NFPA® 951

Guide to Building and Utilizing Digital Information

2022

NFPA®

NFPA® 951

Guide to

Building and Utilizing Digital Information

2022 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 March 18, 2021, with an effective date of April 8, 2021, and supersedes all previous editions.

This edition of NFPA 951 was approved as an American National Standard on April 8, 2021.

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 International Association of Fire Chiefs (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 use 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 industrywide 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 building NFPA 950-compliant systems. This effort was undertaken 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.

The technical committee created a records management chapter, encompassing as many conceivable uses as possible for data, with explanations for how they should be used in each case.

The areas align with NFPA 950, which include restructuring other existing chapters to make them easier to use and access and coordinate with NFPA 950. There were also adjustments to reflect emerging and new technology not available during first publication.

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, US Department of Interior, ID [E]

Ron G. Corona, Los Angeles City Fire Department, CA [U]

Matthew Darley, W. S. Darley & Company, IL [M]

Jason Dolf, Aerial Services Inc, IA [U]

Vern Elliott, Leduc County Fire Services, Canada [U]

Tim J. Gardner, 3M Company, MN [M]

Peter D. Hallenbeck, Softwhere Syzygy, LLC, NC [M]

Jeffrey P. Hartberger, Hilton Head Island Fire Rescue, SC [U]

Jennifer Heatly, Austin Fire Department, TX [U]

April Heinze, National Emergency Number Association (NENA), VA [U]
Rep. National Emergency Number Association

Vickie Hodges, State Farm Insurance Companies, IL [I]

Cory James Hobs, HAAS Alert, IL [M]

Aaron Johnson, Rural/Metro Corporation, FL [M]

Kevin P. Kuntz, Verisk Analytics/Insurance Services Office, Inc., PA [I]

Louis A. LaVecchia, Milford, CT [SE]

Thomas Randall MacKay, The Arizona Fire & Medical Authority, AZ [E]

Robert W. McClintock, IAFF, DC [L]

Nathaniel J. Melby, Town of Campbell Fire Department, WI [U]
Rep. Volunteer & Combination Officers Section

Paul Morgan, Santa Clara County Fire Department, CA [E]

Clarence William Potter, Carrboro Fire Rescue, NC [U]

Vincent Powers, National Fire Sprinkler Association (NFSA), MD [IM]

Kenneth A. Pravetz, City of Virginia Beach Fire Department, VA [E]

David Rocco, StationSmarts, MA [IM]

Sarah Shola-Lachowicz, UL LLC, IL [SE]

Paul Siebert, Texas A&M Engineering Extension Service (TEEX), TX [U]

Stewart Smith, Emergency Reporting, WA [U]

Chris Tubbs, Southern Marin Fire District, CA [U]

Bart Van Leeuwen, Netage B.V., Netherlands [M]

Michael D. Varney, FirstNet, CT [C]

Daniel G. Walton, Intterra, CO [M]

Alternates

James Patrick Danylik, Los Angeles Fire Department, CA [U]
(Alt. to Ron G. Corona)

Gus Delgado, Austin Fire Department, TX [U]
(Alt. to Jennifer Heatly)

Billy Freeman, FirstNet Authority, VA [C]
(Alt. to Michael D. Varney)

Cynthia Giedraitis, National Fire Sprinkler Association (NFSA), TX [IM]
(Alt. to Vincent Powers)

Todd M. Iaeger, UL LLC, PA [SE]
(Alt. to Sarah Shola-Lachowicz)

Michael A. Mocerino, W. S. Darley & Company, IL [M]
(Alt. to Matthew Darley)

Thomas R. Mueller, California University of Pennsylvania, PA [SE]
(Voting Alt.)

Thomas M. O'Toole, International Association of Fire Fighters, DC [L]
(Alt. to Robert W. McClintock)

Kimber Rosehlle Pedersen, US Department of the Interior, ID [E]
(Alt. to Andrew D. Bailey)

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

NFPA 951

Guide to

Building and Utilizing Digital Information

2022 Edition

IMPORTANT NOTE: This NFPA document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notices and Disclaimers Concerning NFPA Standards." They can also be viewed at www.nfpa.org/disclaimers or obtained on request from NFPA.

UPDATES, ALERTS, AND FUTURE EDITIONS: New editions of NFPA codes, standards, recommended practices, and guides (i.e., NFPA Standards) are released on scheduled revision cycles. This edition may be superseded by a later one, or it may be amended outside of its scheduled revision cycle through the issuance of Tentative Interim Amendments (TIAs). An official NFPA Standard at any point in time consists of the current edition of the document, together with all TIAs and Errata in effect. To verify that this document is the current edition or to determine if it has been amended by TIAs or Errata, please consult the National Fire Codes® Subscription Service or the "List of NFPA Codes & Standards" at www.nfpa.org/docinfo. In addition to TIAs and Errata, the document information pages also include the option to sign up for alerts for individual documents and to be involved in the development of the next 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. 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 and extracted publications can be found in Chapter 2 and Annex C.

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 munial 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:

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

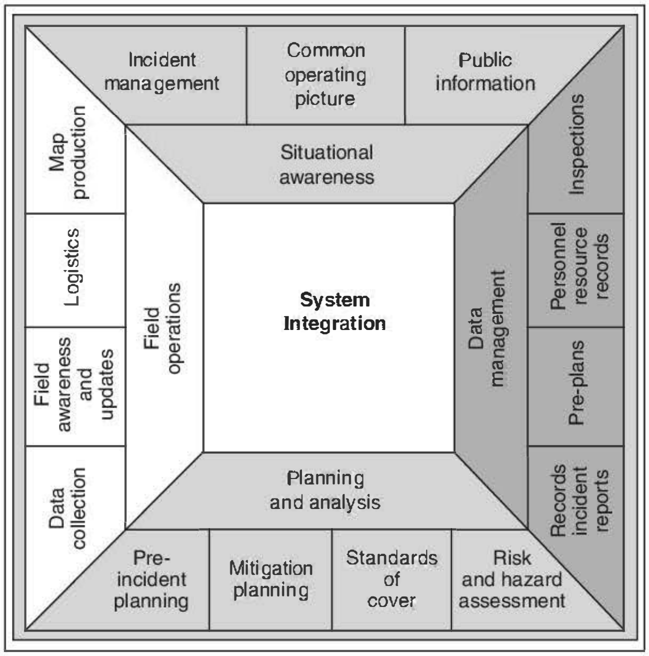

FIGURE 1.3.5.1 Information Systems Framework for Fire and Emergency Service Organizations.

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.

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

NFPA 921, *Guide for Fire and Explosion Investigations*, 2021 edition.
NFPA 950, *Standard for Data Development and Exchange for the Fire Service*, 2020 edition.
NFPA 1600®, *Standard on Continuity, Emergency, and Crisis Management*, 2019 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*, 2021 edition.

NFPA 950, *Standard for Data Development and Exchange for the Fire Service*, 2020 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,** 2021]

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,** 2020]

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 functions to successfully implement NFPA 950. The following are the main elements in this process:

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

4.1.1 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 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.

4.1.2* Technology Strategic Planning. Establishing a strategic visioning construct is an underpinning to drive the technology strategy. Technology strategic planning is a process 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.

4.1.2.1 A properly written strategic plan will provide the organization with the necessary guidance to develop the 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.4.1.2.

4.1.2.2 Critical to the strategic planning process will be learning how to incorporate technology, particularly geospatial technology, into the fabric of an 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 with a clear understanding of workflows. It is critical that an agency's relevant functions be incorporated into the technology planning process.

4.1.3 Mission Requirements and User Needs. A needs assessment is an integral part of planning. Conducted properly, a needs assessment 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 can help to avoid single-point solutions that operate as silos and fail. Each agency can have a unique community risk reduction approach and standard of cover. Agencies can use *NFPA 1600*® and its associated documents to develop and prioritize organizational objectives. Once understood, the technology planning committee can identify the workflows and associated applications certain technology can support. Mission priorities must drive the technology — not the other way around.

4.1.4 Governance and Policy.

4.1.4.1 Governance Structure. There are many ways to organize a strategic technology plan governance 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.

4.1.4.1.1 Governance Structure Scalability. The governance model should evolve as the organization's capabilities mature and should be as scalable as the system, resources, and demands require. This can be different for different-sized systems. The systems 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 agreements (JPAs) and memorandums of understanding (MOUs) among AHJs and across regions and states.

4.1.4.2 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.

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

4.1.5.1 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 its format must be compliant with Chapter 7 of NFPA 950 to be recognizable and exchangeable by all system users. This enables standardized analytical methods and decision making that can 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

4.1.5.2* 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, 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 of NFPA 950 will enable the migration of valuable data as the system evolves, including legacy data.

4.1.6 Planning and Implementation of NFPA 950: An Overview of Implementing Technology and Technical Standards for Fire and Emergency Services Organizations. The single most important factor for successfully implementing technology within any organization is proper project planning and management. Technical projects seldom fail due to technology; rather, their failure results from a lack of vision, poor planning, communication failures, and imperfect execution. Technical solutions are often created 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, beginning 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 the 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.

4.1.6.1 Identify the Issue. To identify the scope of the issue, the organization should review all the data systems together rather than individually. For example, a department might dispatch companies to incidents using Computer-Aided Design (CAD), using a separate system to track responding or available companies with automatic vehicle location (AVL), and using 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, different 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 of data integration.

4.1.6.1.1 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.

4.1.6.1.2 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 department directives or as mandates from the most senior executive level (e.g., chief of department or higher). This can provide 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.

4.1.6.1.3 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 services 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.

4.1.6.2 Identification of the Parties Involved. The needs assessment process is completed by a group empowered by a single convening authority. The group should represent the broadest possible base of potential stakeholders and should include system users, managers, creators, and subject matter experts. This approach not only guarantees a diversity of ideas, but it 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.

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

4.1.6.3 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 should guide the development of an educational session about the problem and a potential range of solutions for presentation to the larger stakeholder audience by the 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 should capture comments from the stakeholder audience. Educational sequencing, as recommended in this guide for technology efforts, is as follows:

(1) Interview all the potential participants and users.
(2) Synthesize the results to create the optimal solution.
(3) Draft an implementation plan.
(4) Train — and train some more.
(5) Put the solution in play.
(6) Maintain and improve the solution.

4.1.7* Technology Planning.

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

(1) Have a group complete an assessment 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 workflow process of the target audience and identify where technology can serve as a force multiplier or can 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 the desired outcome.
    (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) Note the data requirements.
        i. Data designs that meet NFPA 950
        ii. The data needed to support each application and its inherent functions
    (d) Identify the data maintenance procedures. Identify who, what, when, where, and how each data element will be created and maintained, including who will financially support those activities.
    (e) Determine how it will be managed.
        i. Fiscal responsibility (Who is finding the system and how?)
        ii. Accountability (Who manages the people, the hardware, etc.?)
        iii. Pitfalls and common mistakes (How does data and people's needs drive the needs assessment process?)

4.1.7.2 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 ways:
    (a) Each job function, its importance, and its frequency should be captured.
    (b) The data required for each job function should be identified.
    (c) The workflow should be documented.
    (d) The dataflow should be documented.

4.1.7.3 Develop an Implementation Plan. An implementation plan should include the stated purpose, as well as the timelines and budgets required to create the following components:

(1) The 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 the 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 of 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 independent of the data sourced
   (b) Data independence in accordance with NFPA 950
(6) Acquisition as follows:
   (a) Database construction and assembly of all the 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)

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

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

4.2* Data Sources and Acquisition. Acquiring data requires consideration of how the data is going to be used. Issues of accuracy, formatting, licensing, maintenance, and security 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 the associated applications.

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

4.3 Data Management/Organization. There should be an overall data management plan for how data elements are used, shared, and exchanged both presently and in the future. 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

4.3.1 New Data. There might be situations where new data elements need to be created. 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.

4.3.2 Data Structure. Data can be stored in many formats and locations. To make use of the data, it needs to be structured, compiled, and documented. The data is typically stored in a relational or tabular structure. The structure of internal data is largely defined and maintained by the AHJ. The AHJ might not have the ability to change the data structures from external data sources. All data structures should be documented to facilitate interoperability and usability. Consideration should be given to data exchange and interoperability.

4.3.3* 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 are related.
(2) *Data dictionary.* A data dictionary standardizes the data elements and is a centralized repository of information about data, such as its 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 it defines the objects that are included in the database.

Chapter 5 Data Administration

5.1 General. 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 on need and is a function of the system architecture. Management of issues associated with data administration, such as integration, security, replication, modification, import and translation processes, and updates should be included in the policy in accordance with Sections 5.1 and 5.2 of NFPA 950.

5.1.1 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 5.3.4)*
   (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 a policy for standardized training)

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

5.1.3 Manually Generated Data. There are numerous methods for creating data to populate databases or geographic information systems (GIS), including manual digitization, data entry, document or map scanning, and conversion of existing digital data.

5.1.4 Data Collection. There are many methods for creating data. Some examples include data entry, sensors, telemetry, imagery, and software systems.

5.1.5 Derived Data. New data can be created from existing information in systems such as Computer-Aided Dispatch, Records Management Systems, and automatic vehicle location. New data is generated from the output of these kinds of applications. Derived data also includes the results of analysis, such as drive time polygons and risk layers.

5.1.6 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 an entire database. Update frequency varies based on the type of data. Some fields can be updated as new information becomes available, while other fields can be updated on a monthly/quarterly basis or on another periodic schedule.

5.1.7 Purge and Retention. As new information is updated, or as existing information becomes dated, a process is needed to define how long the data should be 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 is obtained? What is the medium for retention (e.g., disk, tape, online 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., returning information to a supplying agency, purging it via approved methodologies, or just archiving and maintaining it for a specified period of time).

5.2 External Data. For the purposes of this guide, external data is defined as data acquired from 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 4.3. 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.

5.2.1 Free or Open-Source Data. Many sources of data are publicly available (e.g., the United States Geological Survey and the Geography Network) at low or no cost to the user. This data can be of 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.

5.2.2 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.

5.2.3 Commercially Available Data. Another source of 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.

5.3 Internal Data.

5.3.1 Internal vs. External Data. There is a distinction between internal and external data. This distinction is based on the extent to which the data has 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, as well as the choices of the strategic planning committee. While the approach will vary based on these factors, the strategic planning process should generate a consensus on this distinction and on the ownership of data. These decisions should be clearly stated in the policies governing data administration.

5.3.2 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 5.3.4)*
(3) Accuracy of data *(see 6.2.1.2)*
(4) Data validation and verification of data exchange *(see Section 6.2)*
(5) Data timeliness *(see 4.1.8)*
(6) Include spatial components with data *(see Section 6.2)*
(7) Provide metadata for all data *(see 5.3.6)*
(8) Quality assurance and control *(see 5.3.5)*
(9) Data exchange and compatibility *(see Chapter 7)*
(10) Shared data access policy *(see 5.3.4)*
(11) Data ownership *(see Section 5.1)*

5.3.3 Intra-Agency Data. The first step in determining data sources and acquisition should be to investigate what data has been developed and is available from other local agencies. Many local governments have invested in extensive data gathering and collection and might already have many data elements that can be useful to support the functions of fire and emergency services organizations. Because much of the data that is used in fire and emergency services organizations is 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, and public works) will be key as the technological and data infrastructure is established, implemented, and maintained.

5.3.4 Security.

5.3.4.1 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 by role or type of data. These information-sharing rules and management responsibilities should be documented in the standard operating procedures and periodically reviewed as required in NFPA 950.

5.3.4.1.1 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 to publicly disseminated information. These limitations should consider privacy issues, Health Insurance Portability and Accountability Act (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.

5.3.4.1.2 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.

5.3.4.2 Security Features. Security systems should be established for both internal and external data. Security requirements might be different between systems and agencies. Security features might include system security, data exchange physical security, and metadata and life cycle maintenance.

5.3.4.2.1 System Security. Information can be secured with physical parameters such as a lock, digital keycard, or security token or software parameters such as passwords and biometrics. Ideally, two-factor authentication using something known, such as a password, and something one has, such as a digital security token, should be used.

5.3.4.2.2 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.

5.3.4.2.3 Metadata and Life Cycle Maintenance. Once data has reached the end of its useful life, much of the data will become obsolete on its 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.

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

5.3.5 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 of collecting data. Where specific accuracy criteria exist, they should be stated so that errors are known and dealt with. Data resolution should be identified, as data accuracy is only as good as the resolution of the data. The quality control function might include sampling 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 data and optimizing the process both from a data collection standpoint as well as from a data accuracy perspective. Ensuring data is not corrupted, truncated, or transposed in the process of collecting information is critical.

5.3.6 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 by 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 might include such characteristics as the name, size, and data type, as well as the field lengths, hierarchical information, and information about the data source.

Chapter 6 Data Exchange

6.1 General.

6.1.1 Protocols. TCP/IP and UDP standards are accepted protocols for transmitting and receiving data. They are common and incorporate the acknowledgment of data transfers. Using these industry-accepted standards facilitates the transfer and exchange of data.

6.2 Spatial Data.

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

6.2.1.1 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 coordinates on 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.

6.2.1.2 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 an actual and measured location. Precision is defined as the repeatability of a measurement within a given tolerance. It is important to be aware of the specifications and limitations of a device in use. The overwhelming majority of data required for use within fire and emergency service organizations when device limitations and consideration are taken into account are of sufficient accuracy for meeting the requirements of NFPA 950.

6.2.1.3 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 in degrees, minutes, and seconds. A projected coordinate system, such as the State Plane Coordinate System or the Universal Transverse Mercator, 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.

6.3* Nonspatial Data. A UTF-8 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 6 of NFPA 950. These standards have been identified for their universal acceptance and use.

Chapter 7 System Design

7.1 General. System design often consists of using a variety of standard pieces of information, which will be discussed below.

7.2 Addresses. This guide follows the protocols established by the Federal Geographic Data Committee (FGDC) and is 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, United States National Grid, or latitude and longitude). While this will not make 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.

7.3 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.

7.3.1 Timestamp. It is recommended that the timestamp be recorded based on the incipient incident record time reference.

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

7.3.3 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.

7.4 Incident Typing Information.

7.4.1 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.

7.4.2 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.

7.5 Text. American Standard Code for Information Interchange (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.

7.6 Media. Computer databases require that a character set be specified for data storage. As such, systems using ASCII will be described as using the UTF-8 character set. Other commonly accepted nonspatial file formats, such as JPG, MPEG 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 6 of NFPA 950. These standards have been identified for their universal acceptance and use.

7.7* Computer-Aided Dispatch (CAD), Records Management Systems (RMS), CAD/CAD, CAD/RMS, and RMS/RMS Exchange.

7.7.1 Design and Construction. Design and construction of CAD/CAD, CAD/RMS, and RMS/RMS interfaces and applications should comply with all the technical elements set forth in Chapters 4, 5, and 6 of NFPA 950. The integration of all the 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.

7.7.2 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 a data environment that can support effective management.

7.7.3 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.

7.7.4 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, such as the following:

(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 can support the scene size-up.

(5) Preplan layouts in scalable formats can provide lifesaving detail for search operations and attack strategies.
(6) Incident command can assist with data.

7.7.5 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.

7.7.5.1 All location data needs to be accurate and consistent with its intended use.

Chapter 8 Data Development and Records Management

8.1 General.

8.1.1 Systems should allow for different levels of access to your information. As you are designing your systems, there are several things to keep in mind. Systems can be rank-based or position-based; however, you should be careful to avoid creating overly complex systems so first responders can remember what they can and cannot do within the system. There are several possible variables for access.

8.1.1.1 Determine the administrative configuration of systems. Consider the scope of needs for the user when designing the administrative configuration. Considerations for the scope should include the need to create, read, update, and delete systems (CRUD).

8.1.1.2 Consider the permissions to enter and change information. Examples include changing administrative and operational data, such as personnel demographics, preplan information, incident records, equipment maintenance, etc.

8.1.1.3 Understand the permissions to access information. In general, systems will have more people who view the information than those who actually change it.

8.1.2* The AHJ can choose to select either an all-in-one system or multiple systems that exchange data. There are advantages and disadvantages to either option.

8.1.2.1 All-in-one systems have the advantage of single points of support, a high level of integration, problem resolution, and single log on.

8.1.2.2 All-in-one systems have the disadvantage of limited options for selecting best-in-class solutions for records management.

8.1.2.3 The multiple systems approach offers the advantage of selecting products that best fit the requirements of the AHJ. When considering a scenario where multiple agencies are routinely sharing data across those agencies, the multiple systems approach might be the most effective method.

8.1.2.4 The multiple systems approach has the disadvantage of multiple points of integration, having to ensuring the interoperability of data, product updates that can create unforeseeable incompatibility, and multiple sources of support/input that might not agree on the source of the problem.

8.1.3 Determine the total system cost, which includes initial costs, training, materials, licensing, importing/exporting data, and ongoing support costs. Understanding the systems' total costs is critical to developing a cost/benefit analysis.

8.1.4 Determine the records retention requirements of the AHJ and determine the capabilities of the systems to meet those requirements. Understanding local, state, and federal requirements is key, as lifetime records might be part of the requirements.

8.2 Base Requirements for All Fire Department-Specific Software.

8.2.1 An agency should identify the business metrics by which they will see the benefit of the system and, as such, should feed the justification of the return on investment. These metrics can be valuable to the creation of a request for proposal and should be formalized early in the procurement process.

8.2.2 Determine the relative costs associated with importing existing data and exporting data to a third party. Develop requirements to ensure the vendor can import and export data into common formats that are easily accessible by the AHJ or their representatives.

8.2.2.1 Determine if your old records management system (RMS) can export all the data, including, but not limited to, the building inspections, roster, training records, and inventory. Also, determine if your new RMS can import and align the same records or data. Outliers and data that will be lost should be clearly recognized, understood, and planned for between the vendor and the AHJ.

8.2.3 Licensing can be based on a variety of terms, allowing for multiple options. The AHJ should understand these terms and the potential increase of costs over the life span of the system.

8.2.3.1 Identify the number of users that will be on the system at once and determine if the system provides the appropriate number of user licenses. Identify the costs associated with supporting the required number of concurrent users. Consider the projected increase of users over the short- and long-term system life.

8.2.3.2 Determine any potential costs within the contract that the AHJ might not anticipate, such as cancellation fees, software extensions, data storage, data communication fees, hardware requirements, hardware leases, etc.

8.2.4 Determine the devices and operating system supported by the software.

8.2.5 For mobile environments, validate that the devices can operate in the expected environment, including, but not limited to, the temperature operational range, vibration resiliency, particulate resistance, and liquid resistance. Data exchange can be degraded by system hardware, radio frequency interference, and connectivity performance issues. Understanding the limitations of location and cellular services is important to developing the expected system performance. The AHJ needs to evaluate both consumer- and industry-specific-grade devices and understand the trade-offs of both.

8.2.6 Determine the data bandwidth requirements and the costs associated with obtaining and maintaining the necessary bandwidth. The AHJ should request an analysis of the data bandwidth requirements of a proposed system from the vendor. The AHJ should consider operational environments where the software will be required — i.e., in large crowds with heavy data traffic usage on complex terrain versus a calm, uneventful time period when data usage is not high and flat and open terrain.

8.3 Record Collection and Records Management Software.

8.3.1 Standardized data requirements, such as NFIRS, for emergency incident documentation, such as the National Fire Incident Reporting System, should be gathered and exported to the appropriate authority.

8.3.2 Fire investigation requirements must be gathered and exported to the appropriate authority. The AJH should determine what information the fire investigation software needs to store, including the requirements of NFPA 921. Make sure that summary reports provide useful information for determined trends and that the information needed to generate a report can be entered by your investigation staff. Fire investigations typically cross the line between public information and criminal investigations, so significant consideration should be given to the viability of a system to maintain the necessary requirements for criminal justice compliance.

8.3.3 Quality assurance applications/processes should be able to identify if required fields are complete and valid prior to a data exchange. Many applications have integrated quality assurance capabilities, and they might also enable a person to review and approve information prior to exchanging data with other systems. Systems that include a human review for samples or the entire data set both enable verification that the quality assurance system is meeting the needs of the jurisdiction.

8.4 Personnel Scheduling, Safety, and Administration Software.

8.4.1 It is important to be sure that the scheduling and rostering software applications are capable of working from a single shared roster record with variable information as required by the AHJ. Entering a schedule or roster in multiple locations can be redundant work that might lead to errors that ultimately degrade the data or confidence in the system because of conflicting data. Scheduling and rostering data elements should be capable of being gathered and exported to other components of a system for use in reporting and analysis.

8.4.2 Health, wellness, and medical records contain protected information about patients and jurisdiction responders and require a higher level of security to protect and isolate the information. However, elements of the data should be capable of being gathered and exported to the appropriate authority. Data security for access and storage are key components of this category. Health information is used to identify responder exposure concerns, so the system needs the ability to redact reports for research or other external uses as required by the AHJ.

8.4.3 Occupational exposure and injury tracking software is a similar component to health, wellness, and medical records, but it is specific to a responder commonly associated with a specific jurisdiction. The data in this category should be able to be isolated from protected information while also allowing for statistical and individual analysis by the jurisdiction or research entities to improve safety in the field. Elements should be gathered and exported to the appropriate authority. Data security for access and storage are key components of this category.

8.4.4 Training, certifications, and qualifications software applications can be gathered, exchanged with, or exported to the appropriate authority. The ability to utilize a single shared roster will reduce the time spent on data entry and analysis and minimize data entry errors.

8.4.5 Human resources and hiring software applications can be gathered, exchanged with, or exported to the appropriate authority. In designing and procuring these applications, a critical component is data security, as well as the ability to redact information as needed.

8.5 Equipment and Facilities Software.

8.5.1 Equipment and facilities data should include sufficient information to maintain the vital data points for a given piece of equipment or a facility. Specific equipment will have variable data points. For example, SCBA will have hydrostatic test data specific to an individual bottle, while a structural firefighting jacket will have cleaning and length of service data. Software applications must have the flexibility to collect the data for individual equipment, allow for batch entry of data, enable analysis of data, and exchange the data with other systems. Facilities components should collect data relative to a specific geographic facility location, as well as the internal facility systems that might require maintenance or testing. Integration of equipment assigned to a specific facility should facilitate easy connection of data to the correct equipment or system and to the facility or other equipment, such as the apparatus or vehicles in which the equipment is stored.

8.5.1.1 The software should have the ability to create reports identifying issues with equipment and facilities. It should be able to be used by multiple responders at the same time, such as when performing truck checks at multiple stations at once. It should identify the time and person who checked off the equipment and allow for an explanation of any issues found that can be displayed in a report. Smart software systems should be able to perform relative software analysis and automatically generate deliverable reports identifying equipment or facility maintenance needs through scheduling or analysis of maintenance records.

8.5.1.2 Common fire industry areas of consideration here include equipment assets, consumable inventory, apparatus, vehicles, hydrants, water supply management, and physical facilities owned or operated by the AHJ.

8.6 Incident Command and Situational Awareness Software.

8.6.1 Applications should have sufficient information to enable the exchange of data to facilitate the display of a summary of information. If the software is to be used in the field, be sure the user interface is suited for field use on the devices your department uses in the field. Consider if the user interface in the given environment is usable. Determine if it is sufficient for the software to simply display all the incident information or display information relative to the responder's role in the incident. Note that most incident command software will need to have access to a greater number of pieces (or tables) of information than other software systems. As such, ensuring data exchange compatibility with this software is critical.

8.7 Analytical and Decision Support Software.

8.7.1 Analytical and decision support software includes applications that can be used preincident, during the incident, or post-incident or for many business purposes. These systems provide information to support the AHJ with decision making. This software is similar to situational awareness software; however, the user interface might be more robust and might not fit on a single screen. User interaction is often a critical component of the software system design. The AHJ should also decide if the software will be used offline or when there are no active incidents. If so, then it might be acceptable to have this software run in a desktop environment where there is more screen space and a mouse interface available. If capturing large amounts of internal or external data is important to the AHJ, consider the system capacity to store, manage, and retrieve the information within the system.

8.8 Risk Reduction Software. Risk reduction software should facilitate the identification and reduction of risk. The AHJ must ensure that the type of information entered into the system meets local needs and helps determine a definitive course of action. Data from risk reduction software is often used in situational awareness systems to alert those responding to a call to hazards in their vicinity. The AHJ should consider any evaluation or accreditation process they might utilize and validate that the proposed system will incorporate the requirements.

8.9 Imaging Software.

8.9.1 A wide variety of software and hardware solutions for capturing, storing, and transmitting imagery, both still and video, are available. These solutions can include imagery that predates an incident (preparedness and mitigation), that is at the scene of an incident, and that is evident during post-incident recovery. Consider the end user and their requirements when determining imaging software requirements. The use case could be responders at an incident, the incident command protocol/command center functions supporting an incident, post-incident investigation, or training.

8.9.2 Each use case has different requirements for capturing, storing, and transmitting imagery. It is critical to consider the infrastructure requirements for each use case. On-the-scene, real-time, or near-real-time video requires high-bandwidth connectivity in the field, while imagery that is loaded onto responder devices before an incident requires time and planning but reduces data bandwidth requirements.

8.9.3 It can be difficult to determine, ahead of time, all of the potential integration opportunities for imagery. For that reason, it is important to select software that supports integration with other systems via an API, as specified in NFPA 950. In addition to the imagery itself, location and timestamp information should be included with the imagery. This information is often useful for cataloging and searching for imagery post-incident.

8.9.4 It is critical that policies and procedures for the use, ownership, and distribution of imagery be established by the AHJ. These policies should be made clear to all the responders under the authority of the AHJ.

8.10 Sensor Software. Sensor technology is a rapidly evolving and developing field. Sensors provide information on the status and performance of both equipment and personnel, and they can provide information on pieces of equipment with no human intervention at all.

8.10.1 Sensor software applications should have sufficient contextual information to enable the exchange of information with responders and other systems, such as dashboards or situational awareness displays. This is a clear way to associate a sensor with whatever or whomever the sensor is attached to. The software should be able to manage timestamps for sensor readings. It should also accommodate different units of measure and measurement intervals. It might also be useful to have the software be able to exchange sensor history.

8.10.2 The AHJ should use best practices for data exchange when handling sensor data. Data sets should be in an acceptable, documented format, and the AHJ should be able to use the data in other systems at their discretion.

8.11 Community Risk Awareness Software.

8.11.1 Community risk awareness data is sufficient to enable the exchange of data to provide information to responders.

8.12* Digital Alert Warning Systems for Emergency Response Vehicles Software.

8.12.1 Systems should include an integration to identify the real-time location of the vehicle and an indicator of the vehicle's emergency response status — i.e. lights and sirens. Systems should integrate location information of the vehicle, as well as the status and location of other emergency response vehicles.

8.12.2 The AHJ should ensure that systems with vehicle location data share that data with other digital alert warning systems and should determine if additional costs might be associated with sharing data.

8.12.3 The information provided for all the above uses has two basic forms: information from a GPS and additional information that is specific to how the location information will be used.

8.12.4 GPS information should include all the basic information a GPS can provide: latitude, longitude, altitude in MSL (altitude above mean sea level), speed, heading, and accuracy. The units for these measurements should use native GPS units, which are metric. Additional information can optionally be provided, such as the number of satellites used, the status of the GPS system (on, off, or syncing), the source of the location information (GPS or IP address to location lookup), and different measurement unit information, such as a vehicle's speed in miles per hour or the altitude in AGL (altitude above ground level directly under the mobile resource). Software systems should be able to handle missing information and process additional information if it is provided.

8.12.5 Location information from GPS systems is updated once a second. As such, a timestamp with one second resolution is sufficient for location information. All location information for the mobile resources being provided by any system should have a timestamp. The use of a simple Unix timestamp is often sufficient, as the system receiving the location information from the mobile resource can convert that into a different format if needed.

8.12.6 Encrypting location information is at the discretion of the AHJ. Encrypting location data is analogous to the decision to encrypt radio voice traffic. There is an additional cost to encrypt data. The process of encrypting information adds substantially to the communications bandwidth and requires that the system have access to the global Internet, which might not be the case in deployed scenarios. If the location of an apparatus is being passed on to the public, encrypting that information serves no purpose. However, if the mobile resource is a surveillance unit or is unmarked, then the overhead and cost can be justified.

8.12.7 Additional information could include any of the following, and, as systems evolve, more types of information not yet envisioned could be included. Software systems using vehicle location information are flexible enough to provide useful functionality with minimal information and can also provide advanced functionality if additional information is in the received data. As information systems evolve and new information is added, older systems might ignore the new information because they are not looking for it. As such, standards for data exchange could evolve without affecting existing software in the field. A list of additional information could include the following:

(1) Identification of the mobile resource, such as Engine 133
(2) Status of the resource, such as in route, on scene, or available
(3) Crew complement
(4) Internet of things telemetry, such as fuel levels, engine temperatures, etc.
(5) Response code information, such as routine or emergency (lights and sirens)

8.12.8 For typical AVL use, the identification of the unit would be required. The response status, crew complement, and the like could come directly from the resource or come from other information stored in a system that might be based on radio traffic. In most systems, mobile resources will provide minimum information to the computer-aided design (CAD) system or situational awareness system, and that system will then provide data with additional contextual information to other systems. You do not want a mobile resource to send similar location-centric information to multiple different systems, as this can tie up mobile data bandwidth.

8.12.9 An example of this process and pass-on information would be supplying information about an apparatus responding with lights and sirens to systems that push Internet-based information out to the public. The CAD system receiving the location information from a mobile resource would also know that the resource was in-route or on scene with emergency response. The CAD system could then push out just the location information, including the timestamp, to these systems, as the systems do not need to know any of the additional information discussed above.

8.13 Building Information Modeling Software (Static).

8.13.1 Building model information is distinctly different from building information management, such as fire alarm or environmental system data. Modeling applications should be able to provide dimensional representations of a structure to a level of accuracy acceptable to the AHJ. This is an emerging field, and the AHJ must identify and plan for the use of the building model to meet those requirements. An example would be the level of detail of a building model in a two-dimensional or three-dimensional image and could include building system symbology that is added by the jurisdiction.

8.14 Building Information Software (Dynamic).

8.14.1 Building information applications should provide key elements of a structure to a level of accuracy acceptable to the AHJ. This is an emerging field, and the AHJ must identify and plan for the use of building information to meet those requirements. An example would be the level of detail of occupant and building processes and procedures.

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.4.1.2 The basic 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.4.1.5 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.4.1.5.2 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.4.1.7 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.

A.4.1.7.3(6)(b) Hardware and software should not be purchased until late in the process to avoid depreciation.

A.4.2 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.4.3.3 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.6.3 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.7.7 Several Association of Public-Safety Communications Officials International (APCO) operational standards reference CAD-to-CAD exchange: www.apcointl.org/standards.

A.8.1.2 An example of single suite applications vs. multiple system applications is found in Table A.8.1.2.

A.8.12 One of the most basic and commonly used types of information is vehicle location information. This information is in use today in the form of AVL (automatic vehicle location) systems used to display maps that show the current locations of responder apparatus. Another use of vehicle location information is collision warning systems that can advise responding apparatus, particularly when approaching an intersection from different directions, that they need to watch out for other emergency response apparatus. Another use is displaying a suggested route for a given apparatus from the apparatus' current location to a destination, such as the location of an incident or a hospital. Another use is to display resources, such as water supplies that are closest to a vehicle. Another use is to push out the location of apparatus that are responding lights and sirens to mapping systems used by the public on their mobile devices for the purpose of alerting the public and providing awareness of the responding apparatus.

Table A.8.1.2 Single Suite Applications vs. Multiple System Applications

	Single Suite (System) of All Applications	Multiple Systems of Applications
Source of Data	Single source of data with native integration	Multiple sources of information require integration with an application programming interface (API)
Support and Maintenance	Single provisioning of services	Multiple locations and potential integration issues
Log On	Single log on	Multiple log ons
Level of Integration	High level	Lower level
Product Performance	Might not fit all requirements	Best fit for requirements
Architecture	System integrated architecture	Multiple integrations require more complex architecture
Updates	Entire suite/ system updates	Single components have to be updated individually
Cost	Typically lower up-front cost and maintenance	Potentially higher up-front cost

Annex B Additional Resources

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

B.1 Introduction. The references in this annex are from complementary standards development organizations and can be used by an AHJ as supplementary material.

B.2 APCO ANS 1.116.1-2015, *Public Safety Communications Common Status Codes for Data Exchange*, 2015. This standard provides a standardized list of status codes that can be used by emergency communications and public safety stakeholders when sharing incident-related information. Creating a common status code does not mean that an agency must change the codes they use internally. The intent is to have each agency map their internal codes to the standardized list.

B.3 APCO ANS 1.111.2-2018, *Public Safety Communications Common Disposition Codes for Data Exchange*, 2018. Disposition codes are used by public safety answering points (PSAPs) and public safety personnel to identify the outcome of an event (incident). These codes typically involve the use of numeric, alpha, or alphanumeric characters that are meaningful only to a specific agency or region. This standard provides a list of common disposition codes for use by PSAPs and public safety personnel when sharing incident information with disparate agencies and authorized stakeholders.

B.4 APCO ANS 2.103.1-2012, *Public Safety Communications Common Incident Types for Data Exchange*, 2012. This APCO ANS document focuses on providing a standardized list of common incident type codes to facilitate effective incident exchange between Next Generation 9-1-1 (NG9-1-1) PSAPs and other authorized agencies, which is a critical component of public safety interoperability. If an agency is receiving information about an incident, a basic level of incident classification might be required to assure they understand the incident type. The creation of this standardized incident type code list does not mean that the agency is required to change the codes they use internally. The intent is to have each agency map their internal codes to the standardized list.

B.5 APCO/CSAA ANS 2.101.2-2014, *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)*, 2014. The purpose of the APCO/CSAA ANS 2.101.2-2014, also known as ASAP 3.3, documentation is to provide a standard data exchange for transmitting information using automation between an alarm monitoring company and a PSAP. There are three primary uses for this Information Exchange Package Documentation (IEPD):

(1) Initial notification of an alarm event by an alarm monitoring company to a PSAP

(2) Update of status by the PSAP's CAD system to the alarm monitoring company as follows:

  (a) Alarm notification accepted, call-for-service created

  (b) Alarm notification rejected due to invalid alarm location address, invalid event type, alarm notification too old, or other reason(s)

(3) Bidirectional update of other events between an alarm monitoring company and a PSAP, such as the following:

  (a) Requests for cancellation by the alarm monitoring company

  (b) Updates concerning key-holder information by the alarm monitoring company

(c) Notice by the PSAP that the primary response agency has been dispatched
(d) Notice by the PSAP that the primary response agency has arrived on scene
(e) Notice by the PSAP that the event has been closed (with a disposition, if applicable)
(f) Updates from the PSAP telecommunicator or field resource requesting additional information, such as an estimated time of arrival for the key-holder

B.6 APCO/NENA ANS 2.105.1-2017, *NG9-1-1 Emergency Incident Data Document (EIDD)*, 2017. The Emergency Incident Data Document (EIDD) provides a standardized, industry-neutral, National Information Exchange Model (NIEM)-conformant (XML-based) specification for sending emergency incident information to agencies and regions that implement NG9-1-1 and Internet Protocol-based emergency communications systems. Emergency incident information exchanges supported by the EIDD include exchanges between disparate manufacturers' systems located within one or more public safety agencies and with other incident stakeholders. The EIDD IEPD is a NIEM-conformant package that describes the construction and content of the EIDD information exchange. It contains all of the schemas necessary to represent and validate the data content of the exchange. It also contains supplemental artifacts, such as documentation, business rules, search and discovery metadata, and sample instances.

B.7 APCO ANS 1.110.1-2015, *Multi-Functional, Multi-Discipline, Computer-Aided Dispatch Minimum Functional Requirements*, 2015. The Multi-Functional, Multi-Discipline, Computer-Aided Dispatch Minimum Functional Requirements standard identifies the minimum functional requirements that a CAD system is required to include, broken down by public safety discipline. Also identified in the document are the optional functional requirements that a CAD system should include. Attachment A, "Unified CAD Functional Requirements (UCADFR)," provides a comprehensive list of functional requirements for CAD systems that can be used by public safety communications centers to assist with the request for proposal process when a need exists to conduct a solicitation for a new CAD system or to upgrade an existing CAD system.

Annex C Informational References

C.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.

C.1.1 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*, 2020 edition.

C.1.2 Other Publications.

ArcGIS Solutions, "ArcGIS Solutions for Local Government," http://solutions.arcgis.com/local-government.

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.

NAPSG Foundation, www.napsgfoundation.org/.

National Geospatial Advisory Committee, "Geospatial Workforce Development," 2012. www.fgdc.gov/ngac/ngac-geospatial-workforce-development-paper-final.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.

Wiki.GIS.com, "System Design Strategies Preface," http://wiki.gis.com/wiki/index.php/System_Design_Strategies_Preface.

C.1.2.1 APCO International Publications. Association of Public Safety Communications Officials, 351 N. Williamson Boulevard, Daytona Beach, FL 32114-1112.

APCO ANS 1.110.1-2015, *Multi-Functional, Multi-Discipline, Computer-Aided Dispatch Minimum Functional Requirements*, 2015.

APCO ANS 1.111.2-2018, *Public Safety Communications Common Disposition Codes for Data Exchange*, 2018.

APCO ANS 1.116.1-2015, *Public Safety Communications Common Status Codes for Data Exchange*, 2015.

APCO/CSAA ANS 2.101.2-2014, *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)*, 2014.

APCO ANS 2.103.1-2012, *Public Safety Communications Common Incident Types for Data Exchange*, 2012.

APCO/NENA ANS 2.105.1-2017, NG9-1-1, *Emergency Incident Data Document (EIDD)*, 2017.

APCO International, "Standards," www.apcointl.org/standards.

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

C.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.

Fire Protection Research Foundation Report, *A Collection of Geospatial Technological Approaches for Wildland and Wildland Urban Interface (WUI) Fire Events*, https://www.nfpa.org/News-and-Research/Data-research-and-tools/Wildland-Urban-Interface/Geospatial-Technological-Approaches-for-Wildland-and-Wildland-Urban-Interface-Fire-Events.

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.

C.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): https://gwg.nga.mil/guide.php

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

ISO Technical Committee 211 and its scope of work: https://committee.iso.org/home/tc211

Subcommittee for Cadastral Data: www.nationalcad.org

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

C.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/

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

Index