RECOMMENDED FEDERAL INTEROPERABLE COMMUNICATIONS
GRANT GUIDANCE FISCAL YEAR (FY) 2008

Table of Contents

1. INTRODUCTION

New Title XVIII of the Homeland Security Act established the **Office of Emergency Communications (OEC)** within the Department of Homeland Security and charged that Office's Director with, among other duties, planning and overseeing the implementation and management of a new organization focused on interoperable communications. OEC manages the policy and planning elements of the SAFECOM Program and is charged with the development of national interoperability grant guidance and policies.

This grant guidance provides Federal grant programs with recommended criteria to ensure that the limited funding available for emergency response communications is effectively and efficiently dispersed. Federal Fiscal Year (FY) 2008 Appropriations make available grant funding to enhance communications interoperability across the Nation. By definition, communications interoperability refers to the ability to communicate across jurisdictions and disciplines to support incident management when needed and as authorized.

In addition, this grant guidance provides the emergency response community with tools and resources for the development of interoperability solutions. In an effort to coordinate the way in which funding is allocated and to maximize the prospects for interoperable communications, the OEC's SAFECOM program has developed some recommended grant criteria in concert with representatives of the emergency response community.

The guidance criteria reflects a comprehensive approach to interoperability—one that understands that the problem of interoperability is not solely technological. Technology is just one of several critical elements necessary for the development of a robust interoperability solution. As Secretary Chertoff explained at the May 8, 2006 Tactical Interoperable Communications Conference, "…the biggest barrier to interoperability is not technology…[the challenge] has to do with, rather, human beings. It has to do with how do we get people to be able to use this equipment in a way that makes interoperability not just a theoretical possibility, or a technological possibility, but an actual, workable, day-to-day solution."

Achieving effective interoperability across the Nation requires dedicating resources to improving such critical elements as governance, standard operating procedures, training and exercises, and regular use of interoperable capabilities. Further, it requires strong leadership in and among organizations—leadership that promotes and engages in extensive, coordinated, multi-jurisdictional, and multi-disciplinary planning efforts for interoperability.

What follows is an outline of recommended grant funding eligibility (including applicants and activities), application criteria, guidelines, and resources to assist the emergency response community in strengthening interoperability. Frequently asked questions regarding the document, can be found on the SAFECOM Web site (www.safecomprogram.gov).

2. ELIGIBILITY

Section 2.1 – Eligible Applicants

Federal funds that are allocated for improving emergency response communications and interoperability should only be provided to emergency response agencies or organizations at the regional, State, local, or tribal level. They include:

- Emergency Medical Services (EMS) agencies
- Fire service agencies
- Law enforcement agencies
- An organization representing the above agencies
- Any emergency response agency listed as an eligible applicant in Federal grant programs that include this guidance

Section 2.2 – Eligible Activities

The following are the eligible activities for which Federal funding awarded for interoperable voice and/or data communications may be used, subject to the statutory authority of the grantor agency:

- **Planning and Management** activities, including:

  - Establishing a governance structure for emergency response interoperability projects
  - Conducting a capabilities assessment
    - Operational (standard operating procedures, training, usage)
    - Technical
  - Strategic planning
    - Operational (standard operating procedures, training, usage)
    - Technical
  - Implementation and management

- **Equipment Acquisition** for the purposes of:

  - Building emergency response communications systems
  - Upgrading/enhancing emergency response communication systems and equipment
  - Replacing emergency response communication systems and equipment
  - Maintaining emergency response communication systems and equipment

- **Training and Exercising** on the following:

  - Use of equipment and systems
  - Use of standard operating procedures

For more information on eligible activities, see Section 4.

3. APPLICATION CRITERIA

Section 3.1 – Identify the Emergency Response Agency or Agencies for Which Funding Is Requested

Identify the emergency response agency or agencies for which funding is requested, which should include:

- Type of agency (in accordance with eligible applicants defined in the previous section)
- Name of agency
- Location
- Level of government
- Regional planning involvement
- Description of multi-discipline and/or multi-jurisdictional cooperation

Section 3.2 – Identify the Eligible Activity for Which Funding Is Requested

Identify the eligible activity or activities for which funding is requested. Eligible activities may include, subject to the statutory authority of the grantor agency:

- Planning and management
- Equipment acquisition
- Training and exercising

Section 3.3 – Describe How the Proposed Activity Will Improve Interoperability

In order to receive funding, the applicant must be able to convey an understanding of the emergency responder needs and how the funded project might provide a clear path towards interoperability. Provide a summary that describes how any activity for which funding is requested will fit into an overall effort to increase interoperability. At a minimum, the summary should:

- Define the vision, goals, and objectives of the activity and how the proposed project would fit into an overall effort to increase interoperability.

- Include information on the governance structure overseeing the effort, including membership, roles, and responsibilities.

- Describe the specific problems or needs that are to be addressed; where appropriate, applicants should include a description of how the proposed activity will address any deficiencies documented through prior grantor assessments (i.e., urban/metropolitan areas receiving DHS grant funds should ensure that their proposed activity will address areas of decreased capabilities documented in the FY 2006 Scorecard Assessment process).

- Provide a description of this activity will improve multi-discipline and/or multi-jurisdictional interoperability.

- Propose a detailed budget and timeline, including an operational plan that addresses how the effort will be funded now and in the future.

- Provide a communications system plan and a deployment plan that includes operations, maintenance, and training plan(s).

- Identify any potential partners and their roles and staffing requirements, and provide information on any existing agreements such as a Memorandum of Understanding (MOU) or Mutual Response Agreement.

Section 3.4 – Address How the Proposed Activity Will Adhere to the Criteria Set Forth for Each

Each eligible activity will have criteria which should be addressed. Section 4 details these criteria in the form of principles and guidelines. These can help ensure that applicants have both taken the needs of emergency responders and potential partners into account, and have considered short- and long-term goals. Applicants should demonstrate ways in which they will incorporate these principles and guidelines in performing their eligible activity, in addition to the information for the summary required in Section 3.3.

Section 3.5 – Develop, Adopt and Update Statewide Communications Interoperability Plan *(State Applicants Only)*

The FY 2007 Homeland Security Grant program and the FY 2007 Public Safety Interoperable Communications (PSIC) Grant Program required States to submit Statewide Communications Interoperability Plans and PSIC Investment Justifications by December 3, 2007[1].   If your State has not submitted a plan it is recommended that you contact the Office of Emergency Communications.

States should continue to update their plans as needed. An updated criteria for the statewide plans is outlined in Section 5.

Section 3.6 – Share Information on Interoperability Solutions *(Block Grant Recipients Only)*

This provision is recommended for Federal grant programs providing block grant interoperable communications funding and is subject to the statutory authority of the grantor agencies.

To promote cross-jurisdictional coordination and information sharing, block grant recipients are encouraged to gather information regarding the amount of money received and the ways in which the funding is spent. Information to be gathered includes:

- The amount of funding received for communications interoperability
- The entity receiving the grant funding
- Additional jurisdictions involved in coordination
- The timeline for the grant funding
- The ways that the Federal funding is spent, including:

---

[1] The Public Safety Interoperable Communications (PSIC) Grant Program identifies the Statewide Communications Interoperability Plans as one of its evaluation factors for States and Territories to receive PSIC funding. The statutory requirements as related to the PSIC Grant Program can be found in the PSIC Grant Program Guidance and Application Kit, dated August 16, 2007, and located on the NTIA website http://www.ntia.doc.gov/psic

- o Planning
- o Training
- o Equipment
- o Exercises
- o Promoting routine follow-on usage

Section 3.7 – Demonstrate National Incident Management System (NIMS) Compliance

Homeland Security Presidential Directive (HSPD) 5 required the adoption of NIMS by all Federal departments and agencies. The directive also requires that Federal preparedness assistance funding for States, territories, local jurisdictions, and tribal entities depends on NIMS compliance. Information regarding the most recent compliance criteria is available at: http://www.fema.gov/emergency/nims/nims_compliance.shtm. FY 2008 grant applicants are encouraged if possible to demonstrate NIMS integration in their plans.

DHS created NIMS to provide a consistent nationwide approach for all levels of government to work together effectively and efficiently to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

4. PRINCIPLES AND GUIDELINES FOR ELIGIBLE ACTIVITIES

Section 4.1 – Planning and Management

When planning for improved interoperability, a number of critical elements must be addressed. The Interoperability Continuum (Figure 1) depicts the critical elements for successful planning and implementation of a robust interoperability solution, including governance, standard operating procedures, technology, training/exercises, and usage of equipment. Applicants should demonstrate an understanding of this framework and how element is interdependent. For example, if an applicant proposes procurement of new equipment, the proposal should include plans for procedures, training, and exercises to ensure the best use of that equipment. More detailed information on the Interoperability Continuum can be found on the SAFECOM Web site at www.safecomprogram.gov.

Figure 1
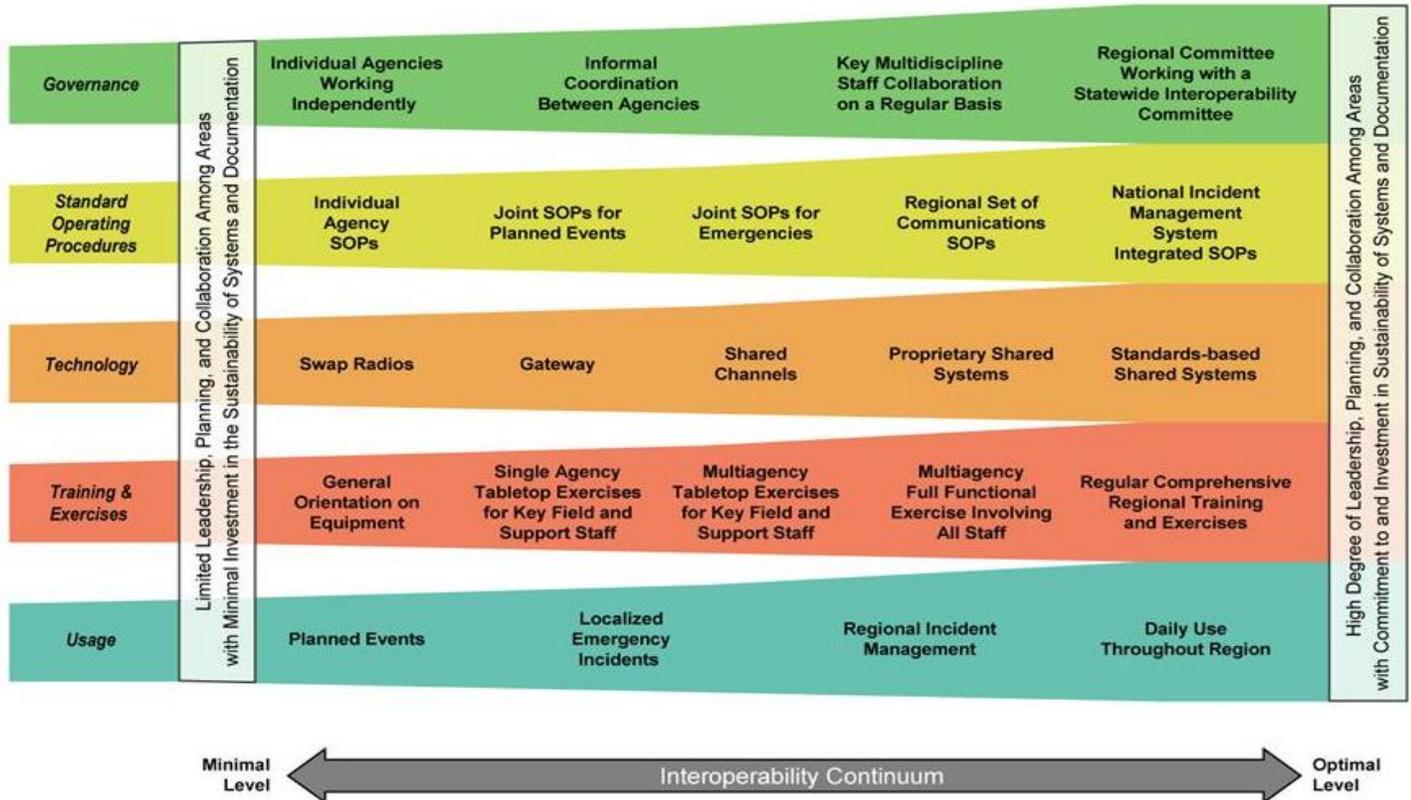
In addition to incorporating an understanding of these five critical elements, planning activities in general should be conducted on a regional or statewide basis and take into account both short- and long-term goals. Once planning activities are established, consistent leadership and management are needed to oversee development, implementation, and maintenance of the interoperability projects.

Eligible Planning and Management Activities
Planning and management activities include establishing a governance structure, conducting capabilities assessments (for both operational and technical capabilities), strategic planning (for

both operational and technical needs), and managing the implementation of a strategic plan (equipment acquisition, standard operating procedures (SOPs), and training development, etc.) After the governance structure is established, assessment, planning, and implementation should be carried out by the committee or working groups that are established as part of the structure.

Establishing a Governance Structure

Consistent leadership and management ensure that planning, equipment procurement, training, and funding are in place when developing an emergency response communications interoperability project. A common governing structure improves the policies, processes, and procedures of any project by doing three things. First, it enhances communication, coordination, and cooperation. Second, it establishes guidelines and principles. Additionally, a common governing structure improves the policies, processes, and procedures by reducing any internal turf battles. The governance structure should consist of representatives of all pertinent local, tribal, State, and Federal emergency response disciplines. This governance structure could also consist of any other agency that is a statutory eligible applicant and are involved in an emergency response communications improvement or interoperability project. This management structure takes the form of a governing body that makes decisions, solicits funding, and oversees the planning, implementation, and management of an interoperability initiative. When establishing a governance structure the following should be considered:

- Is the communications project consistent with similar efforts in the region?
  - Are agreements in place with other agencies or jurisdictions that illustrate cooperative management of the communications improvement or interoperability project?

- Does the project have the support of the relevant State or local governing authority and political leadership?

- What other funding sources has the applicant sought for the ongoing administrative costs of program management?

- Has a mechanism been established for future, sustained funding?

Strategic Planning

When engaging in planning, nearby agencies or jurisdictions from other disciplines or other local, tribal, State, or Federal partners should be included. For those developing statewide strategic plans, specific criteria can be found in Section 5.

The following questions should be considered for strategic planning in general:

- Who are the stakeholders that need to be involved in the planning?

- Which decision makers should be involved?

- What type of technical and field expertise will be needed to develop the plan?

- Will outside expertise be needed to develop this plan? If so, what kind?

- What are the roles and responsibilities of all agencies that are involved? (Include a list of partnering agencies.)

- Do mutual response agreements include interoperable communications?

- What type of governing structure exists to improve the processes for executing any planned project?

In addition to taking an inclusive approach, planning should take into account both short- and long-term goals. The following questions should be considered:

- What should be done in the first phase?

- How many phases will the plan require?

- How much time is needed to accomplish the plan?

- What are the technical solutions available to address the problem in the short- and long-term?

- What funding is available to address the problem in the short- and long-term?

Capability Assessments

The development of a capability assessment—a baseline understanding of existing resources is encouraged to help ensure the assessment meets the needs of a multi-discipline/multi-jurisdiction response. In order to be completely comprehensive and transparent capability assessments should be developed by a discipline-neutral party. For additional considerations on capability assessments, see sections below, Operational Considerations for Capability Assessments and Strategic Planning, and Technical Considerations for Capability Assessments and Strategic Planning.

Operational Considerations for Capability Assessments and Strategic Planning

Operational planning activities for emergency response communications projects may include SOPs, training and exercises, and regular use for the equipment. Planning for such activities should consider the communication needs and requirements of the emergency response community, including:

- What information needs to be exchanged

- With whom the agency or jurisdiction needs to communicate

- How the agency or jurisdiction needs to communicate

- When the agency or jurisdiction needs to communicate and exchange information (i.e., daily, weekly, infrequently)

- Under what circumstances the agency needs to communicate (i.e., during frequently occurring emergencies, major crimes or incidents, large-scale disasters, etc.)

- Whether regional communications applications are considered for daily use (i.e., mutual aid and regional coordinating centers)

- Whether the community/region plans to transition to "plain language"

- Whether the community/region plans to use the standard channel nomenclature for emergency response interoperability channels (see http://www.npstc.org/index.jsp)

Technical Considerations for Capability Assessments and Strategic Planning

Technical planning activities for emergency response communications projects may include such items as needs and requirements assessments, development of the system network architecture, propagation studies, and similar technical proposals.

The following list outlines items that should be included in planning for such activities:

- All interoperability resources available—including radio caches, gateways, shared channels, shared systems (including system type, mode, band, and manufacturer), and software and systems allowing for exchange of information across disciplines and jurisdictions (such as emergency management software, and computer-aided dispatch software)

- Determine the operational level of existing technology

- Determine the incident level of existing technology

- Types of equipment that can immediately be deployed to provide short-term solutions for improved communications

- All agencies to which the interoperability resources are available

- Scale of the system—local, multi-jurisdictional, multi-discipline, regional, statewide, or national

- Coverage—the system footprint of all areas covered

- Capacity—channel capacity and radio capacity within the existing systems

- Identification of capabilities by site including the identification of site users

- Current interoperability capabilities with other systems

- Compatibility with the Project 25 (P25) suite of standards (see Section 4.2 for additional information)

- For data systems, compliance with the Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Markup Language (XML) based Emergency Data Exchange Language (EDXL) data messaging standards in systems and software (see Section 4.2 for additional information)

- Internal and external security requirements in the architecture to secure information and maintain privacy levels for voice and data, as required by law

- Whether the infrastructure is shared with any other agency or organization and is owned or leased

- Whether equipment locations/sites are shared, owned, and/or leased

- Radio frequencies used to communicate with other emergency response agencies

- Networks or systems used to share information with other emergency response agencies

- Channels designated solely for communicating with other agencies (to include the use of common channel nomenclature for public safety interoperability channels, as applicable (http://npstc.org/index.jsp)

- Primary radio language used by the agency when communicating with other agencies or organizations (e.g. "plain" language or code)

- Type of topography or terrain in which the agency operates

- Types of structures in which the agency needs to communicate (e.g., tunnels or high-rise buildings)

Implementation and Management Considerations
Activities during implementation and management may include but are not limited to procurement of equipment, development of SOPs, and coordination of training and exercises. Organizations that govern such projects must be comprised of the relevant law enforcement, fire response, and emergency agencies.

Section 4.2 – Equipment Acquisition

Communications systems and equipment are expensive and technically complex. As outlined in the previous section, before a procurement decision is made, a technical assessment must be made of the current communications system capabilities. This type pf assessment enables the purchaser to determine whether funds should be directed toward the improvement of existing

systems rather than at the development of completely new systems or infrastructure using proprietary or non-proprietary equipment.

Grant funding in regards to applications, systems, and equipment may be used for:

- Building emergency response communications systems and equipment
- Upgrading or enhancing emergency response communication systems and equipment to include the procurement of interoperable solutions
- Replacing emergency response communication systems and equipment
- Maintaining emergency response communication systems and equipment

Applicants requesting funding for equipment acquisition should consider the principles and guidelines discussed in the following sections.

Priority Areas

Before making equipment acquisition decisions, applicants should ensure that two basic communications needs are met—operability and incident-level capabilities. If applicants have not met these needs in their jurisdiction, they should make equipment acquisitions to meet them first, subject to the statutory authority of the grantor agency or the objectives of the grant program if the applicant is seeking Federal grant funding.

Operability. The first priority of Federal funding for improving emergency response communications is to provide within an organization basic, operable communications that has safety as the overriding consideration.

Incident-Level Communications Capabilities. Agencies are encouraged to consider plans that enable them to achieve, at a minimum, incident-level interoperability. This means ensuring the ability of Incident Command and Operations Section staff to adequately communicate with one another and their respective command centers within one hour of an incident. Agencies are encouraged to explore any and all inexpensive and innovative ways to ensure incident-level interoperability. While such incident management interoperability can provide an interim solution to an area's interoperability needs, these solutions should support long-term interoperability goals by building upon or accelerating long-term strategies and efforts.

Standards

Land Mobile Radio (LMR) Systems

When procuring equipment for communication system a standards-based approach should be used to begin migration to multi-jurisdictional and multi-disciplinary interoperability. Specifically, all new digital voice systems should be compatible with the Project 25 (P25) suite of standards. This recommendation is intended for government-owned or -leased digital land mobile public safety radio equipment. Its purpose is to make sure that such equipment or systems are capable of interoperating with other digital emergency response land mobile equipment or systems. It is not intended to apply to commercial services that offer other types of interoperability solutions. Further, it does not exclude any application if the application demonstrates that the system or equipment being proposed will lead to enhanced interoperability.

With input from the user community, these standards have been developed to allow for backward compatibility with existing digital and analog systems and to provide for interoperability in future

systems. The FCC has chosen the P25 suite of standards for voice and low-speed data interoperability in the new nationwide 700 MHz frequency band. The Integrated Wireless Network (IWN) of the U.S. Justice and Treasury Departments has chosen the P25 suite of standards for their new radio equipment. The U.S. Department of Defense has also endorsed P25 for new LMR systems.

This guidance does not preclude funding of non-P25 equipment when there are compelling reasons for using other solutions. However, the first priority of federal funding (subject to the statutory authority of the grantor agency or the objectives of the grant program if the applicant is seeking Federal grant funding) for improving public safety communications is to provide basic, operable communications within a department with safety as the overriding consideration. Funding requests by agencies to replace or add radio equipment to an existing non-P25 system (i.e., procurement of new portables on an existing analog system) will be considered if there is an explanation as to how their radio selection will allow for improving interoperability or eventual migration to interoperable systems. Absent these compelling reasons, SAFECOM intends that P25 equipment will be preferred for LMR systems to which the standard applies.

DHS, in partnership with the National Institute of Standards and Technology, has developed a P25 Compliance Assessment Program (CAP) which allows users to obtain documented evidence from the manufacturers that equipment has been tested and passed critical normative P25 performance, conformance, and interoperability tests published by the Telecommunication Industry Association. This program is being rolled out in phases, the first of which for FY2008 covers only the Common Air Interface (CAI). The specific tests covered by the CAP at this time can be found in the "Project 25 Explanatory Addenda." Grant applicants purchasing equipment should not accept equipment implementing the CAI (base station, portable and mobile radios) unless the manufacturer, at the time of delivery, at the latest, supplies a DHS recognized Suppliers Declaration of Compliance addressing the required tests. A list of the required tests may be found at https://www.rkb.mipt.org/p25.cfm. Grantees should clearly state in the grant application that P25 equipment purchased with FY08 DHS grant funds shall meet the requirements of the P25 CAP at the time of product acceptance, at the latest, for base station, portable and mobile radios implementing the P25 CAI, and have a published Supplier's Declaration of Compliance posted at https://www.rkb.mipt.org/p25.cfm. Project 25 equipment that implements P25 interface standards other than the CAI (i.e., Inter-RF Subsystem Interface, Fixed Station Substation Interface, Console Subsystem Interface, etc.) are not covered by the CAP at this time and therefore do not require a Supplier's Declaration of Compliance.

For assistance in determining allowable communications equipment purchases under this section, as well as when specific justification material is required, grantees can access web-based technical assistance tools at http://www.its.bldrdoc.gov/resources/p25/OICGrantguidancetool.pdf. The OIC Wireless Communications Grant Guidance Tool will also provide users with access to detailed information that will assist in Project 25 equipment selection and procurement, as well as links to documents available under the Project 25 Compliance Assessment Program.

Data-Related Information Sharing Systems
Grant funded systems, developmental activities, or services related to emergency response information sharing should comply with the OASIS EDXL data messaging standards. Compliance should include the OASIS EDXL Common Alerting Protocol (CAP), version 1.1 or latest version, and the OASIS EDXL Distribution Element (DE), version 1.0 or latest version. Systems should also comply with the Hospital AVailability Exchange (HAVE) and Resource Messaging (RM)

standards which are expected to be finalized in late 2007. More information on these standards can be found in Appendix A of this document and at www.oasis-open.org.

This guidance does not preclude funding of non–OASIS EDXL-compliant systems, when there are compelling reasons for using other solutions. Absent such compelling reasons, the OASIS EDXL standards identified above are the preferred standards.

Grant funded systems, developmental activities, or services related to emergency response information sharing should also leverage the National Information Exchange Model (NIEM) for data component or element standards. More information on NIEM can be found at www.niem.gov.

Standard Channel Nomenclature for Public Safety Interoperability Channels
Though not yet a standard, the National Public Safety Telecommunications Council (NPSTC) recently developed the Channel Naming Report. This document outlines the *NCC / NPSTC Standard Channel Nomenclature for Public Safety Interoperability Channels* as revised in June of 2007 (http://www.npstc.org/index.jsp). The requirement for a common naming protocol for public safety's interoperability frequencies was described in early 2000 by the Public Safety National Coordination Committee (NCC), a Federal Advisory Committee chartered by the Federal Communications Commission (FCC) that operated from 1999 to 2003, and provided recommendations to the Commission on operational and technical parameters for use of the 700 MHz public safety band.

Functional Requirements
When planning for the development of communications systems and looking to ensure both operability and interoperability, emergency responders should employ a standards-based network of networks approach. When procuring voice and data communications equipment, emergency responders should seek equipment that supports specific functional requirements, or equipment capabilities. A list of functional requirements for various components of voice and data communications systems is included in Appendix B. These requirements outline the minimum capabilities that equipment should have for effective interoperable procurement selections.

Section 4.3 – Training and Exercises

To use equipment properly and effectively in emergencies, personnel must be trained through joint exercises that allow them to practice SOPs, become familiar with the equipment, and enhance preparedness in responding to all emergencies. Eligible grant applicants should include multi-disciplinary and multi-jurisdictional training in overall emergency response communications plans.

Consider the following topics in the development of training and exercise plans:

- Participation from all levels and functions of emergency response (i.e., local, State, Federal, fire, law enforcement, emergency medical services)

- The frequency of training

- Who will conduct the training

- Does the training include multi-discipline and/or multi-jurisdictional interoperability exercises?

- The site at which training will be held (on-site or specified training facility)

- Maintenance efforts to keep personnel up-to-date with changes in procedure, equipment functions, or other relevant policies

- Incorporating lessons learned from training exercises in operational procedures

- Implementing post-exercise evaluations and analyses

- Requisite compliance or certification requirements for the course

- Including topics like the use of "plain language"

- Including a transition to a standard channel nomenclature for public safety interoperability channels (http://www.npstc.org/index.jsp)

No matter the level of management, planning, technology, SOPs, and training that an agency adopts, interoperability solutions must be an integral aspect of training so that staff becomes and remains familiar with the equipment and procedures. Emergency response personnel in high-stress situations depend on using equipment and procedures with which they are familiar and comfortable. Unless both operable and interoperable communications solutions are used as part of routine, daily operations, as applicable, they will not be used during major incidents. As with an agency's general staff, its supervisors and command staff must likewise be familiar with the equipment and protocols required to use the various communications solutions that are available to the agency if they are going to direct its activation. The best way to bring about such familiarity is daily use of and training with the solutions and their related equipment.

5. CRITERIA FOR STATEWIDE INTEROPERABILITY STRATEGIC PLANS

Section 5.1 – Purpose of Criteria

The FY 2007 Homeland Security Grant program and the FY 2007 Public Safety Interoperable Communications (PSIC) Grant Program required States to submit Statewide Communications Interoperability Plans and PSIC Investment Justifications by December 3, 2007.   If your State has not submitted a plan it is recommended that you contact the Office of Emergency Communications. As defined in the Homeland Security Act of 2002, the term "State" means, "any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." To assist this process and to ensure all States include the essential components of a statewide plan, the criteria of what must be included in the communications interoperability plan have been developed. The criteria were formulated with input from local and State practitioners. The criteria are outlined and explained in the Statewide Interoperability Planning Guidebook available at www.safecomprogram.gov

APPENDIX

A – ADDITIONAL DATA COMMUNICATIONS INFORMATION

WHAT IS DATA COMMUNICATIONS INTEROPERABILITY?

Data communications interoperability is the ability of emergency responders to exchange useful data on demand, when needed, and as authorized across separate systems, and software applications.
A few such examples include:

- Two separate computer aided dispatch systems sharing available resource status information to dispatch the closest resource to an incident
- Transportation systems sharing traffic related information with dispatch centers to route emergency response vehicles
- Dispatch systems sharing information with transportation systems to help route traffic around incidents
- Separate emergency operations center systems sharing incident related information
- Alerts being sent between various systems, software applications, and devices, regardless of vendor
- Publish location data to an open GIS platform or other such shared database

WHY IS DATA COMMUNICATIONS INTEROPEARBILITY IMPORTANT?

The use of data communications by the emergency response community is increasing at a rapid pace. Data interoperability must be addressed before the emergency response community has the same communication stovepipes that the voice world is currently working to overcome. Voice communications will remain a primary means of communication in most situations, but the ability to share relevant data when needed and as authorized, is becoming a frequent method of communication as technology advances and becomes more affordable. By sharing data across systems, disciplines, and jurisdictions, emergency responders are able to improve response time and save lives.

HOW DOES ONE ACHIEVE DATA COMMUNICATIONS INTEROPERABILITY?

- Preventing information stovepipes and eliminating turf issues that prevent information sharing.
- Developing partnerships and standard operating procedures with other agencies that outline agreements about what types of information will be shared, when information will be shared, and who will share information.
- Developing and/or purchasing systems that leverage practitioner driven data messaging standards

HOW DOES DHS IMPROVE DATA COMMUNICATIONS?

DHS is improving data sharing by developing tools, methodologies, and messaging standards that help emergency responders manage incidents and exchange information in real time. The primary

focus of DHS is facilitating the development of data messaging standards based on requirements obtained directly from practitioners.

DHS establishes working groups comprised of practitioners and technical experts to draft technical specifications which are then submitted to a Standards Development Organization (SDO) to be technically vetted and approved. Currently, DHS works with the Organization for the Advancement of Structured Information Standards (OASIS) to leverage their international technical perspective to review and finalize the draft standards. DHS also coordinates with the National Information Exchange Model (NIEM) by leveraging the NIEM data dictionary and NIEM Naming and Design Rules (NDR) for element/attribute extension requests. In addition, DHS utilizes and updates the NIEM Emergency Management Domain via a governance structure established by NIEM

Once standards are approved by OASIS, they become part of the suite of data messaging standards called the Emergency Data Exchange Language (EDXL). After the DHS standard is approved by the Standards Development Organization (SDO) it is reviewed by the National Incident Management Systems (NIMS) practitioner-based Technical Working Group for adoption by NIMS. NIMS will then add the standard to a messaging standards to a NIEM repository for re-use.

WHY SHOULD DATA MESSAGING STANDARDS BE IMPLMENTED?

Data messaging standards provide the technical foundation that allows data to pass between systems without changing the way responders view their applications. When implemented into industry and internally-developed software products and systems, data messaging standards enable the seamless exchange of data across disparate systems, software, and devices. This enables end users to purchase any system they choose rather than purchasing a system/software/device just because it is compatible with their neighboring jurisdiction.

WHAT ARE THE EDXL MESSAGING STANDARDS?

Below are the standards that have been developed by DHS and submitted to the SDO as of September 2007. New standards are continuously being developed and grant applicants should visit www.oasis-open.org for a current list of standards.

- **Distribution Element (DE)**
  DE 1.0 was adopted as a standard by OASIS in April 2006. DE provides flexible message-distribution framework for data sharing among emergency response related information systems. DE acts as a header by including key routing information to send a container by specific recipient(s), by a geographic area, or by other codes such as agency type (police, fire, EMS, etc.). The "container" can contain messages and files of any type (such as resource requests, alerts, situation reports, damage assessments, graphics, maps, etc.)

- **Common Alerting Protocol (CAP)**
  CAP provides the ability to exchange all-hazard emergency alerts, notifications, and public warnings, which can be disseminated simultaneously over many different warning systems

(e.g., computer systems, wireless, alarms, TV, radio). CAP allows for increased warning effectiveness while simplifying the warning task.

- **Hospital AVailability Exchange (HAVE)**
  HAVE was submitted to OASIS in January 2006. HAVE will enable the exchange of hospital status, capacity, and resource availability between medical and health organizations and emergency information systems. Final approval of the HAVE standards is anticipated in late 2007.

- **Resource Messaging (RM)**
  RM was submitted to OASIS in August 2005. RM standards will enable the seamless exchange of resource information, such as requests for personnel or equipment, needed to support emergency and incident preparedness, response, and recovery. Final approval of the RM suite of standards is anticipated in late 2007.

Currently, the DE and CAP standards have been vetted by OASIS and NIMS. Approval of HAVE and RM are expected in late 2007.

Implementation documentation and instructions for DE 1.0 and CAP 1.1 can currently be found respectively at:
- http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf
- http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf

Below is a table of the data messaging standards and the functionality they enable.

EDXL Standard	Functionality Enabled
Common Alerting Protocol	- Send alert to all emergency agencies in a specific area - Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions; - Multilingual and multi-audience messaging; - Phased and delayed effective times and expirations; - Enhanced message update and cancellation features; - Template support for framing complete and effective warning messages; - Compatible with digital encryption and signature capability; and, - Facility for digital images and audio.
Distribution Element	The primary use of the EDXL Distribution Element is to identify and provide information to enable the outing of encapsulated payloads, called Content Objects. It is used to provide a common mechanism to encapsulate content information. - Send report, map, generic file, of free form text to specific and/or large distribution groups - Provide an Open Container Model to enable dissemination of one or more emergency messages

	• Provide flexible mechanisms to inform message routing and/or processing decisions • Enable dissemination of messages based on geographic delivery area • Use and re-use of data content and models developed by other initiatives • Business process-driven specific messaging needs across emergency professions • Supporting everyday events and incident preparedness, as well as disasters • Facilitate emergency information sharing and data exchange across the local, State, tribal, national and non-governmental organizations of different professions that provide emergency response and management services • Multi-use format - One message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgments / error messages) in various applications (actual / exercise / test / system message.)
Hospital AVailability Exchange	• The ability to exchange data in regard to hospitals' bed availability, status, services, and capacity • The ability to allow emergency dispatchers and managers to make sound logistics decisions - where to route victims, which hospitals have the ability to provide the needed service.
Resource Messaging	• Provide a standard message format for the Resource Message • Provide separate specific formats for the discrete, distinct Resource Message Types • Enable dissemination of messages based on geographic delivery area • Use and re-use of data content and models developed by other initiatives • Business process-driven specific messaging needs across emergency professions • Supporting everyday events and incident preparedness, as well as disasters • Facilitate emergency information sharing and data exchange across the local, State, tribal, national and non-governmental organizations of different professions that provide emergency response and management services

B – FUNCTIONAL REQUIREMENTS FOR COMMUNICATIONS EQUIPMENT

For Voice, All Equipment Should—

- Support one-to-many and one-to-one communications

- Adhere to standards based architectures; devices should be interchangeable across different vendors.

- Allow for multiple frequency bands and architectures (e.g., conventional, trunked, hybrid, analog, digital).

- Allow feature interoperability across different vendors "out of the box".

- Protect the security of voice and data communications transmissions of emergency responders to the maximum extent possible, while realizing that in a real-time emergency, this is not the emergency response community's primary concern.

- Support advanced mission critical features as appropriate given the system type:
    - Support a system-wide panic button and alerts.
    - Support device- or user-specific identification and device information displays.
    - Be equipped with location technology.

For Voice, User Devices Should—

- Provide a battery life that can operate longer than a typical shift before requiring recharging (i.e., longer than 10 hours)

- Have a form factor that:
    - Has ruggedized casing.
    - Supports intuitive displays and functions similar to common devices such as cellular phones and LMR subscriber units.

- Support fixed or vehicular configuration and installation.

- Support mobile communications from common emergency response vehicles, including motor vehicles, helicopters, marine craft, and small planes.

- Support enhanced emergency response services such as priority service and E-911.

For Voice, Infrastructure Should—

- Communicate in as many locations of operation as possible (e.g., in-building and wide area coverage).

- Allow for adjustments:
  - Allow readjustment of the range and area of horizontal and vertical coverage at installation and during system reconfiguration.
  - Support seamless and continuous communications when users roam between connected networks and adjacent coverage areas.

- Provide flexible features useful during an emergency response:
  - Have sufficient backup power sources to support sustained operations during loss of power for the longest period of time anticipated to be required in an all-hazards environment at the location of that infrastructure.
  - Provide extra capacity for an emergency situation.
  - Provide system administration capabilities that are flexible and allow communications personnel to adjust various operating parameters.
  - Allow organizations the ability to establish specific user groups and networks for both preplanned and "on the fly" mutual aid, if appropriate given the system type.

- To enable command and control, allow for communications with various types of user devices (e.g., LMR subscriber units, pagers, cell phones, satellite phones) either through gateways or directly.

- Ensure the identity of the user and the device, if appropriate given the network.

- Support minimal performance requirements
  - Mouth-to-ear delay of less than 200 ms.
  - Call setup time of less than 250 ms.
  - Immediate detection of critical failure of communications link, device, or function.

For Voice, Dispatch Equipment Should—

- Support monitoring and recording of voice traffic.

- Support interfacing with user devices and dispatchers on other systems.

- Support operations during power outages.

- Support flexible architectures that meet the majority of dispatch center configurations:
  - Support different levels of operator access.
  - Support centralized and remote usage and management.
  - Be able to provide customized user interfaces.

- Be able to interface with external applications (e.g., doors, alarms, sirens).

- Allow dispatchers to page unattended devices and allow users to see who paged them.

For Voice, Interoperability Solutions Should—

- Support voice communications links between disparate systems:
  - Local, State, Federal emergency responders, including DoD

- Commonly available communications system platforms (e.g., conventional and trunked LMR systems, multiple manufacturers, disparate frequency bands (i.e., VHF, UHF, 700 MHz, 800 MHz)
- Unencrypted, analog audio
- Hardware and software definable links
- Fixed solutions should be capable of at least seven simultaneous two-way linkages between systems

- Provide immediate availability of interoperability to users:
  - Fixed solutions should require users in the field to carry no additional equipment beyond their normally assigned subscriber units.
  - Fixed solutions should provide the capability to have always on, immediately available user communications links without the intervention of dispatch personnel.

- Support minimal level of communications delays between systems (i.e., less than 250 ms delay, allowing for buffering of audio to compensate for longer delays).

- Be easily configurable:
  - Have a Graphical User Interface (GUI) that is computer-based.
  - Take less than five seconds to execute technical steps to configure links
  - Allow for distributed control between dispatch centers.

- Provide ease of use with existing equipment:
  - Interface with existing equipment.
  - No adverse impacts on existing equipment.
  - Support of multiple technologies (e.g., leased lines, fiber, RF) to link communication systems.

- Deployable solutions should provide ease of use when used at an incident scene:
  - Capable of being transported to the scene of an incident via typical emergency response vehicles.
  - Capable of linking users on an ad-hoc basis using user devices that responding agencies bring onto scene.
  - Capable of being used in conjunction with cached user devices.

For Data, All Equipment Should—

- Support general data requirements:
  - Able to withstand harsh environments (e.g., casing of the device that is water-resistant, high-heat-resistant and rugged).
  - Adhere to industry guidelines on security configurations for operating systems and applications.
  - Use standardized technology that supports industry data protocols and that will interface directly with "off-the-shelf" laptops, hand-held computers, and personal digital assistants (PDAs).
  - Authenticate and authorize the devices with little or no interaction by personnel.
  - Provide seamless roaming and transfer between device types (cellular, satellite, WAN, LAN, WiMax, etc.)
  - Support current and pending locator technologies.

- Support resources, patient, and victim tracking technologies.

For Data, Interoperability Solutions Should—

- Support data messaging standards:
  - o All data sharing equipment should support the EDXL standards for data messaging.

- Support database queries and messaging:
  - Ability of incident commander to query real-time status of all users involved in the incident, including personnel, equipment, and vehicles.
  - Accessing and retrieving query results from Federal, State, local, and commercial databases.
  - Sending and receiving text and short messages.
  - Sending and receiving instant messages.
  - Sending, receiving, and downloading email messages with attachments.
  - Bulk file transfer (e.g., images, GIS overlays, building floor plans).
  - Devices capable of being used as wireless modems.

- Provide locating capabilities:
  - Support of two-dimensional and three-dimensional location technologies.
  - Devices capable of initiating an automated transmission to other users based on location information.

- Support full range of video transmission, from passive video (e.g., still photographs) to full-motion video:
  - Support video telephony.
  - Provide a minimum of 256 Kbps bi-directional bandwidth for video teleconferencing.
  - Compliance with International Telecommunications Union (ITU) standards are also strongly encouraged. The standards are as follows:
    - H.323 for video/audio
    - H.239 for content (such as Power Point)
  - More information on these standards can be found at www.itu.int

C – SAFECOM RESOURCES TO ASSIST INTEROPERABILITY ACTIVITIES

Based on practitioner input, the SAFECOM Program has developed guidance, tools, and templates on communications-related issues to assist local, tribal, State, and Federal emergency response agencies strengthen their interoperability efforts. A list of these resources is provided below. Each of these tools can be accessed at https://www.safecomprogram.gov.

Interoperability Continuum: Designed to help the emergency response community and local, tribal, State, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. These elements include governance, SOPs, technology, training and exercises, and usage of interoperable communications.

Operational Guide for the Interoperability Continuum—Lessons Learned from RapidCom: Documents Lessons Learned from RapidCom—an effort that improved command level

interoperability in ten high-threat urban areas—and lists key actions that practitioners should consider for each element of the Interoperability Continuum.

Statewide Communications Interoperability Planning (SCIP) Methodology: Based on lessons learned from the Virginia planning process, SAFECOM released the SCIP Methodology for integrating practitioner input into a successful statewide strategic plan.

Writing Guide for a Memorandum of Understanding (MOU): Provides questions to consider and example text to assist practitioners with the creation of an MOU between agencies or jurisdictions for the governance of an interoperability effort.

Creating a Charter for a Multi-Agency Interoperability Committee: Template and Questions to Consider: Provides questions to consider and example text to assist practitioners with the creation of a charter for a multi-agency communications interoperability committee.

Writing Guide for Standard Operating Procedures (SOP): Provides questions to consider and example text to assist practitioners with the creation of SOPs relating to an enhanced communications capability.

Improving Interoperability through Shared Channels v1: Helps State and local interoperability coordinators with the difficult task of creating a regional channel plan for interoperability. An effective regional channel plan can provide interim interoperability using existing resources until long-term solutions are put into place.

General Guidance and Recommendations for Interoperability-Related Governance: This document provides emergency responders and public officials with an explanation of why sound governance is important. It explains some common barriers to setting up governance structures; the role of governance in achieving communications interoperability; characteristics of successful governance models and effective bylaws, and examples of roles and responsibilities. The guidance document also includes a discussion of performance measures, methods used, and lessons learned by some communities as they developed their governance models.

Enhancing Statewide Communications Interoperability: SAFECOM Assessment and Recommendations on the Status of Governance in the State of Nevada: This document provides a set of recommendations to the State of Nevada on mechanisms to modify its governance model and improve communications interoperability. The recommendations will help Nevada implement its statewide communications interoperability plan. The SAFECOM program developed the document through work with the Nevada Communications Steering Committee, which is charged with developing the statewide communications plan, and local practitioners and policy makers throughout the State. The SAFECOM program will leverage the experience gained from developing the Nevada governance recommendations in case studies and models that can be used nationwide.

Public Safety Architecture Framework (PSAF) Volumes I and II: These documents assist emergency response agencies in mapping system requirements and identifying system gaps.

Statement of Requirements (SoR) Volume I, v1.0 and v1.1: This statement defines future requirements for crucial voice and data communications in day-to-day, task force, and mutual aid

operations. The SoR helps the emergency response community convey a shared vision that ultimately will help private industry better align research and development efforts with critical interoperable communication needs. The SoR provides specifications to manufacturers and enables them to build equipment that meets emergency responders' communications needs.

SAFECOM Technology Initiatives Brochure: This guide describes the SAFECOM technical initiatives such as the SOR and PSAF and explains how practitioners are impacted based on their role (i.e., emergency responders, State or local interoperability coordinator, political leadership, industry, etc.).

Disaster Management Data Messaging Standards Initiative Brochure: This guide describes the Disaster Management standards development process including practitioner input, industry input and partnerships in standards development. The brochure describes the current messaging standards and standards that are in development.

Plain Language Tool: This web site is intended to be a resource for first responder agencies that are interested in using plain language instead of coded language (e.g., 10-codes) during radio transmissions. The information on this web site will help agencies understand the effort, resources, and key actions required to implement a plain language initiative. The web site does this by providing:

- The reasons to move to plain language
- The process on how to transition
- A list of related documents and other media

D – List of Recommended Criteria

The following table summarizes the recommended criteria contained within this document. This list is designed as a quick reference guide for Federal grant programs and grant applicants seeking to quickly understand the criteria recommended by the guidance document*. This table is not intended for use by grant applicants in applying for Federal grant funding as each Federal grant agency has its own application forms.*

Eligible applicants: Federal funds that are allocated for improving public safety communications and interoperability are available to public safety agencies or organizations at the regional, State, local, or tribal level, including:	
☑	Emergency Medical Service agency
☑	Fire Service agency
☑	Law Enforcement agency
☑	An organization representing the aforementioned agencies
☑	Any emergency response agency listed as an eligible applicant in Federal grant programs that include this guidance
Eligible activities: The following are the eligible activities for which Federal funding that is awarded for interoperable communications may be used, subject to the statutory authority of the grantor agency:	
☑	Planning and Management
☑	Equipment Acquisition
☑	Training/Exercises
Demonstrate how the proposed activity will improve interoperability: To receive funding, the applicant must be able to convey an understanding of the first responder's needs and a clear path towards interoperability. Provide a summary that describes how the activity or activities for which funding is requested will fit into an overall effort to increase interoperability. At a minimum, the summary should:	
☑	Identify the activity or activities for which funding is requested, using categories listed in the eligible activities section.
☑	Define the vision, goals, and objectives of what is to be accomplished and how the proposed effort would fit in an overall effort to increase interoperability.

☑	Describe the specific problems or needs that are to be addressed.
☑	Identify any potential partners and their roles and staffing requirements, and provide information on any existing agreements such as a Memorandum of Understanding (MOU) or Mutual Response Agreement.
☑	Propose a detailed budget and timeline.
☑	Include an operational plan that addresses how the effort will be funded now and in the future.
☑	Describe the governance structure in place that will lead the proposed project, including membership, roles, and responsibilities.

Describe how the proposed activity, subject to the statutory authority of the grantor agency, will incorporate the principles and guidelines outlined in Section 4:

☑	If applying for funding to perform planning and management activities, address the principles and guidelines outlined in Section 4.1.
☑	If applying for funding to perform equipment acquisition, address the principles and guidelines outlined in Section 4.2.
☑	If applying for funding to perform training and exercise activities, address the principles and guidelines outlined in Section 4.3.

Develop and adopt a statewide plan for interoperability *(State Applicants Only—subject to the statutory authority of the grantor agency)*:

☑	Adhere to the criteria for statewide plans outlined in Section 5

Share Information on interoperability solutions, including, the items below *(Block Grant Recipients Only—subject to the statutory authority of the grantor agency)*:

☑	The amount of funding received for communications interoperability
☑	The organization receiving the grant funding
☑	Additional jurisdictions involved in coordination
☑	The timeline for the grant funding
☑	The ways that the Federal funding will be spent

Demonstrate National Incident Management System (NIMS) compliance:	
☑	Demonstrate NIMS compliance based on the most recent compliance criteria available at http://www.fema.gov/emergency/nims/nims_compliance.shtm

E – GENERIC EXAMPLES OF LINKING DISPARATE EMERGENCY RESPONSE COMMUNICATIONS SYSTEMS

Multiple approaches exist for linking disparate networks. Descriptions of common technologies are provided below.

Cross-Band/In-band Repeater Gateways

Although there are more robust solutions available today, repeaters still provide improved interoperability for agencies needing to link disparate systems.

Cross-band/in-band repeater gateways instantly retransmit signals input from one channel or system to another. These may be in the same or a different frequency band. Cross-band repeaters range from simple devices supporting frequency transfers across two bands (e.g., ultra high frequency (UHF) and very high frequency (VHF), to more complex devices capable of bridging multiple frequency bands (e.g., UHF, VHF Low Band, VHF High Band, and 800 MHz). Within minutes after arriving on the scene of an incident, a portable gateway can be quickly configured to support the frequencies of participating agency radios. Some of these solutions also allow access to disparate systems via Public Switched Telephone Network (PSTN).

Network-to-Network Gateways

Numerous initiatives are already underway to put into effect short-term integration technologies that provide a reasonable level of interoperability among disparate networks.

Network-to-network gateways provide radio interoperability during missions that require communications between diverse organizations using different systems and technologies across multiple frequency bands. Network-to-network gateways offer a standard way to link wireless infrastructures. These gateways are usually at fixed locations and often support the transmission between participating systems or more advanced features such as unit ID. As repeater gateways, many of these gateways allow access to disparate systems via the PSTN, as well as to allow data sharing. Ideally, these gateways operate in an "always-on" mode, requiring no set-up time; users need only switch their radios to the designated channel or talkgroup to initiate communications.

Minimum specifications have been developed for instances where gateway solutions, either cross band/in-band or network-to-network, are to be placed in effect. Where such interconnect devices are to be used, the following specifications should be followed:

- Operating Modes
  - The device must be able to retransmit the audio of radios that operate in different parts of the radio spectrum, use different modulation and access techniques, and use analog or digital encoding. However, the interconnect of multiple digital voice devices using disparate Vocoders is highly discouraged due to typically poor voice reproduction. The audio shall be distributed or switched throughout a shared audio distribution bus where it can be presented to and shared amongst all, or a selected subset, of radios interfaced to the device.

- Capacity
  - The device must support a minimum of four LMR radios in different operating modes. The ability to support cellular phones and the ability to connect to PSTN may be desirable.

- Power Sources and Physical Features
  - o The device must be capable of being powered either from vehicular power, battery power, or portable AC power sources.
  - o The device must accommodate being rack-mounted or standing alone in a portable enclosure. The device must be able to withstand shock and vibration typically encountered in field operations activity.
  - o The device must include documented cable specifications for audio (speaker and microphone) and control (push-to-talk, or PTT) in order to interface with the basic audio and transmit controls for standard off-the-shelf LMR manufacturers' subscriber units. Such units are typically employed by emergency responders.
  - o The device must have input mechanisms or modules that can support balanced or unbalanced two- or four-wire circuits.
  - o The device must have input mechanisms or modules that can transmit (TX) audio, receive (RX) audio, PTT, and Carrier Operated Relay/Carrier Operated Squelch (COR/COS) signaling. The ability for supporting Tone Remote Control (TRC) and Voice Operated Transmit (VOX) signaling is desirable. Further, some form of adjustable automatic gain control should be provided for each device interface.

- Control and Administration
  - o The device must provide local control to establish two or more talk groups of the radios or phone interfaces that are provided.
  - o The device must provide adjustable audio/PTT delay to the radio interfaces to accommodate unknown repeater operating parameters such as hang times and squelch trails.
  - o The device must be easily configurable with short setup times.

Console Interfaced Gateways

Similar to fixed network-to-network gateways, some consoles provide similar support either manually or electronically.

Console interfaced gateways (i.e., "patches") route audio signals from one channel or system to other channels or systems through a dispatch console, either by dispatcher intervention or by a pre-wired configuration through the console electronics, thereby supporting direct connections between disparate systems.

Shared Networks

Many States and regions have significant investments in large-scale, shared networks. These networks offer a high degree of interoperability within their geographic coverage areas, and can be linked to other networks through network-to-network gateways. Some of these networks meet the P25 suite of standards.

Shared networks have common backbone infrastructures and interfaces. These are often single-vendor solutions covering large geographic areas or commercial networks. The typical model calls for participating jurisdictions to purchase subscriber radios compatible with the network and to pay a monthly service fee.

Middleware Technologies

For information sharing and exchange, many regions have adopted middleware technologies, like Enterprise Service Bus and Messages Switches, to connect different applications. These middleware technologies, using one or more networks, are used to provide shared services in a region.

F – ADDITIONAL RESOURCES

The following Web sites provide additional information for applicants to construct their grant applications and to seek funding sources.

Association of Public Safety Communications Officials – International, Inc. (APCO). APCO is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of emergency response communications.
http://www.apcointl.org/

Bureau of Justice Assistance Local Law Enforcement Block Grants (LLEBG). Funds from the LLEBG program may be used for procuring equipment, technology, and other material directly related to basic law enforcement functions.
http://www.ojp.usdoj.gov/BJA/

CommTech. The CommTech Program within the Office of Science and Technology at the National Institute of Justice (NIJ) has a mission to assist State and local law enforcement agencies to effectively and efficiently communicate with one another across agency and jurisdictional boundaries. It is dedicated to studying interoperability options and making valuable information on that issue available to law enforcement, firefighters, and emergency technicians across the country.
http://www.ojp.usdoj.gov/nij/topics/technology/communication/welcome.htm

Justice Technology Information Network (JUSTNET). The official Web site for the Justice Technology Information Network under the National Law Enforcement and Corrections Technology Center, JUSTNET lists many grants and funding sources. It also contains various publications on communications interoperability issues.
http://www.justnet.org/

National Incident Management System (NIMS). NIMS, created by the Department of Homeland Security, is the Nation's first standardized management plan that creates a unified structure for Federal, State, and local lines of government for incident response.
http://www.fema.gov/emergency/nims/

National Information Exchange Model (NIEM). NIEM is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as to support the day-to-day operations of agencies throughout the nation.
http://www.niem.gov/

National Institute of Justice (NIJ). NIJ is the research and development agency of the U.S. Department of Justice. It is the only Federal agency solely dedicated to researching crime control and justice issues. Its Web site lists the most recent solicitations issued by NIJ.
http://www.ojp.usdoj.gov/nij/

National Public Safety Telecommunications Council (NPSTC). NPSTC is a federation of associations representing government telecommunications and security matters related to the public. NPSTC serves as a resource and advocate for public safety telecommunications issues.
http://www.npstc.org/index.jsp

National Telecommunications and Information Administration (NTIA). NTIA, an agency of the Department of Commerce, works to spur innovation, encourage competition, help create jobs, and provide consumers with more choices and better quality telecommunications products and services at lower prices.
http://www.ntia.doc.gov/

Office of Community Oriented Policing Services (COPS). COPS, within the Department of Justice, provides grants to tribal, state, and local law enforcement agencies to hire and train community policing professionals, acquire and deploy crime-fighting technologies, and develop and test innovative policing strategies. COPS-funded training helps advance community policing at all levels of law enforcement.
http://www.cops.usdoj.gov/Default.asp?Item=34

Federal Emergency Management Agency (FEMA). FEMA, within DHS, oversees the distribution of Departmental grant funds designed to enhance the ability of states, local and tribal jurisdictions, and other regional authorities in the preparation, prevention, and response to terrorist attacks and other disasters. Localities can use grants for planning, equipment, training and exercise needs.
http://www.dhs.gov/xopnbiz/grants/

Office of Justice Programs (OJP) Information Technology Initiatives. The OJP Information Technology Initiatives Web site offers access to timely and useful information on the information sharing process, initiatives, and technological developments. The funding section of this site provides information on both Federal and private funding sources, examples of innovative funding ideas, and tips on researching funding legislation.
http://www.it.ojp.gov/

Office of National Drug Control Policy, Counterdrug Technology Assessment Center (CTAC) Technology Transfer Program. The CTAC Technology Transfer Program assists State and local law enforcement agencies in obtaining the necessary equipment and training for counterdrug deployments and operations.
http://www.whitehousedrugpolicy.gov/science_tech/index.html

Organization for the Advancement of Structured Information Standards (OASIS). OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organization, along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets.
http://www.oasis-open.org/

SAFECOM Program. SAFECOM is the communications program of the Office for Interoperability and Compatibility (OIC) within the DHS. SAFECOM, with its Federal partners, provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues.
http://www.safecomprogram.gov/

Department of Homeland Security (DHS). A cornerstone of the DHS philosophy is a commitment to partner closely with other Federal agencies, State and local governments, first responders, and law enforcement entities to ensure the security of the United States. Its Web site explains how DHS and local governments can work together.
http://www.dhs.gov/

U.S. Department of Justice (DOJ). DOJ offers funding opportunities to conduct research, to support law enforcement activities in State and local jurisdictions, to provide training and technical assistance, and to put into effect programs that improve the criminal justice system.
http://www.usdoj.gov/

G – FREQUENTLY ASKED QUESTIONS

What is the Office of Emergency Communications?

What is SAFECOM?

What is SAFECOM's background?

Does SAFECOM provide funding for communications and interoperability?

What is SAFECOM's grant guidance?

What is the history of SAFECOM's grant guidance?

How has SAFECOM's grant guidance been used?

How is the grant guidance different from past versions?

How can agencies receive Federal funding?

What can grant funding be used for?

How much funding is available for interoperable communications?

How easy or difficult is it to obtain grants?

Does SAFECOM provide direction or advice for grant applicants?

What is Project 25 (P25)?

Does SAFECOM's recommended guidance allow for the purchase of equipment that is not P25-compliant?

With which standards in the P25 suite do equipment procurements need to comply?

Can grants be used to fund the purchase of interim interoperability solutions, such as gateways and backbone technologies to connect radio systems together?

Can grants be used to fund the purchase of equipment and interoperability solutions that operate in the public safety radio bands other than 700 MHz?

Who should be involved in interoperability coordination efforts?

Why has the grant guidance included the recommendation that states develop and adopt statewide plans?

Will statewide plans be evaluated?

Does SAFECOM evaluate grant applications?

How were the functional requirements that are contained within the grant guidance developed?

What is the Office of Emergency Communications?
New Title XVIII of the Homeland Security Act established the Office of Emergency Communications (OEC) within the Department of Homeland Security and charged that Office's Director with, among other duties, planning and overseeing the implementation and management of a new organization focused on interoperable communications. The OEC was created to support and promote the ability of government officials and first responders to continue to communicate in the event of a natural disaster, act of terrorism, or other disaster, and to ensure and advance interoperable communications capabilities nationwide. In support of this mission, the Office of the Director was established to oversee the transition of three programs from other DHS entities into OEC – the Integrated Wireless Network (IWN), the Interoperable Communications Technical Assistance Program (ICTAP), and the SAFECOM program (excluding its research, development, testing and evaluation, and standards functions2). In addition, the Director, OEC is to conduct periodic assessments of the state of interoperability and regularly report to Congress on progress toward achieving national objectives and the effectiveness of methods to address emerging emergency communications vulnerabilities.

What is SAFECOM?
The Department of Homeland Security's (DHS) SAFECOM program is creating the capacity for increased levels of interoperability by developing tools, best practices, and methodologies that emergency response agencies can put into effect immediately, based on practitioner feedback.

With its Federal partners, SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and Federal emergency response agencies. The scope of the community SAFECOM services is broad, and includes more than 60,000 local and state emergency response agencies and organizations. Federal customers include agencies engaged in emergency response disciplines—law enforcement, firefighting, public health, and disaster recovery—and agencies that provide funding and support to local and state emergency response organizations.

What is SAFECOM's background?
SAFECOM was established by the Office of Management and Budget and approved by the President's Management Council as an e-Government initiative in 2002. The program was created to coordinate all Federal efforts related to communications interoperability.
- SAFECOM was originally managed by the Federal Emergency Management Agency (FEMA), and was then transferred in 2003 to the DHS Science and Technology Directorate.
- In 2004, the Intelligence Reform and Terrorism Prevention Act (Public Law 108-458) established OIC and placed SAFECOM under OIC.
- In 2007, management and administration of the SAFECOM program (excluding its research, development, testing and evaluation, and standards functions was transferred to the Office of Emergency Communications.

Does SAFECOM provide funding for communications and interoperability?
SAFECOM is *not* authorized to provide funding for communications equipment. Although SAFECOM does not provide funding, it does provide coordinated grant guidance to maximize the efficiency and effectiveness with which emergency response communications and interoperability

---

2 These SAFECOM functions remained within the Office for Interoperability and Compatibility (OIC) within the Science and Technology Directorate.

grant dollars are allocated and spent. More information about finding and applying for DHS grant funding is available at http://www.dhs.gov/xopnbiz/grants/. Information about finding and applying for grants from all Federal agencies is available at http://www.grants.gov/.

What is SAFECOM's grant guidance?
In FY 2003, SAFECOM developed coordinated grant guidance to maximize the efficiency and effectiveness with which emergency response communications and interoperability grant dollars are allocated and spent. The guidance outlines recommended grant funding eligibility—including applicants and activities, application criteria, guidelines, and resources—to assist the emergency response community in strengthening interoperability. SAFECOM's grant guidance represents the first time every communications-related grant agency in the Federal Government has incorporated the same criteria for agencies receiving Federal funds for interoperable communications. The guidance is available at http://www.safecomprogram.gov/SAFECOM/grant/default.htm.

What is the history of SAFECOM's grant guidance?
Over the past three years, Federal agencies—principally DHS—have provided grants to local and state emergency response agencies, more than $2 billion of which has been used for interoperable communications. In FY 2003, SAFECOM developed coordinated grant guidance with input from the emergency response community. The purpose of the grant guidance is to maximize the efficiency and effectiveness with which emergency response communications and interoperability grant dollars are allocated and spent. Each year, SAFECOM updates its grant guidance to accommodate for changes in technologies, standards, and other conditions affecting the emergency response community.

How has SAFECOM's grant guidance been used?
Since its creation, SAFECOM's grant guidance has been incorporated in grant awards from the former Office of Grants and Training (G&T), FEMA, as well as the Department of Justice's (DOJ) Office of Community Oriented Policing Services. SAFECOM is working with the Department of Commerce's National Telecommunications and Information Administration (NTIA) to incorporate SAFECOM's grant guidance into NTIA's new interoperable communications grants.

Federal grant programs providing funding for interoperable communications can leverage grant guidance by including SAFECOM's recommended grant criteria in their grant application packages. Grant applicants can use the recommended criteria as they apply for interoperable communications funding. Identified tools and resources assist grant applicants in their interoperable communications activities.

How is the grant guidance different from past versions?
SAFECOM recently updated its grant guidance tool. The updated grant guidance features a new organizational structure aimed at improving the tool's clarity and accessibility, and new content that captures lessons learned:

- *Organizational Structure.* SAFECOM reorganized the guidance to clarify the recommended criteria contained within the guidance. The new structure provides users with a clear explanation of the recommended, eligible applicants and activities.
- *Content.* Updated content incorporates lessons learned and best practices to help the emergency response community strengthen interoperability through procurement decisions and statewide planning. The document includes new information on:
  - Project 25 (P25), and methods for ensuring equipment purchases comply with the standard

- o Recommended standards for data-related information sharing systems
- o Statewide planning criteria for developing comprehensive statewide plans
- o Capabilities assessment criteria for ensuring that technical assessment recommendations meet the needs of multi-jurisdiction emergency responses
- o Functional requirements for communications equipment that are aimed at informing procurement decisions
- o Tools and resources available to grant applicants to assist them in meeting recommended criteria

How can agencies receive Federal funding?

Each year, Congress appropriates billions of dollars to state and local agencies through Federal grant programs. State and local agencies can find and apply for this funding at Grants.gov (http://www.grants.gov/). Grants.gov is a web resource that provides agencies with a single access point for all grant programs offered by the Federal Government. Each individual grant program has specific application, eligibility, and award requirements defined by or left to the discretion of the Federal agency through statute. State and local agencies should adhere to these requirements when applying.

Over the past three years, Federal agencies—DHS, DOJ, Departments of Commerce and Transportation—have provided grants to local and state emergency response agencies. The eligible activities for which grant funding may be used varies from program to program. Information about finding and applying for grants from all Federal agencies is available at http://www.grants.gov/.

What can grant funding be used for?

Some programs permit agencies to use funding only for equipment purchases. Other programs permit agencies to use funding for a broad range of interoperable communications activities. A number of factors—governance, standard operating procedures, technology, training and exercise, and usage of interoperable communications—are critical to interoperability progress. As such, while it is important that grant applicants seek funding for equipment purchases, it is also crucial that applicants obtain funding for other critical, related interoperable communications activities.

Program funding from the Homeland Security Grant Program, managed by the DHS FEMA, has made possible a broad range of interoperable communications activities, including planning, organization, training, and exercises. Information on this grant program, as well as others offered by DHS, can be found http://www.dhs.gov/xopnbiz/grants/.

How much funding is available for interoperable communications?

Funding varies from year to year, depending on appropriations from Congress. Since September 11, 2001, DHS has provided more than $3 billion in grants for interoperable communications.

How easy or difficult is it to obtain grants?

The ability to obtain grants is based on the needs of the applicant and the availability of funds. DHS encourages all eligible groups to apply for grants, including funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from incidents of terrorism involving chemical, biological, radiological, nuclear, or explosive weapons and cyber attacks.

Does SAFECOM provide direction or advice for grant applicants?

SAFECOM's grant guidance provides the emergency response community with resources to assist in developing comprehensive grant applications for communications and interoperability-related funding.

It is important that grant applicants adhere to the respective grant program's criteria and requirements. Applicants should also recognize that all grant packages are different, and that most grant program application criteria change from year to year.

What is Project 25 (P25)?

P25 is a suite of eight standards intended to help produce equipment that is interoperable and compatible regardless of manufacturer. The P25 suite of standards involves digital Land Mobile Radio (LMR) services. It includes the following standard interfaces:

- Common Air Interface (CAI)
- Fixed/Base Station Subsystem Interface (FSSI)
- Inter Radio Frequency Subsystem Interface (ISSI)
- Console Subsystem Interface (CSSI)
- Data Network Interface
- Network Management Interface
- Telephone Interconnect Interface
- Subscriber Data Peripheral Interface

At the request of Congress, SAFECOM is working with the National Institute of Standards and Technology and DOJ to develop and implement a compliance assessment program to validate that P25 standardized systems are indeed P25-compliant, and that equipment from different manufacturers can interoperate. This is to ensure that Federal grant dollars are used appropriately.

P25 standards are constantly being defined and updated based on the efforts of the P25 working groups and steering committee.

Does SAFECOM's recommended guidance allow for the purchase of equipment that is not P25-compliant?

Yes. SAFECOM's recommended guidance does allow for the purchase of equipment that is not P25-compliant, provided there are compelling reasons for using other solutions. SAFECOM recommends that agencies requesting funding to replace or add radio equipment to an existing system that is not P25-compliant (i.e., procurement of new portables on an existing analog system) can be considered. The requirement is providing an explanation for how the agencies' radio selections will allow for improving interoperability or eventual migration to interoperable systems. However, SAFECOM discourages the procurement of a new system that is not P25-compliant. Absent these compelling reasons, P25-compliant equipment will be preferred for Land Mobile Radio (LMR) systems.

What standards in the P25 suite do equipment procurements need to comply?

Equipment procurements should comply with the relevant and completed standards within the P25 suite. Updated information on completed P25 standards and compliance requirements is available at http://www.safecomprogram.gov/SAFECOM/grant/default.htm.

Can grants be used to fund the purchase of interim interoperability solutions, such as gateways and backbone technologies to connect radio systems together?
Yes, fund requests should not be limited to the purchase of new radios. Grant applicants are also encouraged to pursue current and next generation interoperability solutions, such as gateways and backbone technologies that connect existing radio systems. These technologies may include, but are not limited to, Internet Protocol (IP) based solutions. These solutions may provide interim or long-term interoperability capabilities that obviate the need for new equipment or systems, and their implementation should not require the acquisition of new, non-P25 systems. Absent compelling reasons for using other solutions, communities considering new radio or system acquisitions are expected to migrate to P25-compliant equipment.

Can grants be used to fund the purchase of equipment and interoperability solutions that operate in the public safety radio bands other than 700 MHz?
Yes, the purchase of equipment and interoperability solutions is not limited to the 700 MHz band. Agencies should carefully consider and select equipment and solutions that provide the best fit within their current and longer-term radio system architectures, and that provide optimal interoperability for their geographic area. Careful transition planning to new equipment and solutions is extremely important.

Who should be involved in interoperability coordination efforts?
Interoperability coordination efforts should be multi-jurisdictional and multi-disciplinary. Representatives from emergency response organizations across all levels of government should be involved in interoperability planning, as identified by communications needs. Because it is important to identify when and why specific agencies are involved in planning efforts, communities should develop a list of participating agencies and a list of agencies that are not included in particular planning efforts.

Below is a list of agencies that may be considered for involvement in coordination efforts. This list is not exhaustive. Rather, it is a starting point for communities to begin considering organizations beyond widely recognized emergency response agencies, e.g., emergency medical services (EMS), fire response, and law enforcement.

- EMS
- Fire response
- Law enforcement
- Emergency management
- Public works
- Public health
- Utilities
- Transportation
- Tribal government
- Tribal law enforcement
- Disaster relief agencies
- Elected government officials
- Media
- National Guard
- Federal agencies that respond in your area

Why has the grant guidance included the recommendation that states develop and adopt statewide plans?

It has become increasingly clear to the emergency response community that communications interoperability cannot be solved by any one organization. The solution requires a partnership among emergency response organizations across all levels of government. State and local governments can play a central role in this solution by preparing comprehensive and integrated statewide plans that address the specific interoperability issues across emergency responder disciplines and jurisdictions. Because statewide planning is critical to ensuring strategic-cross jurisdictional and cross-disciplinary coordination, the FY 2007 Homeland Security Grant Program required the development and adoption of statewide plans as a condition of receipt of interoperable communications funding.

SAFECOM, in cooperation with input from local and state practitioners, has compiled and published criteria that will assist states in developing a comprehensive statewide plan. The criteria recommend a practitioner-driven approach involving local, tribal, state, and Federal stakeholders. The use of a practitioner-driven approach in a statewide strategic planning process will ensure that the perspectives of all emergency responders are included in the plan. In addition, this approach will ensure that states have comprehensive strategies for improving interoperability that take into account end-user needs.

Does SAFECOM evaluate grant applications?

SAFECOM does not evaluate or make decisions on grant applications. The Federal agency managing the grant program performs application evaluations.

How were the functional requirements that are contained within the grant guidance developed?

The functional requirements listed in the appendix of SAFECOM's grant guidance represent a compilation of different efforts defining functional requirements for emergency response communications. The appendix represents the InterAgency Board Standardized Equipment List, the P25 Statement of Requirements, and SAFECOM's Public Safety Statement of Requirements.