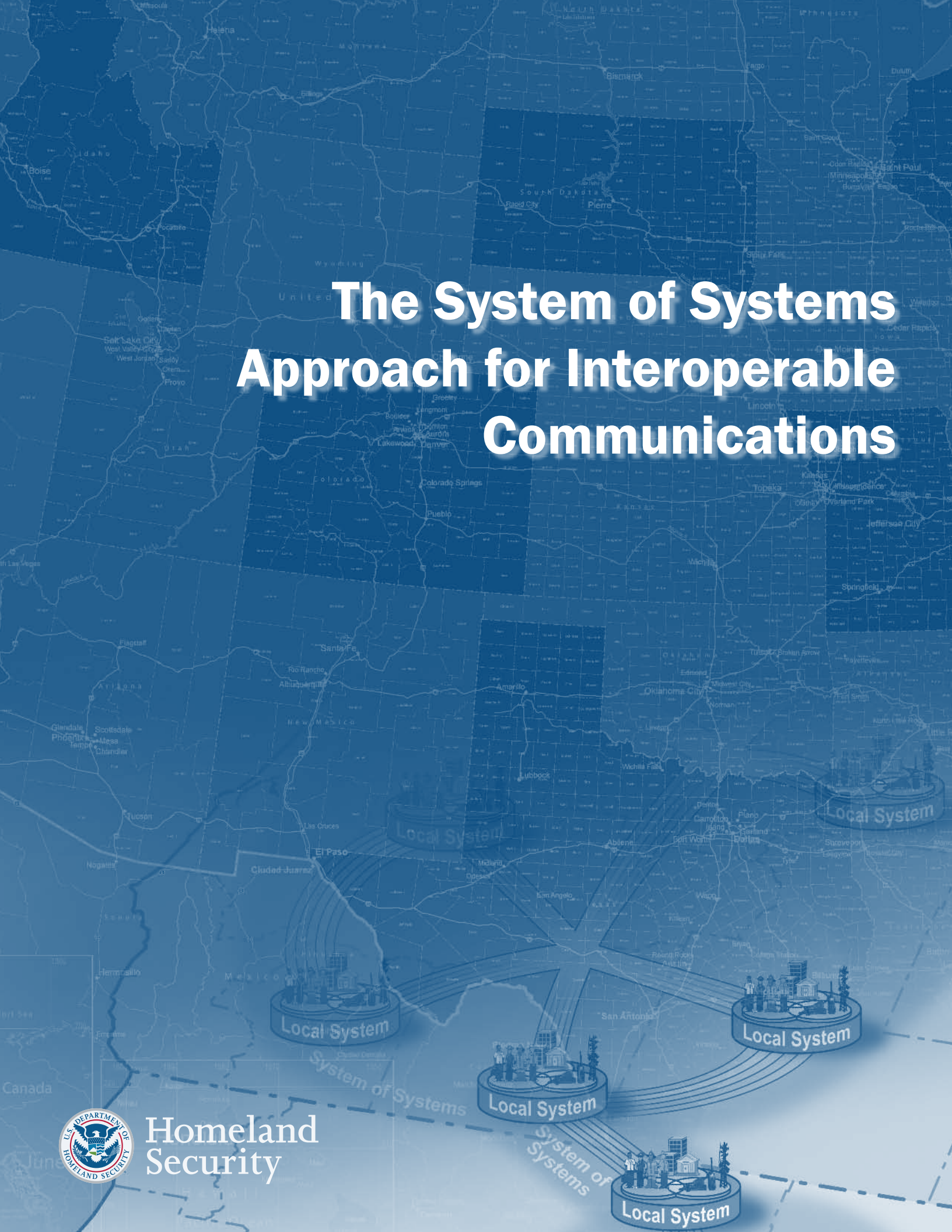
The System of Systems Approach for Interoperable Communications



Homeland Security


Local System
Local System
Local System
Local System
Local System
System of Systems
System of Systems

System of Systems Definition:

A system of systems exists when a group of independently operating systems—comprised of people, technology, and organizations—are connected, enabling emergency responders to effectively support day-to-day operations, planned events, or major incidents.

For many years, the public safety community has used a system of systems approach to achieve interoperable communications. A successful system of systems relies on the following fundamental concepts:

- Systems are composed of human, technological, and organizational components.
- Relationships among governance, technology, standard operating procedures, training, and usage are important to a successful system of systems implementation.
- Systems are independently operated and managed and can connect with other systems without losing this independence.
- A system of systems expands beyond local geographical boundaries.

This brochure was assembled using a practitioner-driven process, leveraging the knowledge and years of experience of public safety and public service practitioners nationwide. It is designed to help the emergency response community, as well as local, tribal, state, and Federal policy makers, understand the system of systems concept, the benefits of applying this concept, and how it can aid agencies in achieving interoperability. While the notion of system of systems is not new, this brochure provides the public safety community with an introduction to the concept and reflects the movement away from describing interoperability only in terms of technology.

This brochure describes:

- A definition for system of systems.
- How a system of systems supports expansion.
- The importance of relationships among governance, standard operating procedures, technology, training and exercises, and usage (the five lanes of the Interoperability Continuum).
- Effective technology planning using a system of systems approach.
- Real-life examples of how a system of systems has improved interoperability.

Defining a System of Systems for Public Safety and Public Service Agencies

A system of systems exists when a group of independently operating systems—comprised of people, technology and organizations—are connected, enabling emergency responders to effectively support day-to-day operations, planned events, or major incidents.

Figure 1 depicts a system of systems in practice. In this scenario, independent systems are *inter*dependently related within and across all lanes of the Interoperability Continuum (governance, standard operating procedures, technology, training and exercises, and usage). Compatible technology between jurisdictions alone will not make an agency interoperable; the jurisdictions must connect technology, people, and organizations to achieve interoperability.

More information on the Interoperability Continuum can be found at www.safecomprogram.gov.

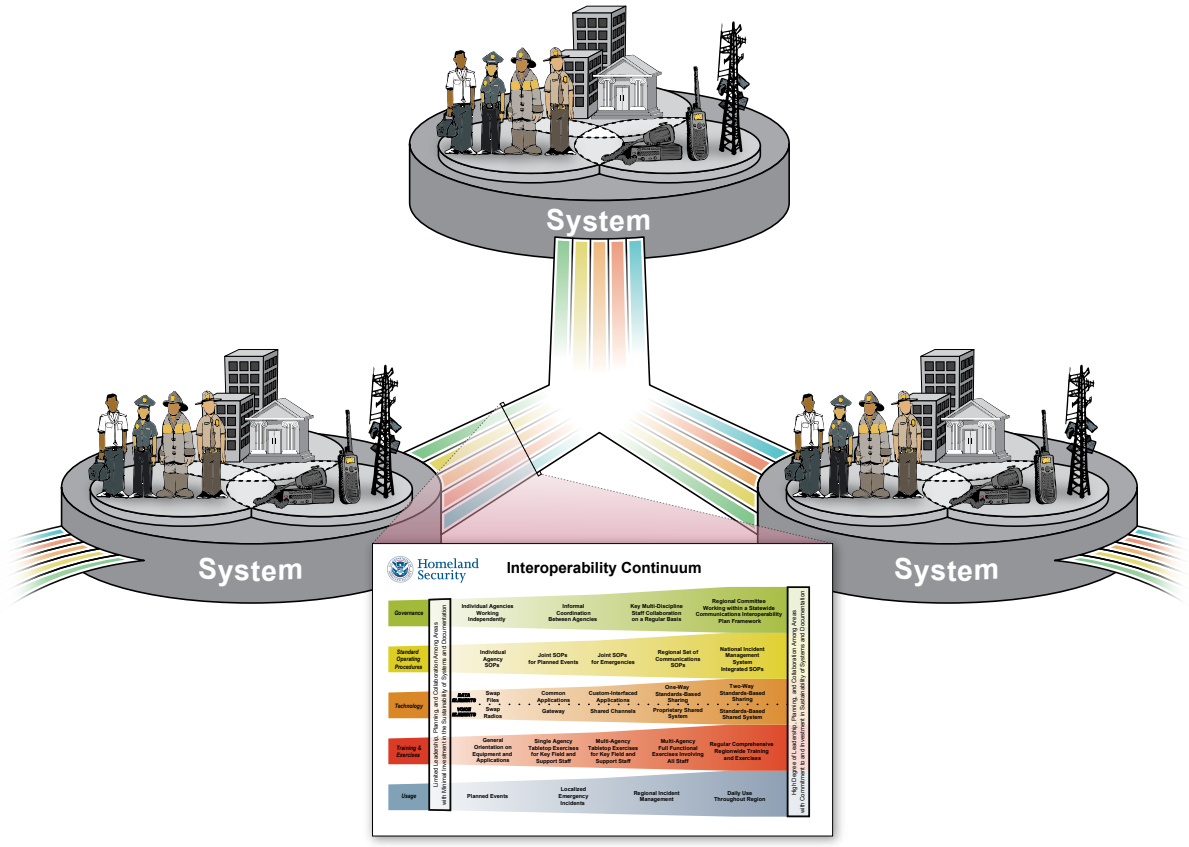


Figure 1: System of Systems in Practice

Expanding a System of Systems

A system of systems approach relies on a local agency's ability to own and manage an independent system while collaborating with other local, regional and state systems. Figure 2 illustrates local, regional, state, and interstate system of systems expansion and collaboration. Communities must consider the demographic and topographic differences of neighboring jurisdictions as they connect or share systems across their own boundaries.

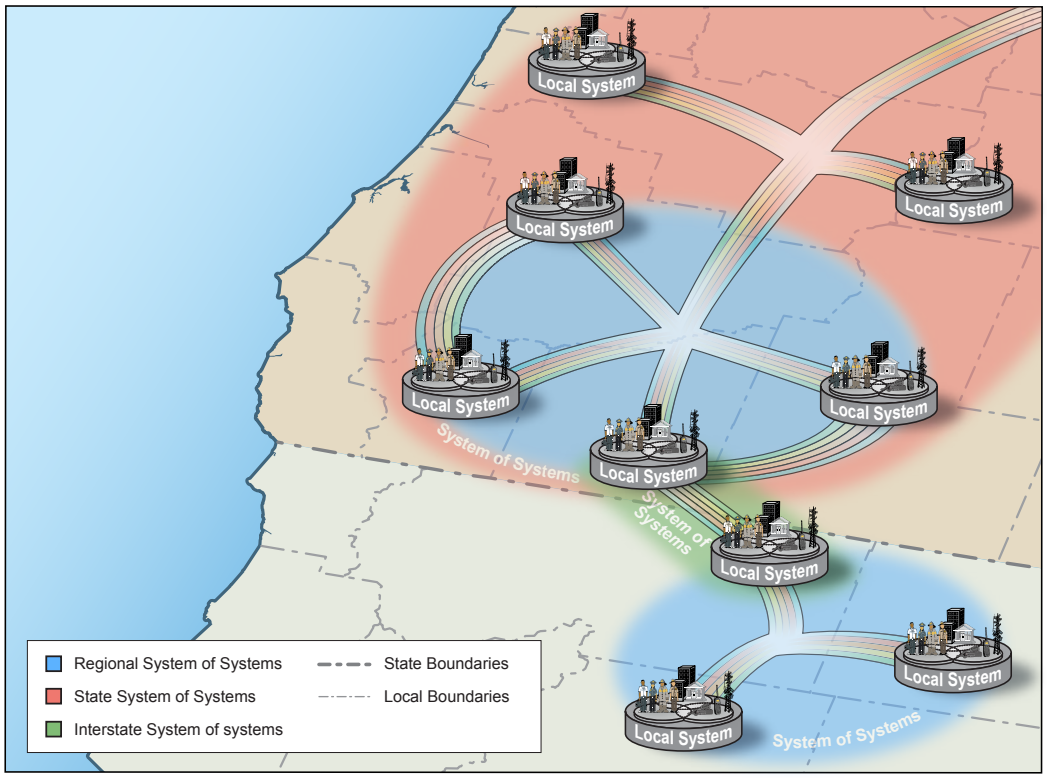


Figure 2: The Expansion of System of Systems

Establishing the Foundation for a System of Systems

Since human, organizational, and technological factors influence public safety communications, a comprehensive system of systems approach involves all lanes of the Interoperability Continuum and their relationships with each other. Strong relationships between the lanes are the foundation for the successful implementation of a system of systems.

Figure 3 illustrates how each lane of the Interoperability Continuum interacts with the other lanes in the system of systems concept. Following the logic of Figure 3, this example demonstrates lane interactions: Standard operating procedures (SOPs) are developed to support the use of technology—SOPs are often developed or vetted by governance committees—and training and exercises put technology and SOPs to use.

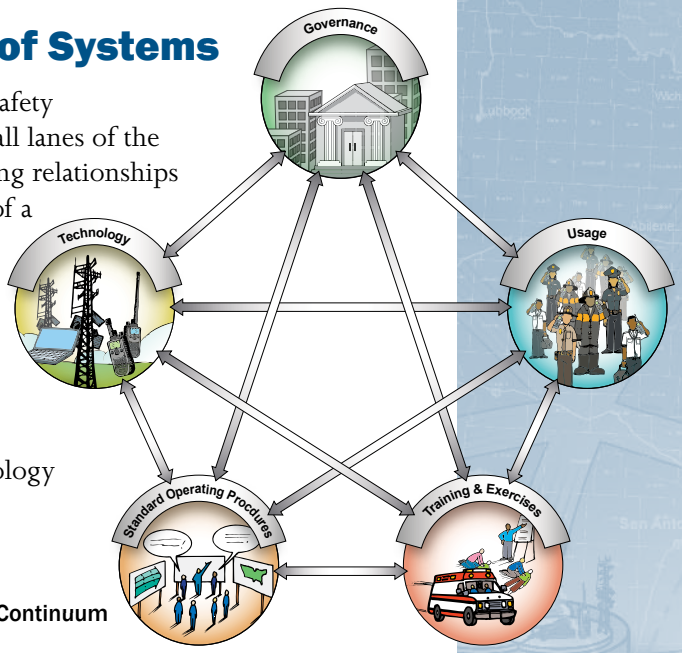


Figure 3: Connections and Relationships among the Lanes of the Interoperability Continuum

Addressing Evolving Technology in a System of Systems

Public safety technology changes rapidly, forcing decision-makers to face the challenge of making the right decisions for their agency. With multiple technologies available—land mobile radio, wireless data, information systems, and a mix of standard and proprietary technologies—it is important for jurisdictions to approach technology planning with people and organizations in mind. Agencies should use their connections and relationships with other agencies and jurisdictions to help drive current and future technology decisions. When agencies work together with their public safety neighbors, they are better positioned to adapt to changing technology and achieve interoperability among multiple independently owned and operated systems.

A System of Systems Approach in a Rapidly Changing Wireless Environment

As technology changes, a system of systems approach allows people and organizations to more effectively adapt to the changing needs of multiple agencies.

Using a system of systems approach, planners are able to consider how technology is evolving to maintain system connections and overcome the challenges associated with differing purchasing cycles, training cycles, and various levels of practitioner knowledge or experience. While independent systems will mature at different rates in a system of systems, this approach allows for greater consideration for backwards-compatibility, training programs for multiple equipment types, and standard technical interfaces.

Figure 4 illustrates the evolution of technology in the near-term future. Traditionally, voice and data communications have required separate user devices and sometimes separate networks. In the near-term future, user devices are evolving to allow for both data communications and non-critical voice communications. In the long-term future, voice and data convergence is likely to increase, and new high bandwidth applications will be introduced. As these changes occur, it is increasingly important that communities coordinate at a technical and organizational level in both planning and procurement.

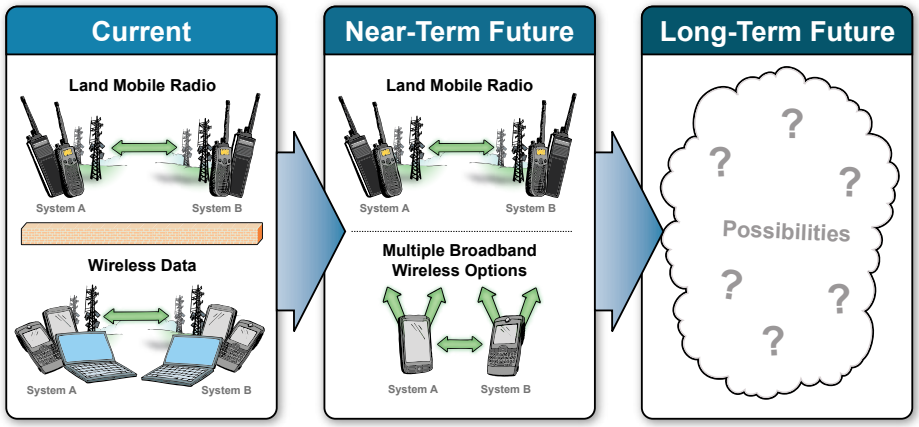


Figure 4: Evolving Wireless Technologies for Public Safety

A System of Systems and Information Sharing

In addition to addressing wireless technology, public safety agencies must also consider the challenges and importance of linking information systems including Computer-Aided Dispatch, Records Management, Crime Analysis, Hospital Capacity, and Crisis Management systems, among many others. As with wireless communications, many agencies have procured information systems that are incompatible with systems used by other agencies or neighboring jurisdictions.

When using a system of systems approach, multiple agencies and jurisdictions collaborate to identify the most appropriate means of sharing information while ensuring successful implementation and sustainability. Agencies develop joint information sharing methods, develop interagency agreements, address mutual security and privacy needs, and develop requirements to meet joint operational needs.

A System of Systems and Standards

Communication improves as agencies, large and small, join together to interoperate. No single solution exists to connect independent systems but standard interfaces can aid in integrating previously incompatible equipment. Connecting systems with standard interfaces has the following operational, technological, and economic advantages over connecting systems using proprietary interfaces:

- Increased Operational Benefits – As standard systems and subscriber devices proliferate, emergency responders can respond anywhere, bring their own equipment, and operate on any network immediately, when authorized.
- Increased Capability – Systems based on standards can connect to other systems without compromising functionality.
- Increased Efficiency – The need for additional equipment and technical resources to improve interoperability decreases.
- Increased Flexibility to Upgrade – Each system can make changes or adopt new technology without affecting other connected, standards-based systems.
- Decreased Reliance on Proprietary Technology – Jurisdictions can choose from multiple vendors.
- Decreased Cost – Price competition increases and the need for expensive customized interoperability solutions is reduced. Training can be standardized across jurisdictions, thus reducing training costs.
- Increased Capacity to Expand – Standards-based solutions are more likely than proprietary solutions to be able to integrate the *next* system into the larger system of systems.

Whether or not standards exist or are available, a system of systems approach supports each agency's ability to think outside its jurisdictional boundaries. Each agency can see itself as a component in a regional and nationwide system of systems connected through compatible equipment as well as collaborative approaches toward a common goal.

Case Studies

Assessing the Operational Impact of a System of Systems Approach

The following case studies are provided to demonstrate how previous challenges for the National Capital Region and Central Nebraska were overcome by creating a seamless system of systems.

National Capital Region (NCR)

Before: Lack of Interoperability Hinders Response after Airline Crash

In January 1982, during a heavy snow storm, Air Florida Flight 90 crashed during take-off from National Airport in Washington, D.C. The plane hit the 14th Street Bridge and plunged into the Potomac River, killing 78 people, including four motorists on the bridge. Because of the location of the incident, multiple local, state, and Federal emergency responders were dispatched to the crash site. Upon arrival at the crash site, the majority of responders from the various Virginia, Maryland, Washington D.C., and Federal agencies could not communicate with each other, resulting in a chaotic response.

Like many agencies across the country, jurisdictions in the National Capital Region (NCR) had developed "stovepipe" systems operating on different frequencies unable to communicate with each other. Most fire departments operated on VHF, many police departments operated on UHF, and Federal responders operated on yet another frequency band. While a single mutual aid channel did exist for fire and one for police, usage of these channels was not wide spread or effective during the incident. Prior to this crash, discussions about the need for a unified response across jurisdictions and state boundaries had not been at the forefront of emergency response agendas. The crash made it evident that there was a need for collaboration and coordination across the NCR.

After: 25 Years of Teamwork & Integration Tested in One Terrorist Attack

Investigations and hearings that followed the Air Florida crash pointed to communication shortfalls within the emergency responder community. The recognition of these shortfalls led to the allocation of new radio spectrum and the realization that the NCR desperately needed radio interoperability across jurisdictions. This increased focus and awareness mobilized stakeholders across the region to improve communications and increase coordination through multiple governance organizations, including the Federal Communications Commission (FCC) Region 20 Regional Planning Committee (RPC) and the Metropolitan Washington National Capital Region Council of Governments (COG). These organizations integrated technology and many emergency response procedures such as: common unit identifiers, standardized radio terminology, standardized radio channel/talk-group programming, and uniform SOPs. The group refined initial aid and mutual aid agreements, implemented regional training, and

adopted the National Incident Management System Incident Command System, a standardized incident organizational structure for the management of all emergencies.

The resulting connections and relationships allowed jurisdictions to better integrate a set of independently owned and operated regional systems, and allowed responders to utilize neighboring systems when necessary. Various subcommittees within the COG, composed of fire response, police operations, and communications personnel, actively addressed the technical and operational needs for providing more effective initial aid and mutual aid response.

The terrorist attack on the Pentagon on September 11, 2001, tested the effectiveness of years of regional planning, collaboration, and system of systems integration to support a large-scale mutual aid response.

> *While no emergency response is flawless, the response to the 9/11 terrorist attack on the Pentagon was mainly a success for three reasons: first, the strong professional relationships and trust established among emergency responders; second, the adoption of the Incident Command System; and third, the pursuit of a regional approach to response.*
>
> *– The 9/11 Commission Report*

By September 11, 2001, a majority of the local agencies in the NCR had transitioned to 800 MHz digital trunked systems. The agencies, through the COG and the RPC, had carefully planned frequency assignments, granting access for responders to other agencies' systems. This access was complemented by initial aid and mutual aid agreements, common naming conventions, and the use of plain language instead of coded language during radio transmissions; in addition, regional training exercises were developed to put the technology to use. Because of the location of the attack on the Pentagon, the Arlington County Fire Department assumed the initial incident command. Communications among local emergency responders from different agencies was highly effective, but there were technical communications problems between the local and Federal responders—the Federal responders were neither informed of the regional standard operating procedures established by the COG members, nor were their radio systems compatible with those within the NCR. Today, the inclusion of Federal representatives in the local Council of Government committees helps to address these issues. To temporarily resolve the problem, following the attack a large cache of radios was delivered on-site to support communication needs of responders not integrated into the local system. This radio cache concept was later developed into a more formal regional radio cache approach to support events that require response from agencies that are not normally engaged in day-to-day regional response.

The lessons learned over the 19 years after the Air Florida crash helped establish a comprehensive wide-area interoperable system of systems used everyday to serve 12 jurisdictions and protect approximately eight million people. The September 11 response is evidence of their successful collaboration.

More details on the Pentagon response can be found in *The 9/11 Commission Report*. Further details on communications during the Pentagon attack (including a brief description of the Air Florida crash) can be found in *Answering The Call: Communications Lessons Learned From The Pentagon Attack*, developed by the Public Safety Wireless Network (PSWN) program and available on the SAFECOM Web site (www.safecomprogram.gov).

Central Nebraska

Before: Jurisdictional Boundary Issues Prevent Communication

Like many agencies across the nation, agencies in the Central Nebraska region developed individual radio systems for specific use and geographic support. The lack of interoperability affected agencies at every level—from the most routine radio runs to large-scale emergency situations. If mutual aid was required, there was no established SOP or mutually agreed upon policy on how agencies could assist each other.

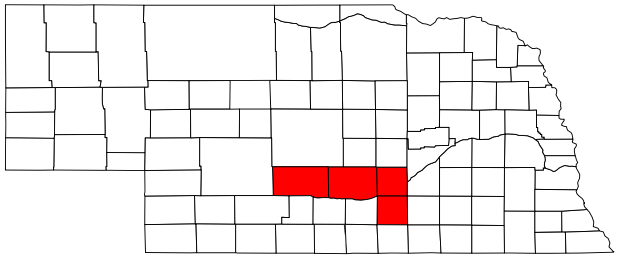
The lack of interoperability was most felt during day-to-day operations, and magnified during emergencies. Several events illustrated why the regions needed to begin thinking about cross-jurisdiction interoperability:

- Following an automobile accident, both State Patrol officers and local agencies within the region responded. A State Patrol officer on one side of the interstate and an emergency responder from the local sheriff's department on the other side could not communicate.
- When an inmate escaped during transport to a prison facility, the sheriff's deputy could not communicate with the corrections officers on the state system through his local network.
- Buffalo County flight helicopters serve a wide region, reaching into Denver and Kansas, but couldn't talk to responders on the ground.
- During an Amber Alert, or police pursuit of a suspect, emergency responders were left without any means to communicate the situation to other jurisdictions.

In 2004, the State of Nebraska proposed an 800 MHz trunked radio system that would connect all emergency responders statewide. Under the state plan, users would be charged a fee for every radio added to the system with the cost burden of procuring the radios and the requisite fees placed on the local jurisdictions. The "top-down" approach left smaller agencies at the local level feeling voiceless and unable to participate in the proposed interoperability solution. That same year, Nebraska's legislature rejected the proposed statewide system as too costly.

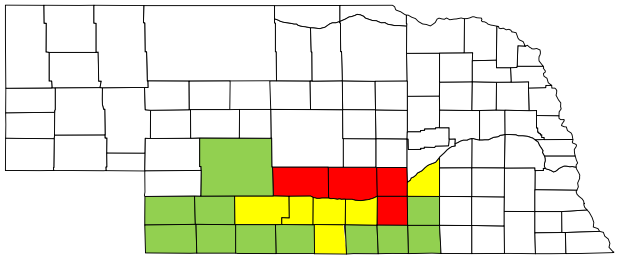
After: Teamwork Leads to Communications Success

After the plan for the statewide radio system was rejected, many agencies realized they had only become interoperable through a collaborative, locally driven, bottom-up approach that integrated all the different human components as well as the technological variations within each agency.



Four counties in Nebraska—Adams, Buffalo, Dawson, and Hall—had already begun collaborating to plan for the failed statewide system and decided to continue their collaboration to address their current and future interoperability issues. The counties collectively established the Central Nebraska Regions for Interoperability (CNRI) to create a system of systems. As word spread about the collaboration, six more counties contacted the CNRI, and the four member counties grew to 10. The CNRI proposed a solution consisting of a multi-county Internet Protocol network and integration software to integrate independently owned and operated regional systems, as necessary, allowing any jurisdiction to communicate with another. To fund the system, the 10 counties applied for a Federal Homeland Security grant through the Nebraska Emergency Management Agency. The result was a $1.2 million grant to establish a multi-county interoperability network.

Representatives from the 10 counties met frequently, defined goals, drafted an interoperability plan, and signed a joint Interlocal Agreement demonstrating their full commitment to the project including usage, costs, and maintenance issues. The CNRI also developed two teams—a user group and a policy group—to develop policies and procedures for the system, including SOPs, which are still being refined today. All 10 counties have also signed, or plan to sign, Mutual Aid Agreements that define mutual aid policies between the state agencies, local agencies, public organizations, and private organizations.



Three years after its inception, the CNRI now has 22 county participants, and stands as a successful example of a system of systems. These counties worked together to overcome disparate technology, demographic and topographic differences, and varying goals; the work of the CNRI has transformed the unique needs of many into a single vision and purpose that links communication systems and emergency responders throughout Nebraska.

Conclusion

Using a system of systems approach, each individual system becomes a component in a regional and nationwide group of other systems. Each system can be connected to others as long as jurisdictions and agencies collaborate when establishing governance structures, creating standard operating procedures, designing training drills, and identifying compatible technology and equipment in use today or for the future. These connections and relationships between jurisdictions and agencies establish the foundation of a system of systems, and lay the groundwork for successful interoperability – they should ultimately drive the decisions jurisdictions make about future technology capabilities.

The Department of Homeland Security established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts in order to improve local, tribal, state, and Federal emergency preparedness and response. Managed by the Science and Technology Directorate's Command, Control and Interoperability Division, OIC is committed to developing technologies and tools—methodologies, templates, models, and educational materials—that effectively meet the critical needs of emergency responders in the field.

Homeland Security

Visit www.safecomprogram.gov
or call 1-866-969-SAFE