Interoperability Continuum

A tool for improving emergency response communications and interoperability

June 2021

Cybersecurity and Infrastructure Security Agency
SAFECOM

Interoperability Overview

Emergency responders—public safety, and as necessary public services and Non-Governmental Organizations (NGO)—need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Many people assume that emergency response agencies across the Nation already have interoperable communications. However, emergency responders cannot talk to some parts of their own agencies—let alone communicate with agencies in neighboring cities, counties, or states.

Developed with practitioner input from the Cybersecurity and Infrastructure Security Agency's (CISA) SAFECOM program, the *SAFECOM 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)/standard operating guidelines (SOGs) and field operations guides (FOGs), 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.

Governance
SOPs/SOGs and FOGs
Technology
Training & Exercises
Usage

To drive progress along the five elements of the Continuum and improve interoperability - public safety, and as necessary public services and NGOs - should observe the following principles:

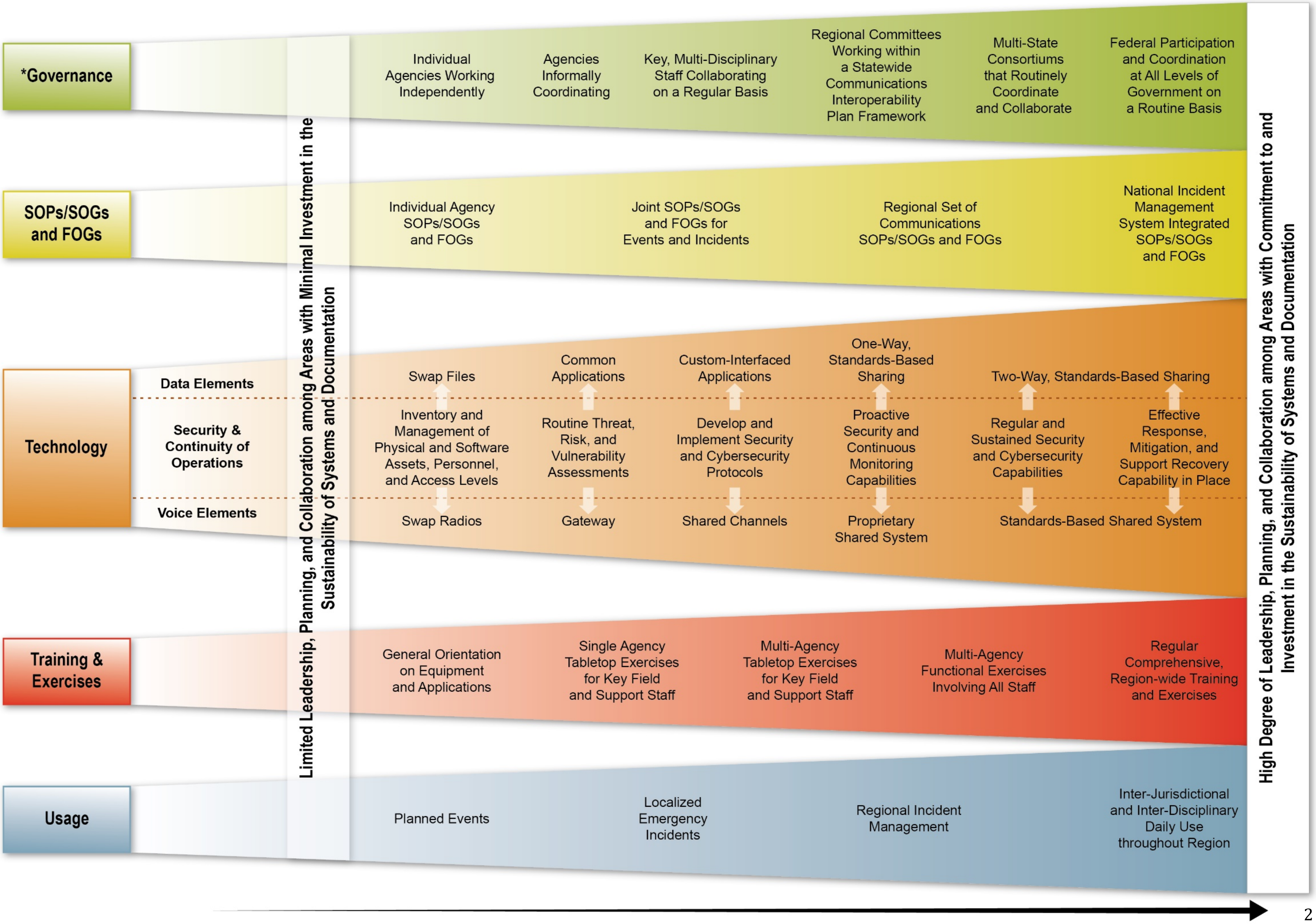
- Gain leadership commitment from all disciplines and jurisdictions
- Foster collaboration across disciplines through leadership support
- Interface with policymakers to gain leadership commitment and resource support, which includes funding and sustainment
- Use interoperability solutions routinely
- Plan and budget for updates to systems, procedures, documentation, and technology

Interoperability Continuum Elements

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

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

Interoperability Continuum



***Governance**

Individual Agencies Working Independently

Agencies Informally Coordinating

Key, Multi-Disciplinary Staff Collaborating on a Regular Basis

Regional Committees Working within a Statewide Communications Interoperability Plan Framework

Multi-State Consortiums that Routinely Coordinate and Collaborate

Federal Participation and Coordination at All Levels of Government on a Routine Basis

SOPs/SOGs and FOGs

Individual Agency SOPs/SOGs and FOGs

Joint SOPs/SOGs and FOGs for Events and Incidents

Regional Set of Communications SOPs/SOGs and FOGs

National Incident Management System Integrated SOPs/SOGs and FOGs

Technology

Data Elements

Swap Files

Common Applications

Custom-Interfaced Applications

One-Way, Standards-Based Sharing

Two-Way, Standards-Based Sharing

Security & Continuity of Operations

Inventory and Management of Physical and Software Assets, Personnel, and Access Levels

Routine Threat, Risk, and Vulnerability Assessments

Develop and Implement Security and Cybersecurity Protocols

Proactive Security and Continuous Monitoring Capabilities

Regular and Sustained Security and Cybersecurity Capabilities

Effective Response, Mitigation, and Support Recovery Capability in Place

Voice Elements

Swap Radios

Gateway

Shared Channels

Proprietary Shared System

Standards-Based Shared System

Training & Exercises

General Orientation on Equipment and Applications

Single Agency Tabletop Exercises for Key Field and Support Staff

Multi-Agency Tabletop Exercises for Key Field and Support Staff

Multi-Agency Functional Exercises Involving All Staff

Regular Comprehensive, Region-wide Training and Exercises

Usage

Planned Events

Localized Emergency Incidents

Regional Incident Management

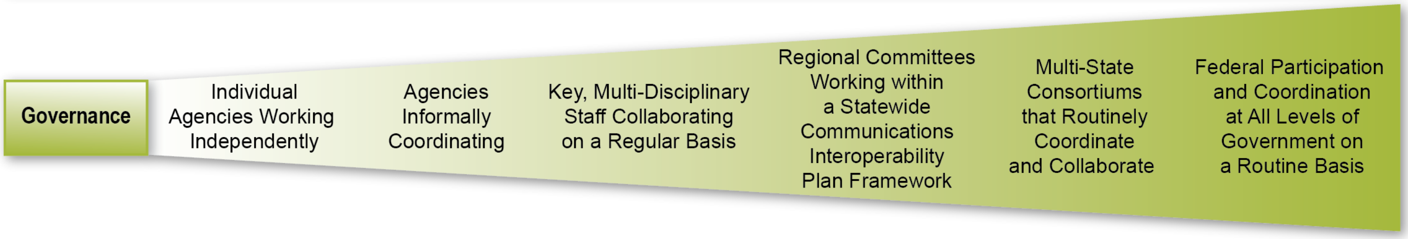
Inter-Jurisdictional and Inter-Disciplinary Daily Use throughout Region

Limited Leadership, Planning, and Collaboration among Areas with Minimal Investment in the Sustainability of Systems and Documentation

High Degree of Leadership, Planning, and Collaboration among Areas with Commitment to and Investment in the Sustainability of Systems and Documentation

*Brochure text updated to include information on Lifecycle Funding within the Governance Section

Governance


Governance
Individual Agencies Working Independently
Agencies Informally Coordinating
Key, Multi-Disciplinary Staff Collaborating on a Regular Basis
Regional Committees Working within a Statewide Communications Interoperability Plan Framework
Multi-State Consortiums that Routinely Coordinate and Collaborate
Federal Participation and Coordination at All Levels of Government on a Routine Basis

Establishing a common governance structure for solving operability and interoperability issues will improve projects, policies, processes, and procedures by enhancing communication, coordination, and cooperation; by establishing guidelines and principles; and by reducing any 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 federal, state, local, tribal, and, territorial (FSLTT) entities as well as representatives from all pertinent emergency response disciplines within an identified region. Governing bodies should drive the enhancements of emergency communications capabilities. As defined in the *2018 Emergency Communications Governance Guide for State, Local, Tribal and Territorial Officials,* "effective governance ...facilitate[s] a greater understanding of existing communications capabilities and gaps, as well as the development of a coordinated strategic plan to prioritize resources, investments, and staffing."[1] For example, the governance structure allows stakeholders to take proactive measures to manage cybersecurity risks, expand training and exercise participation and content to improve operational policies and procedures, and design continuity and resiliency measures, including backup power, overlapping coverage, and route diversity.

Through the governance framework, public safety stakeholders make numerous important decisions to plan, fund, procure, implement, support, and maintain communications systems, and eventually replace and dispose of obsolete systems and components. Funding decisions affect each of the five inter-dependent elements.

For example, when a governance body purchases intrinsically safe radios to work in chemical plants, firefighters and hazardous materials first responders personnel require revised SOPs and training and exercises to effectively use the new equipment. Funding this continuous system lifecycle planning can be daunting. To assist stakeholders, the *2011 Emergency Communications Systems Lifecycle Planning Guide*[2] and the *2018 Compendium*[3] are intended to provide considerations and recommended actions through easy-to-use checklists for each phase of the system lifecycle planning model.

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

Informal Coordination Between Agencies—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

Multi-State Consortiums that Routinely Coordinate and Collaborate— A group of states that routinely work together and coordinate interoperability plans

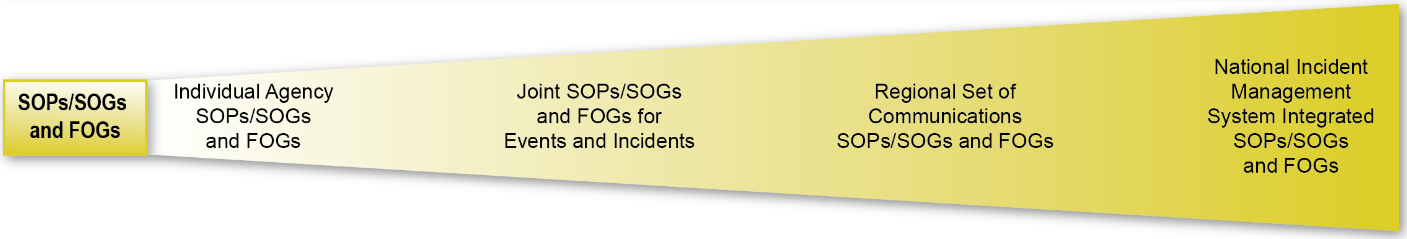
Federal Participation and Cooperation at all Levels of Government on a Routine Basis—Participation and cooperation across all levels of government for interoperable plans and response as needed

[1] 2018 Emergency Communications Governance Guide for State, Local, Tribal and Territorial Officials
cisa.gov/publication/governance-documents

[2] 2011 Emergency Communications Systems Lifecycle Planning Guide
cisa.gov/publication/sustaining-public-safety-communications-systems-documents

[3] 2018 Emergency Communications System Lifecycle Planning Guide Compendium: Best Practices, Considerations, and Recommended Checklists
cisa.gov/publication/sustaining-public-safety-communications-systems-documents

SOPs/SOGs and FOGs


SOPs/SOGs and FOGs
Individual Agency SOPs/SOGs and FOGs
Joint SOPs/SOGs and FOGs for Events and Incidents
Regional Set of Communications SOPs/SOGs and FOGs
National Incident Management System Integrated SOPs/SOGs and FOGs

Standard operating procedures (SOPs)—formal written instructions and practices 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. Standard operating guidelines (SOGs) provide a foundation of policies and procedures for how agencies operate during incidents. SOGs allow responders the flexibility to deviate from the guidance depending on situational or incident mitigation needs. Established SOGs help ensure emergency response activities are consistent, effective, and safe. Field Operations Guides (FOGs) provide detailed interoperable communications resource information about available spectrum, fixed and mobile equipment and how to obtain it, shared resources and how to activate and deactivate them, and other helpful information such as job aids and contact lists to get help when it is needed. A FOG is typically used by Communications Unit Leaders (COML) and their support staff, but it can also be useful information for field commanders and supervisors, dispatchers, and communications center managers. FOGs may also include assets by location and technical assistance references to call upon additional skilled communications personnel.

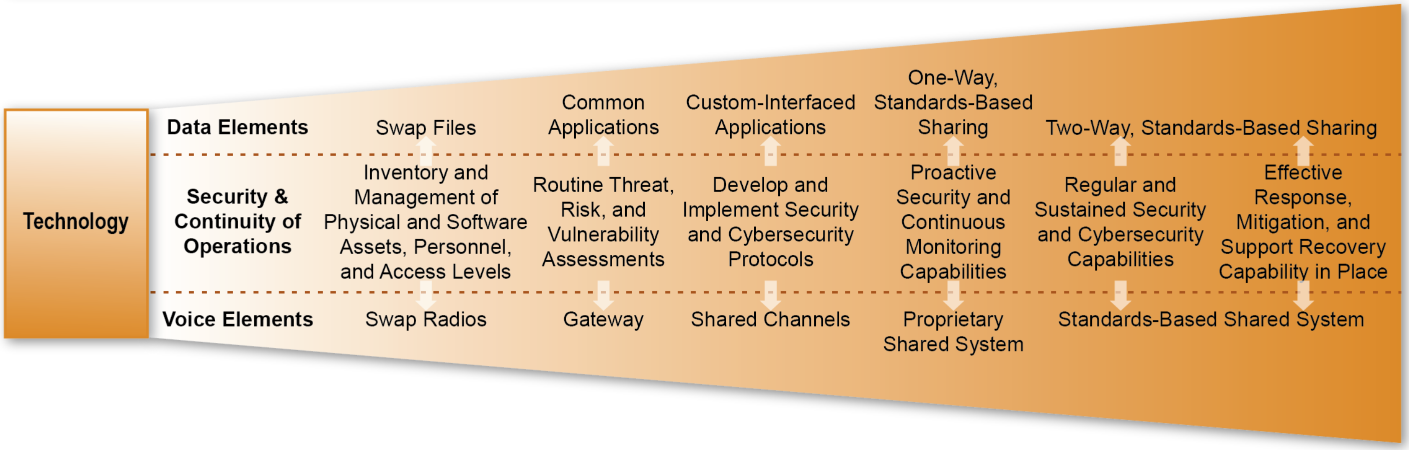
Individual Agency SOPs/SOGs and FOGs—SOPs/SOGs and FOGs created within an individual agency and are not shared, resulting in uncoordinated procedures and/or incompatible data systems among agencies that can hinder effective multi-agency/multi-discipline response

Joint SOPs/SOGs and FOGs for Events and Incidents—The development of SOPs for planned events and emergency level response that are developed as agencies continue to promote interoperability

Regional Set of Communications SOPs/SOGs and FOGs—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/SOGs and FOGs—Regional SOPs and FOGs are molded to conform to the elements of the National Incident Management System

Technology



Technology						
Data Elements	Swap Files	Common Applications	Custom-Interfaced Applications	One-Way, Standards-Based Sharing	Two-Way, Standards-Based Sharing	
Security & Continuity of Operations	Inventory and Management of Physical and Software Assets, Personnel, and Access Levels	Routine Threat, Risk, and Vulnerability Assessments	Develop and Implement Security and Cybersecurity Protocols	Proactive Security and Continuous Monitoring Capabilities	Regular and Sustained Security and Cybersecurity Capabilities	Effective Response, Mitigation, and Support Recovery Capability in Place
Voice Elements	Swap Radios	Gateway	Shared Channels	Proprietary Shared System	Standards-Based Shared System	

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 increases access to a static "snapshot" of information in a given time period; however, swapping files requires planning and training especially when managing beyond one-to-one sharing. With data frequently changing, swapping files requires strong governance to update the age and synchronization of information, schedule the timing of exchanges, and establish the version control of documents. Each of these items can hinder real-time collaborative efforts. In addition, participating agencies must take adequate steps to protect their networks from any potential 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 or 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. 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 FSLTT 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 the most effective in establishing interoperability.

Voice Elements

Swap Radios—While expensive and human-resource intensive, swapping radios or maintaining a cache of standby radios is a reliable but least sophisticated solution to achieve interoperability.

Gateway—Gateways retransmit across multiple frequencies and talk groups, and also allow access to phone and cellular systems. Gateways provide an interim interoperability solution as agencies move toward shared systems. However, gateways encumber 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. A gateway may also create latency and other technical obstacles between push-to-talk and traffic reception which can be adjusted to decrease impact on operations.

Shared Channels—Interoperability is enhanced when agencies share a common frequency, talk group, or air interface (analog or digital) and are able to agree on common channels. A clear understanding of the nature and availability of interoperable communications channels in a given area is essential to prevent congestion, and to assure that shared channels and/or talk groups can be assigned quickly and to appropriate end users when needed.

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. An optimal technology solution can be provided with proper talk group architecture and capacity planning, and both operability and interoperability addressed by system design.

Security & Continuity of Operations

To prepare for a multitude of possible threats and incidents, emergency responders and policy makers must continually identify risks and evolve security requirements in coordination with partners in their Emergency Communications Ecosystem (see page 9 for information on the Emergency Communication Ecosystem). Successful security risk management starts with strong governance and is highly integrated with the remaining elements of the Continuum. An integrated approach to address infrastructure and physical security, cybersecurity, and encryption collectively strengthens the security posture of the Emergency Communications Ecosystem.

Inventory and Management of Physical and Software Assets, Personnel, and Access Levels—Accurate inventory and management of assets, personnel, and access levels follows generally accepted inventory protocols compliant with state and federal statutes, rules, and best practices. Equipment purchased with grant funding must follow the specific grant requirements. Documenting lost, stolen, and misplaced devices as well as current or outdated software is critical to understanding and identifying potential vulnerabilities. Use of federated Identity, Credential, and Access Management solutions builds trust among inventory management personnel and helps prevent inappropriate access to critical information and unauthorized use of resources.

Routine Threat, Risk, and Vulnerability Assessments—Routine assessment and testing of the entire Emergency Communications Ecosystem is a component of a threat, risk, and vulnerability gap analysis. Testing of software, hardware, and infrastructure (e.g., penetration testing) coupled with testing of people, practices, and procedures (e.g., phishing campaigns) can uncover gaps and areas for improvement.

Develop and Implement Security and Cybersecurity Protocols—Security and cybersecurity protocols reflect an agency's specific requirements and generally accepted best practices and protocols. Successful cybersecurity programs are consistent with Criminal Justice Information Services Guidelines[4] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[5]

Proactive Security and Continuous Monitoring Capabilities—Proactive security and continuous monitoring and testing of all physical, infrastructure, and software assets reduces the risk of a system breach. Proactive security may include encryption and key management best practices, non-systematic penetration testing, and continuously updating software and security patches. Additionally, these capabilities work to monitor and detect security risk or threat events and verify the effectiveness of protocols and protective measures.

Regular and Sustained Security and Cybersecurity Capabilities—The security posture of the Emergency Communications Ecosystem must continually evolve and strengthen to address new and more sophisticated threats and risks. Capabilities should reflect ongoing NIST work to plan for setting, testing, and maintaining cybersecurity minimum standards. Vendor maintenance agreements should be consistent with industry standards and best practices and include staff education and training during system updates and upgrades.

Effective Response, Mitigation, and Support Recovery Capability in Place—Optimal security risk management enables an organization to detect, mitigate, and continue to function in the event of a threat or an incident (e.g., unauthorized access, malware, social engineering, system failure). This broadening set of capabilities enables timely discovery and supports the ability to contain the impact of a potential cybersecurity incident. Further, appropriate plans are in place to maintain resilience, highlight contact lists to get help when it is needed, and restore any capabilities or services that were impaired due to a cybersecurity incident.

Infrastructure and Physical Security

Critical infrastructure are those assets, systems, and networks that underpin American society. Managing the

[4] Criminal Justice Information Services Guidelines
fbi.gov/services/cjis/cjis-security-policy-resource-center

[5] NIST Cybersecurity Framework
nist.gov/cyberframework

risks from significant threat and hazards to physical and cyber infrastructure requires critical infrastructure partners to collectively identify priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment. To assist stakeholders, the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, guides the national effort to manage risk to the Nation's critical infrastructure[6]. Additionally, CISA's Interoperable Communications Technical Assistance Program offers the Communications Assets Survey Mapping Tool (CASM), [7] the primary nationwide resource for the state, local, tribal, and territorial emergency communications community to inventory and share asset information. Agencies should strive to maintain and update their information in CASM.

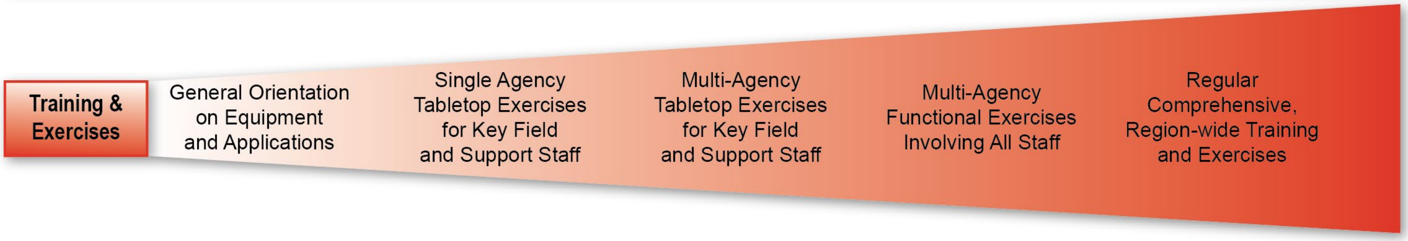
Cybersecurity

Cybersecurity is the process of protecting connected electronic systems and information by preventing, detecting, and responding to threats and attacks. Managing cybersecurity risk starts with an effective governance structure that encourages emergency responders and policy makers to evaluate, communicate, and advocate for cybersecurity services and resources in each of the five interdependent Interoperability Continuum elements. To assist stakeholders in improving cybersecurity, the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, provides approaches to strengthen cybersecurity in critical infrastructure as well as the overall Emergency Communications Ecosystem.[8]

Encryption

Encryption is a primary method of mitigating threats from the potential compromise of personal or sensitive data by encoding information in such a way that only authorized parties can access it. While encryption is not required for interoperability, successful encrypted interoperability depends largely upon strong coordination between agencies that need to interoperate. Encryption can add a significant level of complexity and should be considered only when the incident requirements outweigh the additional complications. To assist stakeholders in properly implementing encrypted communications, the Federal Partnership for Interoperable Communications Security Working Group's *Determining the Need for Encryption in Public Safety Radios* provides guidelines and best practices to be considered when implementing encrypted communications.[9]

Training & Exercises


Training & Exercises
General Orientation on Equipment and Applications
Single Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Functional Exercises Involving All Staff
Regular Comprehensive, Region-wide Training and 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. Public safety personnel require training and exercises to develop the knowledge, skills, abilities, and mindset to use their communications resources to achieve interoperability, regardless of discipline or level of government in a given area. Building on the set of guiding principles for exercise programs provided by the Federal Emergency Management Agency (FEMA) Homeland Security Exercise and Evaluation Program[10], communications training will ideally include all public safety, and as necessary public services and NGOs personnel. A broad level of participation builds familiarity, trust, and understanding about available resources and capabilities. Effective training and exercises should be developed and executed using existing SOP/SOG and FOG resources. Evaluating and documenting performance

[6] National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience
cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[7] Communications Assets Survey and Mapping Tool (CASM)
cisa.gov/safecom/casm-tool

[8] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology
nist.gov/cyberframework

[9] Determining the Need for Encryption in Public Safety Radio
cisa.gov/publication/encryption

[10] Homeland Security Exercise and Evaluation Program, April 2013
fema.gov/emergency-managers/national-preparedness/exercises/hseep

following training and during exercises should be done to provide insight into revisions or improvements that need to be made to training programs and content as a result.

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.

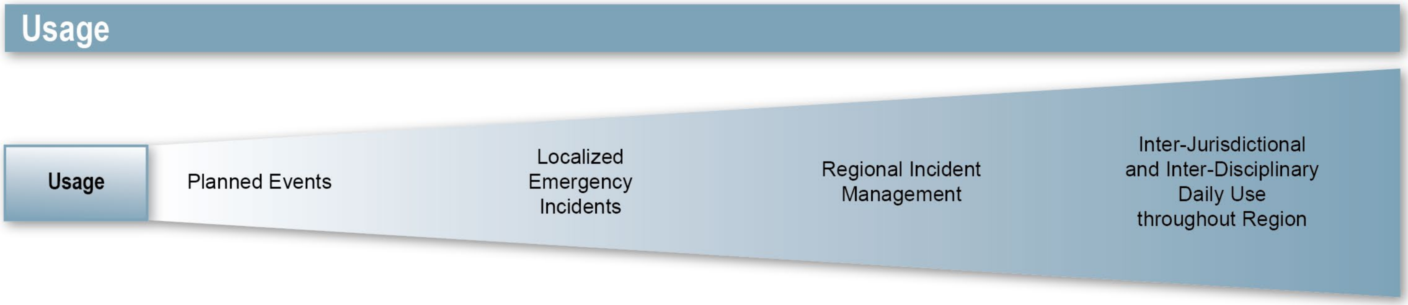
Single Agency Tabletop Exercises for Key Field and Support Staff—Structured tabletop exercises promote planning and identify response gaps. However, single agency activities do not promote interoperability across disciplines and jurisdictions. Additionally, management and supervisory training is critical 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. Tabletop exercises should address data and/or voice communications interoperability and focus on effective information flow.

Multi-Agency 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 functional 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 serve as the COMLs. The role of the COML 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
Planned Events
Localized Emergency Incidents
Regional Incident Management
Inter-Jurisdictional and Inter-Disciplinary Daily Use throughout Region

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, time, and locations are known (e.g., athletic events and large conferences/conventions that involve multiple responding agencies). Planned events may be regional in application.

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 mutual aid interjurisdictional and/or interdisciplinary response as well as response to natural and man-made disasters.

Inter-Jurisdictional and Inter-Disciplinary 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., emergency medical services, fire-rescue response, and law enforcement) and jurisdictions. Leaders of all agencies and all levels of government 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, 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 interoperable communications 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.

The Emergency Communications Ecosystem

The ecosystem is dynamic, depending on the incident or planned event, as well as multi-directional because anyone can initiate emergency communications. As a result, four key functions are necessary to achieve reliable, secure, and interoperable communications. These increasingly interwoven and complex functions include reporting requests for assistance; incident coordination and response; alerts, warnings, and notifications (AWN); and public interaction. As these functions have become increasingly interwoven and complex, the Interoperability Continuum is focused on assisting the emergency response agencies and policy makers to plan and implement interoperability solutions for sharing data and voice communications among each other.

The Emergency Communications Ecosystem consists of the various functions and people that exchange information prior to, during, and after incidents and planned events. The Emergency Communications Ecosystem includes traditional emergency response agencies and other entities that share information during emergencies, such as medical facilities, utilities, nongovernmental organizations, as well as the media and private citizens. While responders rely heavily on interoperable government to government communications, comprehensive strategies for emergency communications must integrate the full Emergency Communications Ecosystem, including broadband, AWN, social media, and Next Generation 911 (NG911). For example, with the First Responder Network Authority's (FirstNet Authority) implementation of the Nationwide Public Safety Broadband Network, agencies will be able to supplement existing systems to provide public safety users with dedicated spectrum, added broadband capabilities, and advanced technologies to increase situational awareness. Further, the Nation's transition to NG911 enables interconnection among a wide range of public and private networks, providing greater situational awareness to dispatchers and emergency responders and establishing a level of resiliency not previously possible. NG911 will allow Public Safety Answering Points/Emergency Communication Centers to accept and process a range of information from emergency responders and the public, including text, images, video, and voice calls.

SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001, as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across federal, state, local, tribal, and territorial governments, and international borders.