



Interoperability Continuum

A tool for improving emergency response communications and interoperability



**Homeland
Security**

Interoperability Overview

Emergency responders—emergency medical services (EMS), fire-rescue personnel, and law enforcement officers—need to share vital data or voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Many people assume that emergency response agencies across the Nation are already interoperable. In actuality, emergency responders often cannot talk to some parts of their own agencies—let alone communicate with agencies in neighboring cities, counties, or states.

Developed with practitioner input by the Department of Homeland Security's SAFECOM program, the Interoperability Continuum is designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications. This tool identifies five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures (SOPs), technology, training and exercises, and usage of interoperable communications. Jurisdictions across the Nation can use the Interoperability Continuum to track progress in strengthening interoperable communications.

To drive progress along the five elements of the Continuum and improve interoperability, emergency responders should observe the following principles:

- Gain leadership commitment from all disciplines (e.g., EMS, fire-rescue response, and law enforcement).
- Foster collaboration across disciplines through leadership support.
- Interface with policy makers to gain leadership commitment and resource support.
- Use interoperability solutions regularly.
- Plan and budget for ongoing updates to systems, procedures, and documentation.
- Ensure collaboration and coordination across all Interoperability Continuum elements.

Interoperability Continuum Elements

Interoperability is a multi-dimensional challenge. To gain a true picture of a region's interoperability, progress in each of the five interdependent elements must be considered. For example, when a region procures new equipment, that region should plan and conduct training and exercises to make the best use of that equipment.

Optimal interoperability is contingent on an agency's and jurisdiction's needs. The Continuum is designed as a guide for jurisdictions that are pursuing a new interoperability solution, based on changing needs or additional resources.

Governance

Establishing a common governing structure for solving interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establishing guidelines and principles; and reducing any internal jurisdictional conflicts. Governance structures provide the framework in which stakeholders can collaborate and make decisions that represent a common objective. It has become increasingly clear to the emergency response community that communications interoperability cannot be solved by any one entity; achieving interoperability requires a partnership among emergency response organizations across all levels of government. As such, a governing body should consist of local, tribal, state, and Federal entities as well as representatives from all pertinent emergency response disciplines within an identified region.

Individual Agencies Working Independently—A lack of coordination among responding organizations.

Informal Coordination Between Agencies—Loose line level or agency level agreements that provide minimal incident interoperability.

Key Multi-Discipline Staff Collaboration on a Regular Basis—A number of agencies and disciplines working together in a local area to promote interoperability.

Regional Committee Working within a Statewide Communications Interoperability Plan Framework

—Multi-disciplinary jurisdictions working together across a region pursuant to formal written agreements as defined within the larger scope of a state plan—promoting optimal interoperability.

Standard Operating Procedures

Standard operating procedures—formal written guidelines or instructions for incident response—typically have both operational and technical components. Established SOPs enable emergency responders to successfully coordinate an incident response across disciplines and jurisdictions. Clear and effective SOPs are essential in the development and deployment of any interoperable communications solution.

Individual Agency SOPs—SOPs exist only within individual agencies and are not shared, resulting in uncoordinated procedures and/or incompatible data systems among agencies that can hinder effective multi-agency/multi-discipline response.

Joint SOPs for Planned Events—The development of SOPs for planned events—this typically represents the first phase as agencies begin to work together to develop interoperability.

Joint SOPs for Emergencies—SOPs for emergency level response that are developed as agencies continue to promote interoperability.

Regional Set of Communications SOPs—Region-wide communications SOPs for multi-agency/multi-discipline/multi-hazard responses serve as an integral step towards optimal interoperability.

National Incident Management System Integrated SOPs—Regional SOPs are molded to conform to the elements of the National Incident Management System.

Technology

Technology is a critical tool for improving interoperability, but it is not the sole driver of an optimal solution. Successful implementation of data and voice communications technology is supported by strong governance and is highly dependent on effective collaboration and training among participating agencies and jurisdictions. Technologies should meet the needs of practitioners on the frontlines and should address regional needs, existing infrastructure, cost vs. benefit, and sustainability. The technologies described within the Continuum must be scalable in order to effectively support day-to-day incidents as well as large-scale disasters. Many times, a combination of technologies is necessary to provide effective communications among emergency responders. Security and authentication challenges are present in each technology and must be considered in all implementation decisions.

Data Elements

Swap Files—Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, emails, faxes). This process effectively creates a static “snapshot” of information in a given time period. Though swapping files requires minimal planning and training, it can become difficult to manage beyond one-to-one sharing. With data frequently changing, there may be issues concerning the age and synchronization of information, timing of exchanges, and version control of documents. Each of these issues can hinder real-time collaborative efforts. In addition, the method of sharing files across unprotected networks raises security concerns.

Common Applications—The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data. Common proprietary applications can increase access to information, improve user functionality, and permit real-time information sharing between agencies. However, the use of common proprietary applications requires strong governance to coordinate operations and maintenance among multiple independent agencies and users; these coordinated efforts are further compounded as the region expands and additional agencies use applications. Common proprietary applications also limit functionality choices as all participating agencies must use compatible applications.

Custom-Interfaced Applications—Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom “one-off” links or a proprietary middleware application. As with common applications, this system can increase access to information, improve user functionality, and permit real-time information sharing among agencies. Improving upon common applications, this system allows agencies to choose

their own application and control the functionality choices. However, if using one-to-one interfaces, the use of multiple applications requires custom-interfaces for each linked system. As the region grows and additional agencies participate, the required number of one-to-one links will grow significantly. Proprietary middleware applications allow for a more simplified regional expansion; however, all participants must invest in a single “one-off” link to the middleware, including any state or Federal partners. Additionally, custom-interfaced applications typically require more expensive maintenance and upgrade costs. Changes to the functionality of linked systems often require changes to the interfaces as well.

One-Way Standards-Based Sharing—One-way standards-based sharing enables applications to “broadcast/push” or “receive/pull” information from disparate applications and data sources. This system enhances the real-time common operating picture and is established without direct access to the source data; this system can

also support one-to-many relationships through standards-based middleware. However, because one-way standards-based sharing is not interactive, it does not support real-time collaboration between agencies.

Two-Way Standards-Based Sharing—Two-way standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly. As with other solutions, a two-way approach can increase access to information, improve user functionality, and permit real-time collaborative information sharing between agencies. This form of sharing allows participating agencies to choose their own applications. Two-way standards-based sharing does not face the same problems as other solutions because it can support many-to-many relationships through standards-based middleware.

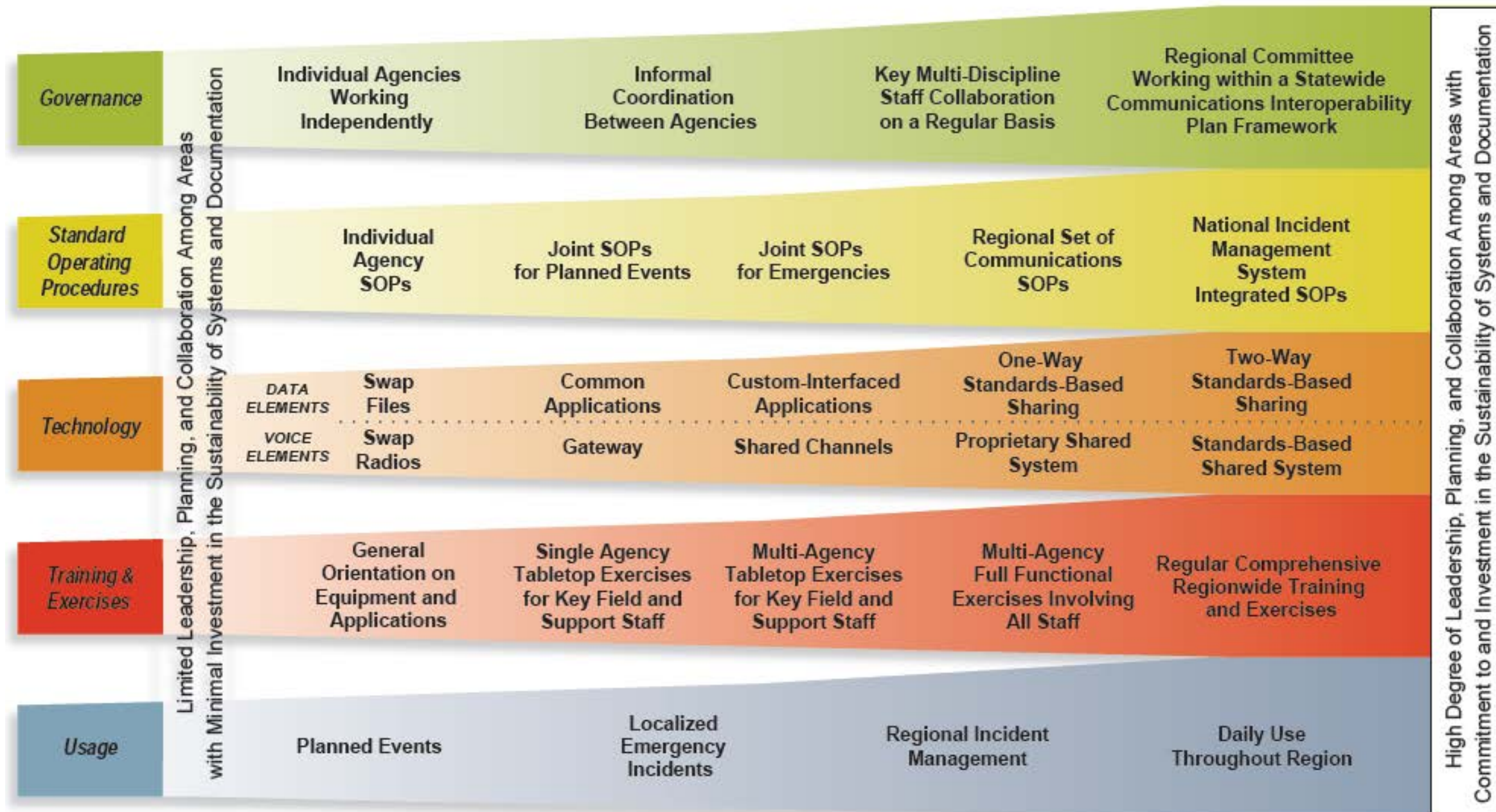
Building on the attributes of other solutions, this system is most effective in establishing interoperability.

Voice Elements

Swap Radios—Swapping radios, or maintaining a cache of standby radios, is an age-old solution that is time-consuming, management-intensive, and likely to provide limited results due to channel availability.

Gateway—Gateways retransmit across multiple frequency bands, providing an interim interoperability solution as agencies move toward shared systems. However, gateways are inefficient in that they require twice as much spectrum because each participating agency must use at least one channel in each band per common talk path and because they are tailored for communications within the geographic coverage area common to all participating systems.

Interoperability Continuum



Shared Channels—Interoperability is promoted when agencies share a common frequency band or air interface (analog or digital), and are able to agree on common channels. However, the general frequency congestion that exists nationwide can place severe restrictions on the number of independent interoperability talk paths available in some bands.

Proprietary Shared Systems and Standards-Based Shared Systems—Regional shared systems are the optimal solution for interoperability. While proprietary systems limit the user's choice of product with regard to manufacturer and competitive procurement, standards-based shared systems promote competitive procurement and a wide selection of products to meet specific user needs. With proper planning of the talk group architecture, interoperability is provided as a byproduct of system design thereby creating an optimal technology solution.

Training & Exercises

Implementing effective training and exercise programs to practice communications interoperability is essential for ensuring that the technology works and responders are able to effectively communicate during emergencies.

General Orientation on Equipment and Applications—Agencies provide initial orientation to their users with regard to their particular equipment and applications. Multi-agency/multi-jurisdictional operations are often an afterthought to this training, if provided at all.

Single Agency Tabletop Exercises for Key Field and Support Staff—Structured tabletop exercises promote planning and identify response gaps. However, single agency activities do not promote interoperability across disciplines and jurisdictions. Additionally, management and supervisory training is critical to promoting routine use of interoperability mechanisms.

Multi-Agency Tabletop Exercises for Key Field and Support Staff—As agencies and disciplines begin working together to develop exercises and provide field training, workable interoperability solutions emerge. Tabletops should address data and/or voice communications interoperability and focus on effective information flow.

Multi-Agency Full Functional Exercises Involving All Staff—Once multi-agency/multi-discipline plans are developed and practiced at the management and supervisory level, it is critical that all staff who would be involved in actual implementation receive training and participate in exercises.

Regular Comprehensive Regionwide Training and Exercises—Optimal interoperability involves equipment familiarization and an introduction to regional/state interoperability at time of hire (or in an academy setting). Success will be assured by regular, comprehensive, and realistic exercises that address potential problems in the region and involve the participation of all personnel.

Despite the best planning and technology preparations, there is always the risk of the unexpected—those critical and unprecedented incidents that require an expert at the helm who can immediately adapt to the situation. Within the Incident Command System, these specialists are called Communications Unit Leaders. The

role of the Communications Unit Leader is a critical function that requires adequate training and cannot be delegated to an individual simply because that person “knows about communications systems.” Rather, the proper training of these individuals is of significant importance to a region's ability to respond to unexpected events, and it should prepare them to manage the communications component of larger interoperability incidents by applying the available technical solutions to the specific operational environment of the event.

Usage

Usage refers to how often interoperable communications technologies are used. Success in this element is contingent upon progress and interplay among the other four elements on the Interoperability Continuum.

Planned Events—Events for which the date and time are known (e.g., athletic events and large conferences/conventions that involve multiple responding agencies).

Localized Emergency Incidents—Emergency events that involve multiple intra-jurisdictional responding agencies (e.g., a vehicle collision on an interstate highway).

Regional Incident Management—Routine coordination of responses across a region that include automatic aid fire response as well as response to natural and man-made disasters.

Daily Use Throughout Region—Interoperability systems are used every day for managing routine as well as emergency incidents. In this optimal solution, users are familiar with the operation of the system(s) and routinely work in concert with one another.

Leadership, Planning, and Collaboration

In addition to progression along the five elements of the Interoperability Continuum, regions should focus on planning, conducting education and outreach programs, and maintaining an awareness of the specific issues and barriers that affect a particular region's movement towards increased interoperability. For example, many regions face difficulties related to political issues and the relationships within and across emergency response disciplines (e.g., EMS, fire-rescue response, and law enforcement) and jurisdictions. Leaders of all agencies and political sub-divisions should help to work through these challenging internal and jurisdictional conflicts as well as set the stage for a region's commitment to the interoperability effort. Additionally, leaders must be willing to commit the time and resources necessary to ensure the sustained success of any interoperability effort. For example, ongoing maintenance and support of the system must be planned and incorporated into the budget.

In addition, collaboration should involve other agencies and organizations that may be critical in supporting the mission of emergency responders. Examples include emergency management agencies, the National Guard, public works, educational institutions/schools, transportation, medical facilities, and large private facilities.

Sustainability

Communications interoperability is an ongoing process, not a one-time investment. Once a governing body is set up, it must be prepared to meet on a regular basis, drawing on operational and technical expertise to plan and budget for continual updates to systems, procedures, and training and exercise programs. If regions expect emergency responders to use interoperable equipment on a daily basis, supporting documentation and the installed technology must be well-maintained with a long-term commitment to upgrades and the eventual replacement of equipment.

Lastly, an interoperability program should include both short- and long-term solutions. Early successes can help motivate regions to tackle more time-consuming and difficult challenges. It is critical, however, that short-term solutions do not inappropriately drive the planning process, but function in support of a long-term plan.

National Frameworks

As an evolving tool, the Interoperability Continuum supports the *National Preparedness Strategy* and aligns with national frameworks including, but not limited to, the National Response Framework, the National Incident Management System, the National Emergency Communications Plan, and the National Communications Baseline Assessment. To maximize the Interoperability Continuum's value to the emergency response community, SAFECOM will regularly update the tool through a consensus process involving practitioners, technical experts, and representatives from local, tribal, state, and Federal agencies.

SAFECOM is a communications program of the Department of Homeland Security. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies. The Office of Emergency Communications (OEC) supports SAFECOM's development of grant guidance, policy, tools, and templates, and provides direct assistance to local, tribal, state, and Federal practitioners. The Office for Interoperability and Compatibility (OIC) supports SAFECOM's research, development, testing and evaluation, standards, and tools such as reports and guidelines. OEC is an office within the Directorate for National Protection and Programs. OIC is an office within the Science and Technology Directorate.



**Homeland
Security**



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