pleasure to work with, and she well represented the Army at meetings, working groups, and other mission-related assignments. Karin wrote that "the hardest part about going out to start the 'good' retirement life, is leaving my wonderful friends and valued colleagues behind." She will be much missed, and we wish her the best.

Passings

Donald Mitchell, former Deputy Director of the Defense Materiel Specifications and Standards Office (DMSSO), died January 5, 2003. One of the grand old gentlemen of the standardization program, Don was responsible for many innovations in the cataloging and standardization fields, and he was a respected expert, patient teacher, and ardent advocate of standardization. Those of us who had the opportunity to work closely with Don will never forget his dogged determination and dedication to the work he loved, his enjoyment of travel, his sometimes loud "discussions" (when he had his hearing aid turned down), his corny sense of humor, his wonderful artwork, and his duets with Les Fox, the DMSSO Director. Don was a jewel, and we miss him.

Don and his wife Betty were on a cruise (he finally made it to all seven continents—his lifetime wish) when he passed away. He went into a coma in his sleep and died the next morning from complications brought on by Parkinson's disease.

Just 6 days earlier, while dining with a group of friends, Don clinked his fork against his water glass and made the announcement that he just wanted to share with his friends that he felt he'd had a terrific life. He told them that he'd grown up a poor boy in the little town of Beaver Falls, PA, had worked to help support his family, and had put himself through college and gotten a terrific job. He also noted that he'd had two lovely wives and a nice family and that he'd just accomplished his lifetime dream of visiting all seven continents with his lovely wife Betty. Betty says that he died a happy man. His ashes will be interred at Arlington Cemetery.

Editor's Corner

Sharon Strickland
Defense Standardization Program Journal

Farewell, for when this issue reaches many of you, I will be retired. I drafted this column many times, and it was very hard for me to type out "farewell." I have loved being a member of the defense standardization community and have truly enjoyed being editor of *The Standardization Newsletter* and then, along with Greg Saunders, creating the *Defense Standardization Program Journal* and serving as its editor. Both were labors of love. The *DSP Journal* is a quality magazine. I leave it in good hands, and I expect our readers to continue supporting it with quality articles. Entertainer Dean Martin always closed his television show by saying,"keep those cards and letters coming in." I ask you to do the same.

My August 1 retirement closes out a 37-year federal career. I have "come a long way, baby" since I listened to John F. Kennedy call my generation to civil service. We baby boomers are now retiring and turning our work over to a younger work force. We wish them well in all endeavors.

I began my career at the General Services Administration in July 1966 and moved to DoD in 1986. I never looked back. The future only brought more exciting projects. And I met remarkable people along my journey, had my hand kissed by an emperor, worked with celebrities, and traveled. I feel truly grateful for having had a civil service career. I leave with a happy heart and with pride for work completed. Karin Allen (Army Aberdeen, who retired on July 1) and I often shared stories as we prepared to retire. She wrote the following to me, and I feel the same way: "Having a civil service career where the emphasis was always on ensuring that the troops have the safest and best equipment has always been both humbling and rewarding. Serving my nation has indeed been a privilege." I can't write any comment better than that.

My husband and I are looking forward to more family time, church work, travel, gardening, softball, and classes and community outreach programs—the freedom of retirement. Come by or call me for lunch!

Sharon Strickland

Upcoming Issues—
Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme	Deadline for Articles
January–March 2004	Army Standardization	August 15, 2003
April–June 2004	Logistics	November 15, 2003
July–September 2004	Standardization and Contracting	February 15, 2004
October–December 2004	Navy Standardization	May 15, 2004

If you have ideas for articles or want more information, contact the Editor, *DSP Journal*, J-307, Defense Standardization Program Office, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.

dsp