NFPA®

951

Guide to Building and Utilizing Digital Information

2016

NFPA®

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® DOCUMENTS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA DOCUMENTS

NFPA® codes, standards, recommended practices, and guides ("NFPA Standards"), of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in NFPA Standards.

The NFPA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on NFPA Standards. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Standards available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of NFPA Standards. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

REMINDER: UPDATING OF NFPA STANDARDS

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that NFPA Standards may be amended from time to time through the issuance of Tentative Interim Amendments or corrected by Errata. An official NFPA Standard at any point in time consists of the current edition of the document together with any Tentative Interim Amendment and any Errata then in effect.

In order to determine whether an NFPA Standard has been amended through the issuance of Tentative Interim Amendments or corrected by Errata, visit the Document Information Pages on NFPA's website. The Document Information Pages provide up-to-date, document specific information including any issued Tentative Interim Amendments and Errata.

To access the Document Information Page for a specific NFPA Standard, go to http://www.nfpa.org/docinfo to choose from the list of NFPA Standards or use the search feature on the right to select the NFPA Standard number (e.g., NFPA 101). The Document Information page includes postings of all existing Tentative Interim Amendments and Errata. It also includes the option to register for an "Alert" feature to receive an automatic email notification when new updates and other information are posted regarding the document.

ISBN: 978-145591309-1 (Print)
ISBN: 978-145591338-1 (PDF)

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Standards

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments or corrected by Errata. An official NFPA Standard at any point in time consists of the current edition of the document together with any Tentative Interim Amendments and any Errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of Tentative Interim Amendments or corrected through the issuance of Errata, consult appropriate NFPA publications such as the National Fire Codes® Subscription Service, visit the NFPA website at www.nfpa.org, or contact the NFPA at the address listed below.

Interpretations of NFPA Standards

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing the Development of NFPA Standards shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights referenced in, related to, or asserted in connection with an NFPA Standard. The users of NFPA Standards bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Standards.

NFPA adheres to the policy of the American National Standards Institute (ANSI) regarding the inclusion of patents in American National Standards ("the ANSI Patent Policy"), and hereby gives the following notice pursuant to that policy:

NOTICE: The user's attention is called to the possibility that compliance with an NFPA Standard may require use of an invention covered by patent rights. NFPA takes no position as to the validity of any such patent rights or as to whether such patent rights constitute or include essential patent claims under the ANSI Patent Policy. If, in connection with the ANSI Patent Policy, a patent holder has filed a statement of willingness to grant licenses under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, copies of such filed statements can be obtained, on request, from NFPA. For further information, contact the NFPA at the address listed below.

Law and Regulations

Users of NFPA Standards should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

NFPA Standards are copyrighted. They are made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making these documents available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to these documents.

Use of NFPA Standards for regulatory purposes should be accomplished through adoption by reference. The term "adoption by reference" means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA Standards, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Standards and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA standards during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101; email: stds_admin@nfpa.org

For more information about NFPA, visit the NFPA website at www.nfpa.org. All NFPA codes and standards can be viewed at no cost at www.nfpa.org/freeaccess.

NFPA®951

Guide to

Building and Utilizing Digital Information

2016 Edition

This edition of NFPA 951, *Guide to Building and Utilizing Digital Information*, was prepared by the Technical Committee on Data Exchange for the Fire Service. It was issued by the Standards Council on November 14, 2015, with an effective date of December 4, 2015, and supersedes all previous editions.

This edition of NFPA 951 was approved as an American National Standard on December 4, 2015.

Origin and Development of NFPA 951

In 2007, at the recommendation of the late Bill McCammon, NFPA Treasurer, a letter was advanced by the Metro Fire Chiefs Association (a joint section of the NFPA and the IAFC) and signed by six of the major international fire service organizations, requesting that the NFPA Standards Council embark on an effort to develop a standard on "data exchange" for fire departments.

As described in the letter, the purpose of the new standard would be to enable a higher level of technology penetration in the fire service to enhance data sharing and analytic capability. The issue was framed to support effective communication and information management on a routine basis and to enhance situational awareness before, during, and after disasters.

This information exchange need was identified as particularly critical with respect to the following:

(1) The ability to exchange geographic information between local systems and evolving regional and national systems to support such functions as vulnerability/risk assessment and coordinated incident management
(2) The requirements of evolving mutual aid and resource exchange programs
(3) The requirements for participation in systems designed to monitor local, regional, and national preparedness levels during times of high risk
(4) Fire and emergency service access to and utilization of critical infrastructure data collected and distributed through national systems

The effort was initiated to enhance the analysis of organizations, promote exchange of concepts and data development, focus on GIS systems efforts with an industry-wide perspective rather than a "one-off," per-organization approach, and streamline and maintain comprehensive inducements to invest in data systems for the digital age. Solicitation of members was approved by the Standards Council, and subsequent industrywide response created the membership necessary to draft code-type and scope documents. Efforts by that group at the initial meeting, held at the IAFC headquarters in Fairfax, Virginia, resulted in the Standards Council creating a committee and approving efforts to create a standard on Fire Service Data Exchange (NFPA 950) in 2008.

The new Technical Committee, Data Exchange for the Fire Service, met several times between November 2008 and February 2011 and produced a draft, approved by the Standards Council, to go out for public input in the Fall 2014 cycle. The 2015 edition of NFPA 950, *Standard for Data Development and Exchange for the Fire Service*, was its inaugural edition.

NFPA 951, *Guide to Building and Utilizing Digital Information*, was developed as a companion piece to NFPA 950. NFPA 951 offers guidance to organizations in building NFPA 950–compliant systems. This effort was undertaken in tandem with NFPA 950 and developed concurrently, thus maintaining consistency throughout the documents. This first edition of NFPA 951 is intended to be a building block for data integration in the fire service.

Technical Committee on Data Exchange for the Fire Service

Edward P. Plaugher, *Chair*
International Association of Fire Chiefs, SC [E]
Rep. International Association of Fire Chiefs

Andrew D. Bailey, U.S. Department of Interior, ID [E]
Talbot J. Brooks, Delta State University, MS [SE]
Leandro E. Cieri, City of Hartford Fire Department, CT [U]
Ron G. Corona, Los Angeles City Fire Department, CA [U]
Jeffrey P. Hartberger, Hilton Head Island Fire Rescue, SC [U]
Vickie Hodges, State Farm Insurance Companies, IL [I]
Sarah Ierley, Montgomery County Fire & Rescue Service, MD [E]
Kevin P. Kuntz, Insurance Services Office, Inc., NJ [I]
Louis A. LaVecchia, Milford, CT [SE]
Crystal McDuffie, APCO International, FL [SE]
Rep. Association of Public-Safety Communications Officials International Inc.
Nathaniel J. Melby, Town of Campbell Fire Department, WI [U]
Rep. Volunteer & Combination Officers Section
Jonathan W. Moore, Canterbury, NH [L]
Rep. International Association of Fire Fighters
Paul Morgan, Alameda County Regional Emergency Communication Center, CA [E]
Kenneth A. Pravetz, City of Virginia Beach Fire Department, VA [E]
Michael J. Price, Entrada/San Juan, Inc., WA [SE]
Jennifer Schottke, ESRI, VA [M]
Paul Siebert, Frisco Fire Department, TX [E]
James C. Smalley, Scituate, MA [SE]
Rep. National Alliance for Public Safety GIS Foundation
Christine Klingman Thies, City of Austin Fire Department, TX [U]
Chris Tubbs, Southern Marin Fire District, CA [U]
Michael F. Weins, Gartner, VA [SE]
Ty Wooten, National Emergency Number Association, VA [U]

Alternates

Thomas Dewey, Advanced Justice Systems, CA [SE]
Jay English, APCO International, FL [SE]
(Alt. to Crystal McDuffie)
Russell G. Johnson, ESRI, CA [M]
(Alt. to Jennifer Schottke)
Thomas R. Mueller, California University of Pennsylvania, PA [SE]
(Alt. to Talbot J. Brooks)
Thomas M. O'Toole, International Association of Fire Fighters, DC [L]
(Alt. to Jonathan W. Moore)
Kimber Rosehlle Pederson, U.S. Department of the Interior, ID [E]
(Alt. to Andrew D. Bailey)
Jamilatu Zakari, Austin Fire Department, TX [U]
(Alt. to Christine Klingman Thies)

Nonvoting

Marie E. Martinez, U.S. Department of Homeland Security, MD [C]

Chris Farrell, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents that establish frameworks to 1) provide for the identification, development, management, and exchange of essential data; and 2) enhance an inter-operable geospatial data environment for fire and emergency services. This includes documents that establish criteria for and promote the exchange and use of data in common formats critical to the support for decision making in all phases of administration, planning, prevention, preparedness, mitigation, response, and recovery.

Contents

Chapter 1 Administration **951–** 4
1.1 Scope. **951–** 4
1.2 Purpose. **951–** 4
1.3 Application. **951–** 4

Chapter 2 Referenced Publications **951–** 5
2.1 General. **951–** 5
2.2 NFPA Publications. **951–** 5
2.3 Other Publications. **951–** 5
2.4 References for Extracts in Advisory Sections. ... **951–** 5

Chapter 3 Definitions **951–** 5
3.1 General. **951–** 5
3.2 NFPA Official Definitions. **951–** 5
3.3 General Definitions. **951–** 6

Chapter 4 Process **951–** 6
4.1 General. **951–** 6
4.2 Technology Strategic Visioning. **951–** 6
4.3 Technology Strategic Planning. **951–** 6
4.4 Mission Requirements and User Needs. **951–** 6
4.5 Governance and Policy. **951–** 8
4.6 Interoperability and Scalability. **951–** 9
4.7 Planning and Implementation of NFPA 950: An Overview of Implementing Technology and Technical Standards for Fire and Emergency Service Organizations. **951–** 9
4.8 Technology Planning. **951–** 10

Chapter 5 Data Administration **951–** 11
5.1 General. **951–** 11
5.2 Data. **951–** 11
5.3 Management/Organization. **951–** 11
5.4 Data Models and Schemas. **951–** 11
5.5 Data Sources and Acquisition. **951–** 11
5.6 Security. **951–** 12
5.7 Maintenance. **951–** 12
5.8 Data Exchange. **951–** 13

Chapter 6 Data Sharing and Exchange **951–** 14
6.1 Introduction. **951–** 14
6.2 Addresses. **951–** 14
6.3 Date and Time. **951–** 14
6.4 Incident Typing Information. **951–** 14
6.5 Text. **951–** 14
6.6 CAD, RMS, CAD/CAD, CAD/RMS, and RMS/RMS Exchange. **951–** 14

Annex A Explanatory Material **951–** 15

Annex B Informational References **951–** 18

Index **951–** 19

NFPA 951

Guide to

Building and Utilizing Digital Information

2016 Edition

NOTICE: An asterisk (*) following the number or letter designating a paragraph indicates that explanatory material on the paragraph can be found in Annex A.

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex B. Extracted text may be edited for consistency and style and may include the revision of internal paragraph references and other references as appropriate. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

Information on referenced publications can be found in Chapter 2 and Annex B.

Chapter 1 Administration

1.1 Scope.

1.1.1* The intent of this guide is to provide guidance in the development and integration of information systems to facilitate information sharing and use. The resulting information systems should be designed to support a communications pathway for all relevant components of the national preparedness and response framework.

1.1.2* This guide provides information for the development of consistent methods, processes, and tools to capture, utilize, and share data within scalable information systems. This framework supports and sets the stage for effective data exchange at all operational levels and components.

1.1.3 The intent of this guide is to provide a framework and environment consistent with NFPA 950 that results in an information system for computer aided dispatch (CAD), record management systems (RMS), geographic information systems (GIS), and other associated data systems in common use by fire and emergency service organizations.

1.2 Purpose. The purpose of this guide is to help public safety users envision, plan, build, and maintain an operable, and scalable information system.

1.2.1 A standard approach is essential to manage, use, maintain, and exchange data. This guide assists fire and emergency service organizations in establishing a vision for information management within their organization.

1.2.2 Technology planning is an essential step in creating an integrated information management environment. NFPA 950 mandates a methodology for a step-by-step process for technology planning. This guide recommends a framework for the governance and oversight needed to establish an effective planning process based on NFPA 950.

1.2.3 To create an information system, the authority having jurisdiction (AHJ) must understand the specific requirements for the interoperable use of the data. NFPA 950 sets forth the overarching technical standards these requirements must satisfy. The information in this guide assists the agency in creating a flexible and scalable system that supports data sharing.

1.2.4 This guide provides references and resources for fire and emergency service organization personnel to help identify applications of and uses for data to improve the organization's ability to perform fire prevention, damage mitigation, emergency response, and recovery from emergency incidents.

1.2.5 This guide is a reference tool and job aid that provides practical guidance.

1.3 Application.

1.3.1 This guide was designed to be used by fire and emergency service organizations to develop an information structure and associated requirements and workflows common to fire protection delivery and management for emergency response and administrative use.

1.3.2 When implemented, this guide also creates an environment whereby fire and emergency service organizations will be able to identify best practices, internal and external to the agency, to ensure data operability in mutual and automatic aid environments.

1.3.3 The purpose of this guide is to describe for all levels of the organization the mechanisms for establishing a standards-based information management environment, which is an essential element for optimal functioning of fire and emergency service organizations. Effective information management is a key to be utilized in keeping fire fighters safe, improving outcomes, and satisfying performance metrics. An integrated information technology strategy that adheres to the specifications of NFPA 950 will accomplish these goals by achieving the following objectives:

(1) Establish and maintain accurate and up-to-date understanding of operations and the events that affect them
(2) Collect, organize, exchange, and discover through research relevant and authoritative information

(3) Proactively support community fire planning needs and activities
(4) Exchange information to establish data streams into and out of the field
(5) Integrate data from multiple internal and external sources
(6) Enable a higher level of collaborative decision making with other stakeholder partners
(7) Maximize value from technology investments

1.3.4 To achieve an NFPA 950–compliant data environment, senior executive leadership must support the decision to implement the framework principles described in this guide. For many in the fire and emergency services, managing information technology is a new endeavor. Therefore, this guide is written to enhance knowledge of fundamental information management principles in the context of the work that is done in the fire and emergency services. It is intended to enhance the knowledge of all members of the organization, as well as related entities, which is essential for successful implementation. This allows leadership the framework for implementing the department's technology plan in the context of a shared vision.

1.3.5* NFPA 950 is a standard that identifies the critical building blocks of a fire and emergency service organization's information management system. The standard provides a common framework for all departments regardless of size, shape, and technological resource availability. Embracing this framework will provide the foundation as an organization begins to assess its particular landscape, analyze its specific technology requirements, and develop a plan that fits its unique environment.

1.3.5.1 Figure 1.3.5.1 provides a framework for how an organization-wide strategy for information management can support the entire organization. A wide range of players within an organization contribute data, perform analysis, and exchange important field intelligence. Utilization of these key elements provides the framework for organizations and their members to perform their mission effectively and will enhance the overall safety environment. These different functions within a fire and emergency service organization also have different requirements for data and applications. The integrated information management platform illustrated in Figure 1.3.5.1 will support all of these key elements and the ability to leverage their respective expertise, perspectives, and skills within this data environment.

1.3.5.2 Figure 1.3.5.1 illustrates the concept behind this guide and NFPA 950. It addresses the four fundamental ways information is used to support the goals of a public safety agency. These four categories are as follows *(additional information for each category is detailed in Chapter 4 and in A.1.3.5).*

(1) Planning and analysis
(2) Data management
(3) Field operations
(4) Situational awareness

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this guide and should be considered part of the recommendations of this document.

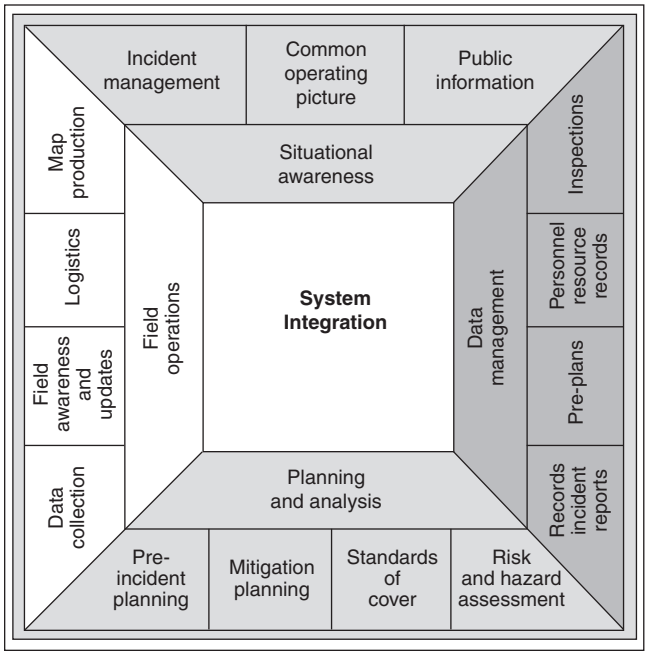

FIGURE 1.3.5.1 Information Systems Framework for Fire and Emergency Service Organizations.

2.2 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 950, *Standard for Data Development and Exchange for the Fire Service,* 2015 edition.

2.3 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2003.

2.4 References for Extracts in Advisory Sections.

NFPA 450, *Guide for Emergency Medical Services and Systems*, 2017 edition.

NFPA 950, *Standard for Data Development and Exchange for the Fire Service*, 2015 edition.

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter apply to the terms used in this guide. Where terms are not defined in this chapter or within another chapter, they should be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary,* 11th edition, is the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1 Approved. Acceptable to the authority having jurisdiction.

3.2.2 Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Guide. A document that is advisory or informative in nature and that contains only nonmandatory provisions. A guide may contain mandatory statements such as when a guide can be used, but the document as a whole is not suitable for adoption into law.

3.2.4 Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

3.2.5 Standard. An NFPA Standard, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and that is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA Manuals of Style. When used in a generic sense, such as in the phrase "standards development process" or "standards development activities," the term "standards" includes all NFPA Standards, including Codes, Standards, Recommended Practices, and Guides.

3.3 General Definitions.

3.3.1 Information System/Geographic Information System (GIS). Integrated sets of hardware and software that people and organizations use to collect, store, process, and communicate data; a GIS is used to analyze relationships, model processes, and display data spatially.

3.3.2 Interoperability. The capability of components or systems to exchange data or information with other components or systems, or to perform in multiple environments.

3.3.3 Response. The deployment of an emergency service resource to an incident. [**450,** 2013]

3.3.4 Scalability. The designed characteristic of a system that allows it to transition in size without showing negative effects.

3.3.5 Scalable. The ability to transition in size or complexity without showing negative effects.

3.3.6 Text Data. Data limited to display as ASCII characters. [**950,** 2015]

3.3.7 Workflow. A set of processes defined by procedural rules or a progression of steps, which can include automation, between activities in a project or function.

Chapter 4 Process

4.1 General. The purpose of this chapter is to describe the process of developing an information system to acquire, manage, use, and share information as it pertains to fire and emergency service functionsto successfully implement NFPA 950. The following are the main elements in this process:

(1) Visioning
(2) Technology strategic planning
(3) Ongoing needs assessment

4.2 Technology Strategic Visioning. A strategic visioning process helps to clarify where the organization, its employees, the political leadership, and other stakeholders see the organization in the future in terms of its fundamental objective and/or strategic direction. To be meaningful and relevant, a vision must be realistic and attainable. A strategic vision must inspire and motivate. Once a vision has been established, the next step is to translate the vision into action.

4.3* Technology Strategic Planning. Establishment of a strategic visioning construct is an underpinning to drive the technology strategy. Technology strategic planning is a tool that should end with objectives and a roadmap of ways to achieve the organization's vision. This section covers the fundamental steps in the strategic planning process.

4.3.1 A properly written strategic plan will provide the organization with the necessary guidance to develop resources needed to satisfy the vision. An effective strategic plan should be all-encompassing and constructed only after a deliberative process such as that suggested in A.4.3.

4.3.2 Critical to the strategic planning process will be learning how to incorporate technology, particularly geospatial technology, into the fabric of the organization's culture and mission. Fundamental to this process is the notion that technology planning is integral in supporting the overall strategic plan and vision. Technology planning must be developed in collaboration with technology professionals and a clear understanding of workflows. It is critical that an agency's relevant functions be incorporated into the technology planning process.

4.3.3 NFPA 950 is a standard for data framework that supports the workflows discussed in NFPA 951.

4.4 Mission Requirements and User Needs. A needs assessment is an integral part of planning. Conducted properly, it is a multitiered structured inventory process that provides the awareness needed to assist an organization through the process of planning for an information management system. Adherence to this process will help to avoid single-point solutions that operate as silos and fail. Each agency will have its own vision of how to fulfill its mission, which should be articulated in the strategic plan as described in Section 4.3. Once this mission is clearly understood and articulated in the organization's policy and planning documents, the technology planning committee will identify the workflows and associated applications that technology can support. The next step is to prioritize which of these will be included in the technology plan, based on mission priorities, cost-benefit timelines, and funding availability. It is the mission requirement that must drive the technology — not the other way around.

4.4.1 List of Workflows. Descriptions of some workflows that can be effectively supported by technology are given in 4.4.1.1 through 4.4.1.4.6. All of these should be considered to the extent they help the organization accomplish its vision. Table 4.4.1 provides some common examples of functions supported by a fire and emergency service organization information system or geographic information system (GIS), or both.

4.4.1.1 Planning. Planning is a multifaceted process that ranges from risk prevention to budgeting across all programs in fire and emergency service organizations. The proper application of technology provides a set of tools that can enhance the planning process. Effective data management leads to meaningful information for enhanced decision making. In

Table 4.4.1 Examples of Functions Supported by a Fire and Emergency Service Organization Information System or Geographic Information System (GIS), or Both

Planning	Preparedness	Response	Recovery
Capability assessment	Pre-incident planning	CAD, AVL, and routing	Damage assessment
Vulnerability/ risk assessment	Resource deployment	In-vehicle applications	Debris removal
Inspections	Targeted mitigation	Mobile/field intelligence	Infrastructure restoration
	Training and exercises	Search and rescue	Economic and community recovery
		Evacuation, shelter, and mass care	Environmental stabilization
		Public warning and notification	Public information
		Command and control	Analysis and management of recovery efforts
		Incident resource management	
		Multidisciplinary coordination	
		Operations dashboard	

particular, it is critical for decision making before, during, and after emergency response.

4.4.1.1.1 Capability Assessment. Capability assessment is a method for evaluating the stakeholder's ability to react to potential all-hazards incidents. A realistic and accurate assessment identifies potential risks, strengths, weaknesses, and the ability to respond. The data and analysis required to assess capability can be efficiently managed using various technology components.

4.4.1.1.2 Vulnerability and Risk Assessment. A vulnerability and risk assessment is one method for evaluating the stakeholder's liability. This assessment identifies potential loss and subsequent impacts to all stakeholders. Technology provides an increased capacity to assess vulnerability and risk and how they can be efficiently managed.

4.4.1.1.3 Inspections. Inspection efforts have the potential to produce substantial amounts of data. Technology can be used to more efficiently collect, update, and manage this data. Technology can also be leveraged to distribute this important information to multiple stakeholders, thus increasing the efficiency of process and systems. Properly implemented, technology can increase safety and focus limited resources to fill the greatest needs.

4.4.1.2 Preparedness. Preparedness is a continuous cycle of planning, managing, training, equipping, exercising, evaluating, and improving activities. Preparedness ensures effective coordination and the enhancement of capabilities of concerned organizations to prevent, protect against, respond to, recover from, and mitigate the effects of all-hazard incidents. The proper application of technology can help efficiently manage the implementation of preparedness efforts. Technology can be a tool to provide timely, critical information to stakeholders.

4.4.1.2.1 Pre-Incident Planning. A pre-incident planning process involves responder familiarization to specific site information. This information is documented for use by all responders. Typical site information might contain access points, automatic systems controls, enunciator panel locations, and travel routes through the building. Technology can help streamline the acquisition, management, and accessibility of this data.

4.4.1.2.2 Resource Deployment. Resource planning and deployment is a dynamic process. Proper resource management requires ongoing analysis. Technology can help agencies provide appropriate resources at appropriate levels.

4.4.1.2.3 Program Management. Program management, targeted mitigation, and special projects include specific programs and projects identified during the planning analysis process. This can include special projects such as accreditation, the identification of equipment failure trends, or incident patterns. Technology can aid in the execution, implementation, and management of various programs and targeted projects.

4.4.1.2.4 Training and Exercises. Training develops skill sets needed to perform a function. Exercises are a practical application of skill development. Training and exercises help ensure that staff have the skills to access the appropriate information from the appropriate technology when it is needed. Additionally, as technological tools are implemented in the agency, much of the success of these tools will depend on proper training.

4.4.1.3 Response. Response is a multifaceted process that ranges from single-resource to multijurisdictional incidents. The proper application of technology provides a set of tools that can enhance incident response and responder safety. Effective data management leads to meaningful information for enhanced decision making. In particular, it is critical for decision making before, during, and after emergency response.

4.4.1.3.1 Computer-Aided Dispatch (CAD). CAD is a suite of hardware and software used to initiate public safety calls for serviceand dispatch and to maintain the status of responding resources in the field.

4.4.1.3.2 In-Vehicle Applications. In-vehicle applications consist of hardware and software systems designed to send and receive information. This information is transmitted and received to create efficiencies in the delivery of services established in the organization's mission. These applications can range from a simple preloaded set of tools and data to a sophis-

ticated system with live data feeds from remote systems. These can include information from pre-incident planning databases with data on access and egress, water source, exposures, and hazards as well as real-time automatic vehicle location (AVL) and data exchanges with other systems.

4.4.1.3.3 Mobile/Field Connectivity. Mobile devices allow responders to send and receive information, assist in locating an incident, assess the incident, implement a response, and provide on-scene information regarding the incident status.

4.4.1.3.4* Search and Rescue (SAR). SAR is a multifaceted process that ranges from finding the lost (search) to bringing them back to safety (rescue). Technology is an integral part of search and rescue operations. Many of the datasets used across the planning, preparedness, response, and recovery phases serve a critical role in SAR operations.

4.4.1.3.5 Evacuation, Shelter, and Mass Care. Technology can support determination of suitable shelter locations and/or mass care operations, including supporting materials and power. Geographic information can be utilized to select shelter locations and route evacuated populations appropriately.

4.4.1.3.6 Public Warning and Notification. Public warning and notification consists of four primary methods: public warning systems, telephony, media, and push notifications. Technology has a significant impact on all four of these methods through faster relay, targeted audience, and control of the message.

4.4.1.3.7 Command and Control. Effective and efficient command and control requires accurate and timely information to fulfill the command function. Depending on the complexity and size of the incident, the information and data requirements can vary. Having access to essential information (including, but not limited to, GIS data) provides an accurate picture of the event and supports critical command decision making.

4.4.1.3.8* Incident/Resource Management. Incident command systems (ICS) organize personnel and resources to manage an emergency. A well-designed information system provides integrated support to the ICS components: finance, logistics, operations, and planning.

4.4.1.3.9* Multidisciplinary Coordination. Through the use of relational data, an integrated information system becomes an ideal platform for enhancing situational awareness and supporting collaborative decision making for events requiring multi-agency and multijurisdictional coordination.

4.4.1.3.10 Operational Intelligence. Technology synthesizes information from different and often disparate systems and delivers it to various platforms. This intelligence provides crucial support for decision making throughout the various functions of the organization.

4.4.1.4 Recovery. The aim of the recovery phase is to restore the affected area to its previous state. Recovery efforts are primarily concerned with actions that involve rebuilding destroyed property, re-employment, and the repair of other essential infrastructure. Recovering from a disaster can be a lengthy process. Technology can make the recovery process faster, more efficient, and available for archiving.

4.4.1.4.1 Damage Assessment and Debris Removal. Mobile devices enable field workers to code debris and parcels with descriptive attributes such as the type and degree of damage, time, and location. This data can be analyzed, queried, and visualized to assess specific problems and area trends. Reports and photographs of damage and debris can be linked to specific geographic sites. Pre-incident imagery and GIS data can be critical during damage assessment and assist during the reimbursement and recovery phase.

4.4.1.4.2 Infrastructure Restoration. After damage to critical infrastructure is assessed, short- and long-term actions can be determined for restoration efforts. Determining reconstruction priorities and costs can be enhanced by technology.

4.4.1.4.3 Economic and Community Recovery. Utilization of existing data and geospatial information enhances effective recovery of critical infrastructure, commerce, and displaced populations.

4.4.1.4.4 Environmental Stabilization. If an incident or response activities result in a disturbed environment, damages from such disturbances must be mitigated and the environment must be stabilized to reduce future damage. Mobile devices are often used to document and catalog needed rehabilitation/stabilization activities, while GIS software provides for visualization, prioritization, and progress tracking. Spatially enabled models provide impact analyses to determine the activities necessary to reduce the risk of future damage.

4.4.1.4.5 Public Information. Information can be published in many forms to facilitate transparency, encourage communications, and engage the public. Access to accurate information about the status of an incident, shelters, and access to supplies and services can be managed, maintained, reported on, and published in an enterprise database. Notification of ability to return, return routes, damage assessments, and reporting requirements (e.g., FEMA, insurance) can also be provided.

4.4.1.4.6 Analysis and Management of Recovery Efforts. The analysis of recovery efforts can integrate information using dynamic data, including incident locations, unit tracking, traffic, weather, and other relevant data. The product of the analysis can be queried based on various attributes including incident type, cause, time, units assigned, or other attributes. With a geospatial framework, organizations can manage the recovery efforts visually. This allows for incident analysis to be done quickly, displayed logically, and understood easily.

4.5 Governance and Policy.

4.5.1 Governance Structure. There are many ways to organize a strategic technology plan governing structure. There is no universal governance model. Determining the governance structure will be unique to each organization. The form of governance that will be most effective depends on many factors such as department size, resources, level of cooperation among stakeholders, existing system dynamics, level of regional coordination, and training. A technology needs assessment entity must have an authorizing document or charter. The governance structure that is selected must enable technology development, participant support, stakeholder representation, user involvement, and management commitment.

4.5.1.1 Governance Structure Scalability. The governance model should evolve as the organization's capabilities mature and should be as scalable as the system, resources, and demand require. This can be different for different-sized systems. They can be as simple or as complex as needed, ranging from an informal agreement with local community groups to large quasi-governmental entities with formal joint power agree-

ments (JPAs) and memorandums of understanding (MOUs) among AHJs and across regions and states.

4.5.2 Policy. The governing body must establish clear policies concerning technology and data access. Policies should be established that relate to both procedure and data management.

4.5.2.1 Procedural Policy. The AHJs must have clearly defined and aligned access policies as described in Chapter 5.

Procedural policies should address the following:

(1) Procurement (infrastructure and software)
(2) Maintenance (infrastructure and software)
(3) Security *(see Section 5.6)*
    (a) Security levels (user access)
    (b) Security system health
    (c) Internal use/misuse access policy
    (d) Protection of sensitive information
(4) Levels of IT support (when and who)
(5) Illegal or prohibited activities
(6) User application guidelines (including policy for standardized training)

4.5.2.2 Data Policy. The AHJs must have clearly defined and aligned access policies as described in Chapter 5. Data policies should address the following:

(1) Integrity *(see Section 5.1)*
(2) Security *(see Section 5.6)*
(3) Accuracy of data *(see 5.8.1.2)*
(4) Data validation and verification of data exchange *(see Section 5.8)*
(5) Data timeliness *(see 5.6.3)*
(6) Include spatial components with data *(see 5.8.1)*
(7) Provide metadata for all data *(see 5.7.2)*
(8) Quality assurance and control *(see 5.7.1)*
(9) Data exchange and compatibility *(see Chapter 6)*
(10) Shared data access policy *(see Section 5.6)*

4.6* Interoperability and Scalability. To maximize the investment of financial and personnel resources, an understanding of interoperable and scalable solutions is imperative.

4.6.1 Interoperability. In general, interoperability refers to the ability of emergency responders to work together seamlessly without any special effort. Emergency responders need to share vital data, information, and communications across disciplines and jurisdictions to respond effectively. Data and format must be compliant with Chapter 6 of NFPA 950 to be recognizable and exchangeable by all system users. This enables standardized analytical methods and decision making that lead to comprehensive situational awareness. Five critical success elements that must be addressed to achieve an interoperable data solution are as follows:

(1) Governance
(2) Technology planning
(3) Policies
(4) Process/application development
(5) Evaluation and feedback

4.6.2* Scalability. To be successful, a technology plan must incorporate the concept of scalability. Scalability implies that the information system will accommodate expansion when requirements evolve, technology advances, and/or funding becomes available. Historically, it has proven most effective to build an information system in manageable phases. The system needs to be able to expand or contract as requirements change. Adherence to the requirements in NFPA 950 will allow migration of valuable data as the system evolves, including legacy data.

4.7 Planning and Implementation of NFPA 950: An Overview of Implementing Technology and Technical Standards for Fire and Emergency Service Organizations. The single most important factor in successfully implementing technology within any organization is proper project planning and management. Technical projects seldom fail due to technology; rather, their failure results from lack of vision, poor planning, communication failures, and imperfect execution. Technical solutions are often attempted without a clear understanding of how the final system should work and are implemented without understanding the impact on users. It is essential that implementation of emergency services information technology adheres to NFPA 950, commencing with a thorough and well-guided needs assessment. All technical solutions must be standards-based and interoperable. Overall, a needs assessment should include the following steps:

(1) Identify the problem.
(2) Identify all parties affected by the problem.
(3) Assemble a representative group to guide the needs assessment process.
(4) Conduct start-up educational sessions.
(5) Interview potential participants and users.
(6) Synthesize results to create the optimal solution.
(7) Draft an implementation plan.
(8) Provide initial training and prepare for ongoing training.
(9) Implement the solution.
(10) Maintain and improve the system.

4.7.1 Identify the Issue. To identify the scope of the issue, the organization should review all data systems together rather than individually. For example, a department might dispatch companies to incidents using CAD, use a separate system to track responding or available companies (AVL), and use GPS for navigation on individual units — which might not work in an interoperable manner. On the surface, integration of all three technologies should be simple as all three technologies share a spatial common base. A deeper analysis of the issue reveals a myriad of challenges, such as multiple users, hardware, and different information systems. Complexity can increase exponentially if interoperability with neighboring departments and jurisdictions is required. By carefully defining the issue and the desired outcome before commencing any action, managers can identify solutions and pitfalls for data integration.

4.7.1.1 Using the Needs Assessment to Identify the Issue. The needs assessment process works best by identifying the issue(s), using consensus to fully scope and create the requirements, and defining and prioritizing the solution(s). Needs assessment findings should result in a clear issue statement, a listing of concerned parties, and a senior/executive level mandate for a solution The outcome of a needs assessment is a set of standardized documents that describe what needs to be created. The resulting system must be standards based and interoperable. *(See 4.8.3.)*

4.7.1.2 Issue Statement. After identification of the issue, an official issue statement should be created. The issue statement and the need for finding a solution should be issued as a department directive or mandate from the most senior execu-

tive level (e.g., chief of department or higher). This provides clear, empowering guidance to seek a solution to the issue and ensures management buy-in to the solutions process. Failure to do so can result in conflicting guidance, competing priorities, and a fragmented or compartmentalized solution that minimizes return on investment.

4.7.1.3 Role of Technology. Technology must be used to improve efficiency — whether through improved response times, appropriate staffing requirements, improved emergency response outcomes, or other measurable results. Implemented technologies must be interoperable within the larger context of fire and emergency service organization operations and management as achieved through the use of standards such as NFPA 950. Technology should never be implemented simply for technology's sake.

4.7.2 Identification of the Parties Involved. The needs assessment process is completed through a group empowered by a single convening authority. The group should represent the broadest possible base of potential stakeholders and include system users, managers, creators, and subject matter experts. This approach not only guarantees a diversity of ideas, but facilitates buy-in at all levels and promotes a high standard of quality throughout the development process, which mitigates "not invented here" syndrome and creates a sense of ownership among all stakeholders. A charter should be established outlining the goals, objectives, and responsibilities of the group.

4.7.2.1 Successful needs assessments are as inclusive as possible at the outset. Consideration should be given to fire fighters, telecommunicators, IT support personnel, and other potential contributors or collaborators. They can benefit not only an individual fire and emergency service organization but also the larger community.

4.7.3 Conducting Start-Up Educational Sessions. As per the charter, initial needs assessment committee meetings should serve to further revise the problem scope and educate participants about potential solutions. A determined effort should seek out case studies that document how similar problems were resolved using a standards-based approach in other places. Where permissible, committee members should experience solutions firsthand. These case studies and experiences guide the development of an educational session about the problem and potential range of solutions for presentation to the larger stakeholder audience by their representative committee members. Again, this approach facilitates maximum buy-in and establishes a high level of competence and awareness among stakeholder organizations. Education sessions represent an important opportunity for bi-directional information flow. Prudent committee members will capture comments from the stakeholder audience. Educational sequencing as recommended in this guide for technology efforts is as follows:

(1) Interviews with all potential participants and users
(2) Synthesize results to create the optimal solution
(3) Draft an implementation plan
(4) Training — and more training
(5) Putting the solution in play
(6) Maintenance and improvement

4.8* Technology Planning.

4.8.1 Needs Assessment. The needs assessment should take into consideration the following elements:

(1) Completion by a group through a single convening authority:
    (a) A diversity of ideas
    (b) Ensure buy-in
    (c) Quality assurance
(2) Identify the users:
    (a) Document workflow processes
    (b) Determine the level of technical competencies of users
    (c) Identify what a final product as applied to the desired outcome looks like
(3) Identify the issue. Look at the work flow process of the target audience and identify where technology will serve as a force multiplier or improve efficiency.
(4) Identify the desired outcome. A technological system of some sort that meets the requirements established by the needs assessment process and NFPA 950
(5) Identify technology elements that support desired outcomes:
    (a) List how the technology will be used to solve a problem, for example, computerized preplans
    (b) Note what type of functionality is required within each application to accomplish the goal, for example, a map that depicts the occupancies with preplan information
    (c) Data requirements:
        i. Data designs that meet NFPA 950
        ii. The data needed to support each application and their inherent functions
    (d) Data maintenance procedures: Identify who, what, when, where, and how each data element will be created and maintained, including who financially supports those activities
    (e) Determine how it will be managed:
        i. Fiscal responsibility (Who is funding the system and how?)
        ii. Accountability (Who manages the people, the hardware, etc.?)
        iii. Pitfalls and common mistakes (How do data and people's need drive the needs assessment process?)

4.8.2 Conducting a Needs Assessment. The needs assessment should be conducted in the following manner:

(1) A start-up meeting should be conducted to educate potential users about the present issue(s).
(2) Potential users should be interviewed about their specific job functions. All interviews should be documented in the following standardized way:
    (1) Each job function, importance, and frequency should be captured.
    (2) The data required for each job function should be identified.
    (3) Workflow should be documented.
    (4) Dataflow should be documented.

4.8.3 Develop an Implementation Plan. An implementation plan should include the stated purpose as well as timelines and budgets required to make the following components possible:

(1) Results of the needs assessment, which should cover the following:

(a) A systematic look at how entities within an organization view and use data
(b) A description of enhanced communication among users of like data types
(c) Its use as a basis for future learning

(2) A theoretical framework that describes in nontechnical terms how the ideal system works
(3) A survey that reviews the following:
(a) Internal and external data that will support all of the applications included in the plan
(b) NFPA 950–compliant hardware and software elements and combinations required to execute all the applications in the plan
(4) Detailed database planning and design, which includes a translation of the theoretical model (how the ideal system works in nontechnical terms) into the logical model (technical terms) used in the application
(5) Application development, as follows:
(a) Standardized data formats that will exist independently of the data sourced
(b) Data independence in accordance with NFPA 950
(6) Acquisition, as follows:
(a) Database construction and assembly of all required data elements into a single database
(b)* Acquisition and timing of hardware and software
(7) Pilot study/benchmark test
(8) Review and modification of original plan
(9) Implementation, as follows:
(a) Training
(b) Identification of gaps
(10) Release of the new system to production
(11) Maintenance (system continuous improvement cycle)

Chapter 5 Data Administration

5.1 General. Once a clear vision, strategy, and technology plan has been developed to implement the system, a data administration plan will guide the actual administration of the data environment. Chapter 5 frames the elements necessary for successful data administration. Developing policies and guidelines for the effective administration of an information system should be based upon need and is a function of the system architecture. Management of issues associated with data administration such as integration, security, replication, modification to, import and translation processes, and updates should be included in the policy in accordance with Sections 5.1 and 5.2 of NFPA 950.

5.2 Data. Data elements are a fundamental key to success. Understanding what data elements are available and their format is imperative to a technology's implementation success.

5.2.1 Internal and External Data. There is a distinction between internal and external data. This distinction is based upon the extent to which the data have been manipulated and integrated into the agency's information environment. These distinctions will vary depending on the specific system architecture and environment, local and regional policies governing data, and the choices of the strategic planning committee. While the approach will vary based on these factors, the strategic planning process should generate consensus on this distinction and on the ownership of data. These decisions should be cleary stated in the policies governing data administration.

5.2.1.1 For the purposes of this guide, external data is defined as data acquired from and/or maintained by an outside source. Once the data elements are integrated and maintained within internal information systems, it becomes internal data and should follow the internal data criteria in accordance with Section 5.3. While the same criteria should apply to validating internal and external data, policy definitions that affect the distinction between the data types should include specific language regarding the limitations and associated risks of using external data sources.

5.2.2 Additional Data. After review and analysis of technology and data needs, it might become evident that additional data is needed. This additional data will be included in the requirements of the new system.

5.2.3 Data Structure. Data can be stored in many formats and locations. To make use of the data, the data needs to be structured, compiled, and documented. The data is typically stored in a relational or tabular structure. This structure is defined by the user. Consideration should be given to data exchange and interoperability.

5.3 Management/Organization. There should be an overall data management plan for how data elements are used, shared, and exchanged. The data management plan should include the following:

(1) Objectives of the plan, including minimizing data redundancy, entry errors, and creating interoperability
(2) A properly designed data structure
(3) Standardized reporting

5.4* Data Models and Schemas. A data model, data dictionary, and database schema are defined as follows:

(1) *Data model.* A data model serves as the foundation of the database. A data model indicates what information is contained in the database, how the information will be used, and how the items in the database will be related.
(2) *Data dictionary.* A data dictionary standardizes the data elements and is a centralized repository of information about data such as meaning, attributes, relationships, origin, usage, and format. The data dictionary specifies the details of the objects in the database. A data dictionary is a useful tool for application developers and database managers to share information.
(3) *Database schema.* A database schema is a blueprint of how a database is constructed, which is based on the data model and defines the objects that are included in the database.

5.5* Data Sources and Acquisition. Acquiring data requires consideration of how the data are going to be used. Issues of accuracy, format, licensing, maintenance, and security are areas that need careful consideration. There are many sources and methods that can be leveraged to obtain or create data, including sources within the agency, from other agencies, from commercial data providers, or from data that the agency develops. Requirements for data acquisition should be defined by the specific uses and its associated applications.

5.5.1 Existing Data. Chances are that much of the data needed to support the agency's data requirements already exist in some format. The challenge comes in knowing where to look for the data.

5.5.2 Intra-Agency Data. The first step in determining data sources and acquisition should be to investigate what data have

been developed and are available from other local agencies. Many local governments have invested in extensive data gathering and collection and might already have many data elements that will be useful to supporting the functions of fire and emergency service organizations. Because much of the data that are used in the fire and emergency service organizations are spatial in nature, determining if a local agency utilizes geospatial technology is a key question to answer. Establishing a strong relationship with information and geographic information professionals (e.g., police, tax assessors, public works) will be key as the technological and data infrastructure is established, implemented, and maintained.

5.5.3 Free or Open-Source Data. Many sources of data are publicly available (e.g., USGS, Geography Network) at low or no cost to the user. This data can come at varying degrees of accuracy and in many formats. As with any data, it must be verified that it meets the requirements to support the anticipated functions.

5.5.4 External Agency Data. Other sources of data are governmental or quasi-governmental agencies, including county, state, or federal governmental agencies, associations of government, and regional authorities. Additional data might be available from water, wastewater, or other utility districts. GIS professional staff, if available, are a good resource for data that other agencies have and might make available for your use. They might already have agreements with these other agencies for the use of their data.

5.5.5 Commercially Available Data. Another source for many types of data is commercial data vendors. Many companies collect, compile, and maintain a wide array of information. This data can be purchased or licensed for use.

5.5.6 New Data. In each case, care must be taken to ensure that the accuracy and resolution is identified and consistent among sources and is adequate for the designated purpose.

5.5.6.1 Manually Generated Data. There are numerous methods for creating data to populate databases and/or GIS, including manual digitizing or data entry, document or map scanning, and conversion of existing digital data.

5.5.6.2 Data Collection. Data can be generated new from sources such as raw GPS data or remotely sensed data such as aerial photography, or by compiling sets of data from various sources like spreadsheets to create a new dataset.

5.5.6.3 Derived Data. New data can be created from existing information in systems such as CAD, RMS, and AVL. New data are generated from the output of these kinds of applications. Derived data also include the results of analysis such as drive time polygons and risk layers.

5.6 Security.

5.6.1 Permissions (Access and Sharing). An organization has the ability to subject its collected data to limitations related to distribution, public dissemination, or disposition of the information. Access to information can be limited to by role and/or type of data. These information-sharing rules and management responsibilities should be documented in the standard operating procedures (SOPs) and periodically reviewed as required in NFPA 950.

5.6.1.1 Role-Based Security. Role-based security can be divided into the following two use categories:

(1) *Internal use*: Access to data can be limited to select individuals who meet specific criteria. It can be categorized as "for official use only," or "for internal use only." It can be classified at various levels with appropriate legal penalties for dissemination.
(2) *External use*: Access to data can be limited for public dissemination information. These limitations should consider privacy issues, HIPAA compliance, and other data security, federal, state, and local regulations, laws, and ordinances. Through the Freedom of Information Act, the public reserves the right to request data from an organization.

5.6.1.2 Types of Data. The ability to access information can be limited to certain types of data. This includes access based on field selection, criteria query, or predefined ranges.

5.6.1.3 Conditional Access. Data can be released based on "need to know" or circumstantial criteria such as legal requirements or emergency events.

5.6.2 Security Features. Once it has been established that there are restrictions to the sharing of information, security features must be put in place. Security features can include system security, data exchange physical security, and metadata and life cycle maintenance.

5.6.2.1 System Security. Information can be secured by physical parameters such as a lock, digital keycard, or security token) or software parameters such as passwords and biometrics. Ideally, a two-factor authentication is recommended using something known such as a password, and something one has, such as a digital security token.

5.6.2.2 Data Exchange Physical Security. Data can be pushed out (all or selected fields) at one time or at periodic intervals, or pulled from either individual sources or a central data warehouse that is populated by contributing agencies. Once the information is gathered, similar rules can apply as to with whom the information can be shared.

5.6.2.3 Metadata and Life Cycle Maintenance. Once data have reached the end of their useful life, much of the data will become obsolete on their own. All open source/readily obtainable information can be disposed of in the easiest manner; however, many fields could retain sensitive information and will need to be disposed of by approved methods. Information can be archived, destroyed, or returned to the source.

5.6.3 Audit/Review. Once the security and distribution rules have been established, it is important to review these policies periodically to ensure that they are being followed and that they are still relevant.

5.7 Maintenance. Proper data maintenance ensures accuracy, currency, and relevancy of information used to support the workflows and functions of the organization.

5.7.1 Quality Assurance and Quality Control. The importance of quality data cannot be overemphasized. Accurate data is critical to the analysis and reporting phase, which is the purpose for collecting data. Where specific accuracy criteria exist, they should be stated so that errors are known and bound. Data resolution should be identified, since the accuracy can be only as good as the resolution of the data. The quality control function will include sampling of data to determine if it is within the required specifications. Report sampling should also be performed to ensure that report calculations and other data

manipulations are correct. The quality assurance procedure includes validating the practice of collecting the data and optimizing the process both from a data collection standpoint as well as a data accuracy perspective. Ensuring data is not corrupted, truncated, or transposed in the process of collecting information is critical.

5.7.2 Metadata (Models, Dictionaries, and Schema). Metadata describes the data that is collected, providing further details about the information. Good metadata simplifies the maintenance process by documenting the information that is collected and stored, as well as describing how it is used. Metadata includes a description of the database schema and it provides information on the structure and content of the data being collected. Metadata would include such characteristics as the name, size, and data type, as well as field lengths, hierarchical information, and information about the data source.

5.7.3 Update Intervals/Methods (per Data Element/Type). An up-to-date accurate address model can be used by many agencies to support many of their business functions. Successful data model implementations should include a plan and process to have contributing agencies regularly use and update the data. The update process will define parameters such as how often the information is updated, how to handle conflicts as well as archival instructions. Updates can vary by data type to include partial updates, such as an individual layer rather than the entire database. Update frequency varies with the type of data. Some fields can be updated as new information becomes available, while other fields can be updated on a monthly/quarterly or other periodic schedule.

5.7.4 Purge and Retention. As new information is updated, or as existing information becomes dated, a process is needed to define how long the data is stored and what to do with old data. Is the data purged, archived, or kept on the system? How are conflicts handled as new data are obtained? What is the medium for retention (e.g., disk, tape, on-line storage)? In addition, there might be security constraints on the old information such that a simple deletion might not be adequate, and additional processes or procedures might be needed (i.e., return information to supplying agency, purge via approved methodologies, or just archive old data and maintain for a specified period of time).

5.8 Data Exchange.

5.8.1 Spatial Data. Spatial data is data that has a spatial component that references a place on earth. Spatial data enables a comprehensive framework for managing and sharing intelligence through geographic awareness and data integration.

5.8.1.1 Spatial Data Component. A spatial data component gives a relative or absolute location to data. It can be an address or a geographic coordinate such as latitude and longitude or the U.S. National Grid (USNG). The added spatial component allows the user of the data to establish where the location is in relationship to the surface of the earth.

5.8.1.2 Accuracy and Precision. Data collection devices and data services identify accuracy and precision levels in their specifications. Accuracy is defined as the relative difference between the actual and measured location. Precision is defined as the repeatability of measurement within a given tolerance. It is important to be aware of the specifications and limitations of the device in use. The overwhelming majority of data required for use within fire and emergency service organizations when captured within 10 m of true location is of sufficient accuracy for meeting the requirements of NFPA 950.

5.8.1.3 Geographic Coordinate System. A geographic coordinate system (which by definition is unprojected) represents the surface of the earth in three-dimensional (round) geometry, such as degrees, minutes, and seconds. A projected coordinate system, such as State Plane or Universal Transverse Mercator (UTM) converts three-dimensional units into two dimensional (flat) or planar units such as an X,Y pair. Using an unprojected geographic coordinate system, like longitude and latitude, facilitates the exchange of spatial data between different software platforms, agencies, and systems.

5.8.1.4* Symbology. Symbology is the set of conventions, rules, or encoding systems that define how geographic information is graphically represented on a map. A characteristic of a map feature can influence the size, color, and shape of the graphic used. An attribute must exist for symbol class that depicts the geographic feature or resource type and capability using an appropriate symbol. Other specialized symbology should be clearly defined and agreed upon as part of the technology planning process established in Chapter 4.

5.8.1.4.1 Emergency mapping symbology are specialized sets of symbols used by various organizations when planning for or responding to emergencies. These emergencies can be naturally caused (tsunami, earthquake, tornado, etc.) or human caused (rioting, terrorism, hijacking, etc.). Currently there is no international standard for emergency mapping symbology, which means that various nations have created their own national symbology set. Recognized and standardized symbol sets help create a common operating picture (COP) for varied organizations that have been brought together during a crisis or emergency. Symbols that are easy to identify with and easy to distribute are seen as key elements in creating maps that can be used to reduce fatalities, injuries, or loss of property.

5.8.1.5 Labeling. Labels are used to identify and quickly communicate information about various features.

5.8.1.5.1 Having label attributes already available in the dataset simplifies the use of exchanged spatial data. If the dataset lacks the attributes needed for labels, the user will have to create or calculate them to produce meaningful maps quickly. For example, to display the coordinates of a helicopter landing zone on a map, the lat/long coordinates need to be recorded as attributes. If they are not an attribute, they need to be calculated before they can be labeled. The minimum attributes required for spatial data to be exchanged are listed in 5.3.1 of NFPA 950.

5.8.1.5.2* U.S. National Grid (USNG) is the national standard coordinate system established by the Federal Geographic Data Committee and was recognized by FEMA in 2001. It is NFIRS-compliant and is a useful supplement to all addressing needs.

5.8.2* Nonspatial Data. ASCII standard is an accepted format for exchanging text data. Other commonly accepted nonspatial file formats, such as JPG and WAV files, can be readily exchanged and used in their native formats. Using these industry-accepted standards facilitates the exchange of nonspatial data between different software platforms, agencies, and systems. The formats required for nonspatial data to be exchanged are listed in Chapter 5 of NFPA 950. These standards have been identified for their universal acceptance and use.

5.8.3 TCP/IP Internet Protocol (IP). TCP/IP standard is an accepted protocol for transmitting and receiving data. It is the most common and incorporates acknowledgment of data transfers. Using these industry-accepted standards facilitates the transfer and exchange of data.

Chapter 6 Data Sharing and Exchange

6.1 Introduction. This chapter sets forth the technical specifications and business rules all fire and emergency service organizations should follow in creating an interoperable data sharing and exchange environment. The technical specifications for acquisition, display, and management are set forth in the previous chapters. This chapter includes a description of the fundamental data components that need to be exchangeable and specifies the format for each of those data components. This in no way limits the AHJ from creating local policies with additional requirements, but for data exchange to be compliant, all components must, at a minimum, be in the formats specified within NFPA 950.

6.2 Addresses. This guide follows the protocols established by the Federal Geographic Data Committee (FGDC) and maintained by the U.S. Census Bureau. This format is most often and easily recognized by geocoding engines. It is readily accepted and recognized by responders and the general public. Addressing in many jurisdictions has traditionally evolved from non-standards-based conventions that do not follow these standards. This often creates challenges for agencies attempting to comply with nationally recognized standards such as NFPA 950. Several approaches exist to resolve these discrepancies. The jurisdiction should adopt a strategy that best fits the data and resource environment within which they operate. The most direct and short-term method for becoming compliant with NFPA 950 is to supplement the street address with a geographic coordinate (in accordance with NFPA 950, USNG, or latitude and longitude). While this will not make an address data NFPA-compliant, it will allow the agency or department to deliver services on time in the right place without a significant change to the jurisdiction's naming conventions.

6.3 Date and Time. NFPA 950 follows the most commonly recognized protocol currently in use in the United States. The committee recognizes that other date schemas are available and preferred by some agencies. This format is widely recognized by civilian and governmental agencies.

6.3.1 Time Stamp. It is recommended that the time stamp be recorded based on the incipient incident record time reference.

6.3.2 Decimal Time. Decimal time is a universal standard format that allows for numeric computations.

6.3.3 Time Reference. Time is referenced to the local time zone and UTC. The committee acknowledges that storing the date twice is redundant but recognizes the inconsistency of time zone applications across regional boundaries.

6.3.4 Time Calibration. Time calibration is a critical component of all incident record keeping because of the legal implications associated with incident response. As such, calibration provides a legal framework for incident records.

6.4 Incident Typing Information.

6.4.1 NFPA 950 recognizes the National Fire Incident Reporting System (NFIRS) and the National EMS Information System (NEMSIS) as the standard incident reporting systems currently required by most U.S. states and territories. This framework establishes a transferrable data set and as such meets the intent of NFPA 950. This guide does not imply the use of any particular software for recording incident data. This component of the standards refers only to the typing standards within these frameworks.

6.4.2 The "plus 1" append provides the local jurisdiction with an opportunity to amend data for local use. This gives jurisdictions the ability to review subsets of data for incident analysis.

6.5 Text. ASCII is a universally accepted text standard. Compliance with this protocol will enable ready transfer of text data using all of the standard data exchange methods specified herein.

6.6* CAD, RMS, CAD/CAD, CAD/RMS, and RMS/RMS Exchange.

6.6.1 Design and Construction. Design and construction of CAD/CAD, CAD/RMS, and RMS/RMS interfaces and applications should comply with all technical elements set forth in Chapters 4, 5, and 6 of NFPA 950. The integration of all department systems, including, but not limited to, CAD and RMS, must be considered at the design level. This guidance is intended to be device and software agnostic. Specific to incident response, this establishes the data framework required to support this essential mission element.

6.6.2 Intent. The intent of this language is to emphasize the importance of a seamless flow of data. This will enable appropriate utilization of data assets throughout the organization and into the entire public safety ecosystem. This environment will enhance data accuracy and drive the ability to leverage data resources for data driven decisions, comprehensive situational awareness, and essential communications to all stakeholders in the community. In short, unlocking data assets from proprietary systems and structures will provide the data environment that can support effective management.

6.6.3 Dynamic Technology. NFPA 950 specifically calls out CAD and RMS systems because these are the dominant nomenclature for computer applications currently in use to perform these functions at the time of this writing. NFPA 950 is written with the full understanding of a rapidly changing landscape. The implicit intention of the committee in the writing of NFPA 950 was to set forth a standard that applies any information system designed to aid in the analysis, visualization, and distribution of data intended to support the fire and emergency service organization mission.

6.6.4 Spatial Data Influence. When an emergency occurs, spatial data becomes an important backdrop to the entire sequence of events. From the moment a 911 call is received, an accurate incident location is the one attribute that ties together and sifts through all the other information available to support a successful outcome. When that location is stored in a modern, standards-based, NFPA 950–compliant information system, it provides the foundation to everything else that follows:

(1) Call takers can confirm the accurate location of the incident.

(2) Station personnel can quickly reference the location.
(3) Digital route maps with standard symbology can augment the driver's situational awareness.
(4) Accurate hazard and hydrant locations support the scene size-up.
(5) Preplan layouts in scalable formats provide lifesaving detail for search operations and attack strategies.
(6) Incident Command assist data.

6.6.5 Accuracy. Call location, initial incident description, routes, locations of responding vehicles, water sources, exposures, hazards, access, and egress are all crucial, all about geography, and all need to be right.

6.6.6 All location data needs to be accurate, consistent with its intended use.

Annex A Explanatory Material

Annex A is not a part of the recommendations of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.1.1.1 The committee believes that in order for the data exchange concept to become a reality, all components must be integrated into a comprehensive information management system. All system components in this context include computer hardware, software, and procedures designed to support the capture, management, manipulation, analysis, and display of information.

This integration is the key element the committee used in the development of NFPA 950 and this guide. By using this approach, the committee believes the environment allows for improvements and development of comprehensive, integrated data and management systems that leads to improved incident and organizational decision making.

A.1.1.2 Data sharing at all operational levels and components refers to the vertical and horizontal integration data exchange. This enables the organization to share information seamlessly throughout.

Users seeking to implement NFPA 950 must be aware of the multifaceted aspect of information systems. Constituent components include the personnel used to staff such systems and the training involved to make them efficient, the hardware and software systems chosen, the well-documented processes that must be followed to achieve repeatable results, and the data stored or analyzed. While the scope of this guide is to provide guidance and best practices about data capture, storage, manipulation/query, retrieval, and presentation, the focus is on doing such in an interoperable fashion.

A.1.3.5 Comprehensive situational awareness is truly possible only when an effective information management strategy helps fire and emergency service organization personnel combine appropriate data and analysis to answer the right questions. By performing these analytics, expanded sets of information become available to support all functions of the agency.

Systems that support effective planning and analysis include the following:

(1) The transformation of current and historic data into actionable information
    (a) Integration of information from disparate systems
    (b) Capture and reuse tradecraft (analytical models)
(2) Community risk and vulnerability analysis
    (a) Augment fire fighter safety
    (b) Community characteristics (physical and social)
    (c) Protection priorities (critical infrastructure)
    (d) At-risk communities /neighborhoods
(3) Preplanning and response analysis
    (a) Resource optimization (staffing, location allocation)
    (b) Response analysis (routing, service areas)
    (c) Demand for service (incident density maps)
(4) Return on Investment (ROI) analysis
    (a) Strategic /capital planning
(5) Actionable information and knowledge
    (a) Command center
    (b) In field collaboration
    (c) Partner organizations

Benefits of such a system include the following:

(1) Improved understanding of the community and its landscape
(2) Ability to prioritize and mitigate risk
(3) Improved ability to preserve life and property and reduce the consequences of emergencies
(4) Improved understanding of agency capacity and performance
(5) Quicker and more informed response
(6) Ability to develop a well-informed incident action plan
(7) Improved level of service
(8) Improved coordination
(9) Informed citizens

Data Management. To accomplish these kinds of analytics, fire and emergency service organizations need accurate information. Collecting, maintaining, and accessing data is central to providing a data environment to support the full range of system requirements.

Systems that support effective data management include the following:

(1) Management of relevant and authoritative content
    (a) Leverages a common information model
    (b) Access to online content
    (c) Supports sharing across roles and jurisdictions
(2) The ability to organize and discover information using a mission/role-based context
    (a) Mission (plan, respond, recover)
    (b) Stakeholders (internal and external)
    (c) Workflow focus
    (d) Support for metadata
(3) Access and exchange of information through multiple mediums
    (a) Intelligent maps (analytical capability included in the delivery of the map)
    (b) Apps
    (c) Services (geoprocessing, locator, etc.)
(4) The ability to collect information from multiple sources
    (a) Supports multiple platforms (desktop, mobile, web)
    (b) Supports integration with other information systems (web services)
    (c) Multiplatform real-time data collection

Benefits of such a system include the following:

(1) Improved access to relevant information
(2) Improved protection, prevention, response, and recovery
(3) Informed and consistent decisions
(4) Improved organizational efficiencies
(5) Reduced risk
(6) Positive public perception

Field Mobility. Increasingly data is supported on multiple devices for many different forms of field support. Safe and effective tactical response actually begins well before an emergency ever happens through years of training, planning, and information gathering.

Systems that support effective field mobility include the following:

(1) The effective exchange of information to and from the field
    (a) Integrated as part of overall system
    (b) Supports multiple mobile devices
    (c) Works in connected or disconnected environments
(2) Effective and safe response
    (a) Supports fire ground accountability
    (b) Supports an accurate and up-to-date COP
    (c) Supports effective resource allocation
    (d) Pre-plans
    (e) Routing
    (f) Hydrants /water sources
    (g) Community assets /hazards (utility networks)
    (h) Photo/floor plans
(3) Timely and accurate exchange of information and knowledge
    (a) Command centers
    (b) In field collaboration
    (c) Mutual aid partners

Benefits of such a system include the following:

(1) Quick and more complete event assessment, ensuring timely and effective response
(2) Improved decision making
(3) Better ability to track, manage, and prioritize field operations and resources
(4) More effective communication from and to the field
(5) Improved fire fighter safety
(6) Improved public service

*Situational Awareness.*Situational awareness systems include the following:

(1) An up-to-date and accurate comprehensive view of operations
    (a) Supports multiple platforms
    (b) Supports sharing across roles and jurisdictions
(2) The ability to collect, organize, exchange, and analyze authoritative information
    (a) Can be leveraged before, during, and after emergency incidents
    (b) Supports the ability to collect and leverage field observations
(3) Knowledge in an easy-to-understand, role-based interface
(4) Access to authoritative information
    (a) Base maps
    (b) Operational information
(5) Access anywhere, anytime, on any device

Benefits of such a system include the following:

(1) Improved ability to manage and monitor operations
(2) Improved decision-making
(3) Reduced risk
(4) Ability to measure organizational performance
(5) Improved internal and external communications
(6) Effective and efficient use of resources and investments
(7) Safe and satisfied constituents

Designing and building a standards-based integrated information management system will provide numerous benefits to the agency. As well, designing and building a standards-based integrated information management system will provide numerous benefits to partner organizations with shared goals and objectives.

Implementing such a vision will provide the agency with more information, more sources of data to draw from, and supplemental sources to aid in the decision making process. Shared and exchanged data enables smooth flow as the incident escalates. Data accuracy also becomes critically important in this process, because inaccurate or incomplete information can lead to poor decisions. These decisions can have an impact on first responder safety and the public.

A.3.2.1 Approved. The National Fire Protection Association does not approve, inspect, or certify any installations, procedures, equipment, or materials; nor does it approve or evaluate testing laboratories. In determining the acceptability of installations, procedures, equipment, or materials, the authority having jurisdiction may base acceptance on compliance with NFPA or other appropriate standards. In the absence of such standards, said authority may require evidence of proper installation, procedure, or use. The authority having jurisdiction may also refer to the listings or labeling practices of an organization that is concerned with product evaluations and is thus in a position to determine compliance with appropriate standards for the current production of listed items.

A.3.2.2 Authority Having Jurisdiction (AHJ). The phrase "authority having jurisdiction," or its acronym AHJ, is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his or her designated agent assumes the role of the authority having jurisdiction; at government installations, the commanding officer or departmental official may be the authority having jurisdiction.

A.3.2.3 Guide. There are other standards-making bodies that define the word *guide* differently.

A.3.2.4 Listed. The means for identifying listed equipment may vary for each organization concerned with product evaluation; some organizations do not recognize equipment as listed unless it is also labeled. The authority having jurisdiction should utilize the system employed by the listing organization to identify a listed product.

A.4.3 The basics needs assessment process required for adequate design and performance are best found in Tomlinson, *Thinking About GIS*, and Becker et al., *GIS Development Guide*.

A.4.4.1.3.4 The MapSAR Group has developed a set of protocols for using GIS to support wilderness search and rescue operations. These protocols can be extended to other types of SAR events as well. Access to group resources is open and available at no charge. To request an invitation to join the group website go to www.mapsar.net

A.4.4.1.3.8 For information on GIS use within ICS, see the National Wildfire Coordinating Group (NWCG) publication *GIS Standard Operating Procedures on Incidents*.

A.4.4.1.3.9 One example is a geospatial system that can be utilized to display incidents, units, target hazards, and available resources. Additionally, integrated information systems store valuable data that can contribute to data fusion centers, allow robust spatial analysis, and improve resource allocation.

A.4.6 Guidance with respect to specific hardware and software performance requirements and expectations can be found at this link:

http://wiki.gis.com/wiki/index.php/System_Design_Strategies_Preface

Investment in personnel trained to use information systems, especially those with a geospatial context, represent a significant investment of time and resources. The National Geospatial Advisory Committee provides sound advice for workforce development in support of efforts such as those proposed herein:

www.fgdc.gov/ngac/ngac-geospatial-workforce-development-paper-final.pdf

A.4.6.2 For scaling across the digital and paper environments, see Brooks and Swaminathan, "Integrating the Paper and Digital Environments for Crisis/Emergency Response: Lessons Learned."

A.4.8 The Capability and Readiness Assessment Tool Prototype prepared by the National Association for Public Safety GIS (http://www.napsgfoundation.org/) provides a video and general guidance about the inclusion of geospatial information for fire service information management and use. This tool is available at:

http://carat.napsgfoundation.org/index.cfm

A.4.8.3(6)(b) Hardware and software should not be purchased until late in the process to avoid depreciation.

A.5.4 Managing and integrating disparate data streams is at the core of NFPA 950. Environmental Systems Resource Institute (Esri) provides a solid geospatial data model in the work below.

A data model describes the thematic layers used in the application (e.g., hamburger stands, roads, and counties), their spatial representation (e.g., point, line, or polygon), their attributes, their integrity rules and relationships (e.g., counties must nest within states), their cartographic portrayal, and their metadata requirements.

The goal of data models is to provide a practical template for implementing GIS projects. Common data models are key to making better decisions based on available geographic information and are designed to provide immediate and long-term benefits to people working on real GIS projects while supporting existing standards.

Organizations representing the fire and emergency services have partnered with Esri to develop a national GIS data model to support regular and disaster-related operations at the local level. This effort will complement and extend existing national geospatial data models. The leadership team for the project includes representatives from the Metropolitan Fire Chief and Volunteer Fire Sections of the International Association of Fire Chiefs (IAFC), The National Association of State Fire Marshals, The National Alliance for Public Safety GIS (NA-PSG), and GIS specialists from the public and private sectors. The U.S. DOT Pipeline and Hazardous Materials Safety Administration (PHMSA) provided initial leadership and project support.

The purpose of this project is to provide reference solutions and information models to assist fire departments in managing geospatial data and implementing solutions. The solutions are incorporated into the local government information model available at http://solutions.arcgis.com/local-government.

A.5.5 Geospatial data can be found through a number of local, regional, and federal sources or can be created by a fire service agency. External sources include internet map services (web services) and internet portals. For guidance on assembling local datasets, see Price, *Fire Mapping: Building and Maintaining Datasets in ArcGIS*, which describes a process and sources for finding, assembling, and maintaining geospatial data.

A.5.8.1.4 Several standard symbology sets have been developed for emergency response and the fire service, including the following:

(1) NFPA 170

www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=170

(2) Federal Geographic Data Committee "Best Practices for Local Government Geospatial Programs":

www.fgdc.gov/ngac/ngac-local-gov-gis-best-practices-paper.pdf

(3) Homeland Security Working Group Symbology Reference

www.fgdc.gov/HSWG/index.html

(4) NAPSG Symbology Working Group:

www.napsgfoundation.org/the-incident-map-symbology-story

(5) NWCG ICS Symbology, pp. 50–52:

www.nwcg.gov/pms/pubs/gstop.pdf

A.5.8.1.5.2 The official USNG website is www.fgdc.gov/usng.

A.5.8.2 To standardize the exchange of data, two established protocols are specified as XML for the transfer of nonspatial data elements and GML for the transfer of geospatial data elements.

A.6.6 Several Association of Public-Safety Communications Officials International (APCO) operational standards reference CAD-to-CAD exchange: www.apcointl.org/standards

Annex B Informational References

B.1 Referenced Publications. The documents or portions thereof listed in this annex are referenced within the informational sections of this guide and are not advisory in nature unless also listed in Chapter 2 for other reasons.

B.1.1 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 170, *Standard for Fire Safety and Emergency Symbols*, 2015 edition.

NFPA 950, *Standard for Data Development and Exchange for the Fire Service*, 2015 edition.

B.1.2 Other Publications.

Fire Protection Research Foundation Report: A Collection of Geospatial Technological Approaches for Wildland and Wildland Urban Interface (WUI) Fire Events:

www.nfpa.org/research/fire-protection-research-foundation/reports-and-proceedings/other-research-topics/geospatial-technological-approaches-for-wildland-and-wildland-urban-interface-fire-events

Becker, P., et al., *GIS Development Guide*, Local Government Technologies Services, State Archives and Records, New York State, 1999.

Brooks, T. J., and S. Swaminathan, "Integrating the Paper and Digital Environments for Crisis/Emergency Response: Lessons Learned." *Proceedings of Global Spatial Data Infrastructures 12*. Singapore, Malaysia, 2011.

Esri, *GIS for the Fire Service*, Redlands, CA: Esri Press, 2012.

NAPSG Foundation, *GIS Geospatial Standard Operating Guidance for Multi-Agency Coordination Centers 2.0*, Washington, DC: NAPSG Foundation, 2011.

www.napsgfoundation.org/resources.

NWCG, *GIS Standard Operating Procedures on Incidents*. PMS #936/NFES #2809, National Interagency Fire Center, Boise, ID, 2014. gis.nwcg.gov/pms/pubs/gstop.pdf

Price, M., *Fire Mapping: Building and Maintaining Datasets in ArcGIS*, Redlands, CA: Esri Press, 2012. www.esri.com/library/ebooks/fire-mapping.pdf.

Tomlinson, R. *Thinking About GIS*, 4th edition, Redlands, CA: Esri Press, 2011.

B.2 Informational References. The following documents or portions thereof are listed here as informational resources only. They are not directly referenced in this guide.

B.2.1 Other Publications.

Sommer, S., and T. Wade, *A to Z GIS: An Illustrated Dictionary of Geographic Information Systems,* Redlands, CA: Esri Press, 2006.

B.2.2 Websites.

Esri information models: http://solutions.arcgis.com/local-government/fire-service

The Federal Geographic Data Committee: www.fgdc.gov

Standards for interoperability: www.opengeospatial.org/standards

Geospatial Intelligence Standards (GEOINT, NCGIS): www1.nga.mil/ProductsServices/geointstandards/Pages/default.aspx

International Organization for Standards (ISO) TC 211 Geographic Information/Geomatics: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=54904

ISO Technical Committee 211 and its scope of work (PDF): www.sbsm.gov.cn/pcgiap/bangalore/bangalore_isorep.pdf

North Carolina Parcel Data Draft Guideline (PDF): www.nationalcad.org/data/documents/NC%20Guideline%20Content%20Elements%20for%20Parcel%20Publishing-v5.pdf

Subcommittee for Cadastral Data: www.nationalcad.org

USGS National Geospatial Program: www.usgs.gov/ngpo

B.2.3 Sample Fire Technology Strategy. Henrico County Division of Fire, Henrico, VA, has developed a technology strategy (plan) utilizing NFPA 950 and the Committee feels is noteworthy as an example. It can be accessed at www.napsgfoundation.org/resources/nfpa-data-development-exchange-standard/

B.3 References for Extracts in Informational Sections. (Reserved)