

NFPA 1600

Standard on Disaster/Emergency Management and Business Continuity Programs

2007 Edition



NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA DOCUMENTS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA DOCUMENTS

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

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

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

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

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Documents

Users of NFPA codes, standards, recommended practices, and guides should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments.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

Interpretations of NFPA Documents

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

Patents

The NFPA does not take any position with respect to the validity of any patent rights asserted in connection with any items which are mentioned in or are the subject of NFPA codes, standards, recommended practices, and guides, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on these documents. Users of these documents are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

NFPA adheres to applicable policies of the American National Standards Institute with respect to patents. For further information contact the NFPA at the address listed below.

Law and Regulations

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

Copyrights

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

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

For Further Information

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

For more information about NFPA, visit the NFPA website at www.nfpa.org.

Copyright © 2007 National Fire Protection Association. All Rights Reserved.

NFPA 1600®

Standard on

Disaster/Emergency Management and Business Continuity Programs

2007 Edition

This edition of NFPA 1600, *Standard on Disaster/Emergency Management and Business Continuity Programs*, was prepared by the Technical Committee on Emergency Management and Business Continuity. It was issued by the Standards Council on December 1, 2006, with an effective date of December 20, 2006, and supersedes all previous editions.

This edition of NFPA 1600 was approved as an American National Standard on December 20, 2006.

Origin and Development of NFPA 1600

The NFPA Standards Council established the Disaster Management Committee in January 1991. The committee was given the responsibility for developing documents relating to preparedness for, response to, and recovery from disasters resulting from natural, human, or technological events.

The first document that the committee focused on was NFPA 1600, *Recommended Practice for Disaster Management*. NFPA 1600 was presented to the NFPA membership at the 1995 Annual Meeting in Denver, CO. That effort produced the 1995 edition of NFPA 1600.

For the 2000 edition, the committee incorporated a “total program approach” for disaster/emergency management and business continuity programs in its revision of the document from a recommended practice to a standard. They provided a standardized basis for disaster/emergency management planning and business continuity programs in private and public sectors by providing common program elements, techniques, and processes. The committee provided expanded provisions for enhanced capabilities for disaster/emergency management and business continuity programs so that the impacts of a disaster would be mitigated, while protecting life and property. The chapters were expanded to include additional material relating to disaster/emergency management and business continuity programs. The annex material was also expanded to include additional explanatory material.

For the 2004 edition, the committee updated terminology and editorially reformatted the document to follow the 2003 *Manual of Style for NFPA Technical Committee Documents*; however, the basic features of the standard remained unchanged. In addition, the committee added a table in Annex A that created a crosswalk among FEMA CAR, NFPA 1600, and BCI & DRII professional practices. The committee added significant informational resources to Annexes B, C, D, and E.

The document continues to be developed in cooperation and coordination with representatives from FEMA, NEMA, and IAEM. This coordinated effort was reflected in the expansion of the title of the standard for the 2000 edition to include both disaster and emergency management, as well as information on business continuity programs.

The 2007 edition incorporates changes to the 2004 edition, expanding the conceptual framework for disaster/emergency management and business continuity programs. Previous editions of the standard focused on the four aspects of mitigation, preparedness, response, and recovery. This edition identifies prevention as a distinct aspect of the program, in addition to the other four. Doing so brings the standard into alignment with related disciplines and practices of risk management, security, and loss prevention.

Technical Committee on Emergency Management and Business Continuity

Lloyd W. Bokman, *Chair*

Ohio Emergency Management Agency, OH [E]
Rep. National Association of SARA Title III Program Officials

Charles (Buck) P. Adams, Medina County Emergency Management Agency, OH [E]
Richard R. Anderson, Anderson Risk Consultants, NJ [SE]
Charles E. Biggs, U.S. Department of Homeland Security (EP&R), DC [E]
Donald P. Boland, AT&T Communications, IL [U]
Pete Brewster, U.S. Department of Veterans Affairs, WV [U]
Steven J. Charvat, University of Washington, WA [U]
Rep. International Association of Emergency Managers
Donald C. Cooper, Cuyahoga Falls Fire Department, OH [U]
Carroll E. Eichhorn, Lawrence Livermore National Laboratory, CA [U]
Robert P. Fletcher, Jr., Readiness Consulting Services, MD [SE]
Robert Gazdik, St. Paul Travelers, MN [I]
David Gluckman, Willis of New Jersey, Incorporated, NJ [I]
Edward J. Hecker, U.S. Army Corps of Engineers, DC [E]
David J. Hiscott, Jr., Marathon Ashland Petroleum LLC, OH [U]
Rep. American Petroleum Institute
David R. Hood, Russell Phillips & Associates, LLC, NY [U]
Rep. NFPA Health Care Section
Gunnar J. Kuepper, Emergency and Disaster Management, Incorporated, CA [SE]

Edgar T. Ladouceur, Transport Canada, Canada [E]
Dana C. Lankhorst, Middlesex Mutual Assurance Company, NH [I]
Dean R. Larson, Purdue University Calumet, IN [SE]
MaryAnn Elizabeth Marrocolo, City of New York, NY [U]
Michael E. Martinet, County of Los Angeles, CA [E]
Carolyn A. McMullen, The McMullen Company, CA [SE]
Patricia A. Moore, Pat Moore Company, TX [SE]
Terry W. Moore, City of Houston, TX [U]
Rep. Emergency Management Association of Texas
Michael J. Morganti, Trinity, FL [SE]
Rep. Disaster Recovery Institute International
Melvyn Musson, Edward Jones Company, MO [SE]
Ashley E. “Lee” Newsome, Emergency Response Educators & Consultants, Incorporated, FL [SE]
William G. Raisch, New York University, NY [SE]
Clay P. Richter, Aon Risk Services, Incorporated, of Northern California, CA [I]
Dale J. Romme, Hallmark Cards, Incorporated, MO [U]
Rep. NFPA Industrial Fire Protection Section
Donald L. Schmidt, Preparedness, LLC, MA [SE]
R. Ian Stronach, Alcan Incorporated, Canada [U]
Lorraine E. Webb, Emergency Management Ontario, Canada [E]
Milt Wilson, City of Oshawa, Canada [U]
Rep. Ontario Association of Fire Chiefs

Alternates

Edward G. Buikema, U.S. Department of Homeland Security, IL [E]
(Alt. to C. E. Biggs)
Win Chaiyabhat, Aon Risk Services, ME [I]
(Alt. to C. P. Richter)
Marjorie L. DeBrot, U.S. Army Corps of Engineers, MO [E]
(Alt. to E. J. Hecker)
William B. Fox, Emergency Management Ontario, Canada [E]
(Alt. to L. E. Webb)
Susan B. McLaughlin, SBM Consulting, Limited, IL [U]
(Alt. to D. R. Hood)

Michael J. Mumaw, City of Beaverton, OR [U]
(Alt. to S. J. Charvat)
John Douglas Nelson, Chiron Corporation, CA [SE]
(Alt. to P. A. Moore)
Robie Robinson, Dallas County, TX [U]
(Alt. to T. W. Moore)
John A. Sharry, Beakmann Properties, CA [SE]
(Alt. to C. A. McMullen)
Michael R. Zanotti, U.S. Department of Veterans Affairs, WV [U]
(Alt. to P. Brewster)

Nonvoting

Emily Bentley, Emergency Management Accreditation Program, KY [U]
Sharon L. Caudle, U.S. Government Accountability Office, DC [U]
John C. Fannin III, SafePlace Corporation, DE [SE]
Rep. TC on Premises Security

Carl Anthony Gibson, La Trobe University, Australia [E]
James W. Kerr, Michael Rogers, Incorporated, MD [SE]
(Member Emeritus)
Gavin J. Love, WorleyParsons Pty Limited, Australia [SE]

Martha H. Curtis, 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 on preparedness for, response to, and recovery from disasters resulting from natural, human, or technological events.



Contents

Chapter 1 Administration	1600- 4	5.6 Resource Management and Logistics	1600- 6
1.1 Scope	1600- 4	5.7 Mutual Aid/Assistance	1600- 6
1.2 Purpose	1600- 4	5.8 Planning	1600- 6
1.3 Application	1600- 4	5.9 Incident Management	1600- 7
Chapter 2 Referenced Publications	1600- 4	5.10 Communications and Warning	1600- 7
2.1 General	1600- 4	5.11 Operational Procedures	1600- 7
2.2 NFPA Publications (Reserved)	1600- 4	5.12 Facilities	1600- 7
2.3 Other Publications	1600- 4	5.13 Training	1600- 7
2.4 References for Extracts in Mandatory Sections	1600- 4	5.14 Exercises, Evaluations, and Corrective Actions	1600- 7
Chapter 3 Definitions	1600- 4	5.15 Crisis Communication and Public Information	1600- 7
3.1 General	1600- 4	5.16 Finance and Administration	1600- 7
3.2 NFPA Official Definitions	1600- 4	Annex A Explanatory Material	1600- 8
3.3 General Definitions	1600- 4	Annex B Disaster/Emergency Management and Business Continuity Related Organizations	1600-16
Chapter 4 Program Management	1600- 5	Annex C Additional Resources	1600-34
4.1 Program Administration	1600- 5	Annex D Emergency Management Accreditation and Certification Programs	1600-41
4.2 Program Coordinator	1600- 5	Annex E Incident Management System (IMS)	1600-44
4.3 Advisory Committee	1600- 5	Annex F Informational References	1600-47
4.4 Program Evaluation	1600- 5	Index	1600-50
Chapter 5 Program Elements	1600- 5		
5.1 General	1600- 5		
5.2 Laws and Authorities	1600- 5		
5.3 Risk Assessment	1600- 5		
5.4 Incident Prevention	1600- 5		
5.5 Mitigation	1600- 6		

NFPA 1600**Standard on****Disaster/Emergency Management and
Business Continuity Programs****2007 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 Documents.” They can also be obtained on request from NFPA or viewed at www.nfpa.org/disclaimers.

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

A reference in brackets [] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex F. Editorial changes to extracted material consist of revising references to an appropriate division in this document or the inclusion of the document number with the division number when the reference is to the original document. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

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

Chapter 1 Administration

1.1* Scope. This standard shall establish a common set of criteria for disaster/emergency management and business continuity programs hereinafter referred to as the program.

1.2 Purpose. This standard shall provide disaster and emergency management and business continuity programs, the criteria to assess current programs or to develop, implement, and maintain aspects for prevention, mitigation, preparation, response, and recovery from emergencies.

1.3* Application. This document shall apply to public, not-for-profit, and private entities.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document.

2.2 NFPA Publications. (Reserved)

2.3 Other Publications.

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

2.4 References for Extracts in Mandatory Sections.

NFPA 1561, *Standard on Emergency Services Incident Management System*, 2005 edition.

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, shall be 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 Shall. Indicates a mandatory requirement.

3.2.4 Should. Indicates a recommendation or that which is advised but not required.

3.2.5 Standard. A document, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions shall be located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard.

3.3 General Definitions.

3.3.1* Business Continuity. An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services.

3.3.2 Damage Assessment. An appraisal or determination of the effects of the disaster on human, physical, economic, and natural resources.

3.3.3 Disaster/Emergency Management. An ongoing process to prevent, mitigate, prepare for, respond to, and recover from an incident that threatens life, property, operations, or the environment.

3.3.4 Emergency Management Program. A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization.

3.3.5 Entity. A governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has emergency management and continuity of operations responsibilities.

3.3.6* Impact Analysis [Business Impact Analysis (BIA)]. A management level analysis that identifies the impacts of losing the entity's resources.

3.3.7 Incident Action Plan. A verbal plan, written plan, or combination of both, that is updated throughout the incident.



and reflects the overall incident strategy, tactics, risk management, and member safety that are developed by the incident commander. [1561, 2005]

3.3.8* Incident Management System (IMS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

3.3.9 Mitigation. Activities taken to reduce the severity or consequences of an emergency.

3.3.10* Mutual Aid/Assistance Agreement. A prearranged agreement between two or more entities to share resources in response to an incident.

3.3.11 Preparedness. Activities, tasks, programs, and systems developed and implemented prior to an emergency that are used to support the prevention of, mitigation of, response to, and recovery from emergencies.

3.3.12* Prevention. Activities to avoid an incident or to stop an emergency from occurring.

3.3.13* Recovery. Activities and programs designed to return conditions to a level that is acceptable to the entity.

3.3.14 Resource Management. A system for identifying available resources to enable timely and unimpeded access to resources needed to prevent, mitigate, prepare for, respond to, or recover from an incident.

3.3.15* Response. Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

3.3.16 Situation Analysis. The process of evaluating the severity and consequences of an incident and communicating the results.

3.3.17 Stakeholder. Any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the emergency.

Chapter 4 Program Management

4.1 Program Administration. The entity shall have a documented program that includes the following:

- (1) Executive policy including vision, mission statement, roles and responsibilities, and enabling authority
- (2) Program goals, objectives, and method of program evaluation
- (3)*Program plan and procedures
- (4) Applicable authorities, legislation, regulations, and/or industry codes of practice
- (5) Program budget and project schedule, including milestones
- (6) Records management practices

4.2* Program Coordinator. The program coordinator shall be appointed by the entity and authorized to administer and keep current the program.

4.3* Advisory Committee.

4.3.1* An advisory committee shall be established by the entity in accordance with its policy.

4.3.2 The advisory committee shall provide input to or assist in the coordination of the preparation, implementation, evaluation, and revision of the program.

4.3.3 The advisory committee shall include the program coordinator and others who have the appropriate expertise, knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.

4.4 Program Evaluation.

4.4.1 The entity shall establish performance objectives for program management addressed in Chapter 4 and program elements identified in Chapter 5.

4.4.2 The entity shall conduct a periodic evaluation of the program based on the objectives.

Chapter 5 Program Elements

5.1* General.

5.1.1 The program shall include the elements given in Sections 5.2 through 5.16, the scope of which shall be determined by the impact of the hazards affecting the entity.

5.1.2* The program elements shall be applicable to prevention, mitigation, preparedness, response, and recovery.

5.2 Laws and Authorities.

5.2.1* The program shall comply with applicable legislation, policies, regulatory requirements, and directives.

5.2.2* The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.

5.3* Risk Assessment.

5.3.1* The entity shall identify hazards, monitor those hazards, the likelihood of their occurrence, and the vulnerability of people, property, the environment, and the entity itself to those hazards.

5.3.2* Hazards to be evaluated shall include the following:

- (1) Natural hazards (geological, meteorological, and biological)
- (2) Human-caused events (accidental and intentional)
- (3) Technological-caused events

5.3.3* The entity shall conduct an impact analysis to determine potential detrimental impacts of the hazards on the following:

- (1) Health and safety of persons in the affected area at the time of the incident (injury and death)
- (2) Health and safety of personnel responding to the incident
- (3)*Continuity of operations
- (4) Property, facilities, and infrastructure
- (5) Delivery of services
- (6) The environment
- (7)*Economic and financial condition
- (8) Regulatory and contractual obligations
- (9) Reputation of or confidence in the entity
- (10)*Regional, national, and international considerations

5.4 Incident Prevention.

5.4.1* The entity shall develop a strategy to prevent an incident that threatens people, property, and the environment.

5.4.2* The prevention strategy shall be based on the information obtained from Section 5.3 and shall be kept current using the techniques of information collection and intelligence.

5.4.3 The entity shall have a system to monitor the identified hazards and adjust the level of preventative measures to be commensurate with the risk.

5.5 Mitigation.

5.5.1* The entity shall develop and implement a mitigation strategy that includes measures to be taken to limit or control the consequences, extent, or severity of an incident that cannot be reasonably prevented.

5.5.2* The mitigation strategy shall be based on the results of hazard identification and risk assessment, impact analysis, program constraints, operational experience, and cost-benefit analysis.

5.5.3 The mitigation strategy shall include interim and long-term actions to reduce vulnerability.

5.6* Resource Management and Logistics.

5.6.1 The entity shall establish resource management objectives consistent with the overall program goals and objectives as identified in Section 4.1 for the hazards as identified in Section 5.3.

5.6.2 The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities procured or donated to support the program.

5.6.3 The resource management objectives established shall include the following:

- (1) Personnel, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed
- (2) Quantity, response time, capability, limitations, cost, and liability connected with using the involved resources
- (3) Resources and any needed partnership arrangements essential to the program

5.6.4 Resource management shall include the following tasks:

- (1) Establishing processes for describing, inventorying, requesting, and tracking resources
- (2) Activating these processes prior to and during an incident
- (3) Dispatching resources prior to and during an incident
- (4) Deactivating or recalling resources during or after incidents
- (5) Contingency planning for shortfalls of resources

5.6.5 An assessment shall be conducted to identify the resource capability shortfalls and the steps necessary to overcome any shortfalls.

5.6.6 A current inventory of internal and external resources shall be maintained.

5.6.7 Donations of goods, services, personnel, and facilities, solicited and unsolicited, and the management thereof, shall be addressed.

5.7* Mutual Aid/Assistance.

5.7.1 The need for mutual aid/assistance shall be determined.

5.7.2 If mutual aid/assistance is needed, agreements shall be established.

5.7.3 Mutual aid/assistance agreements shall be referenced in the program plan.

5.8 Planning.

5.8.1 Planning Process.

5.8.1.1 The program shall follow a planning process that develops plans for the strategy, prevention, mitigation, emergency operations/response, business continuity, and recovery.

5.8.1.2 The entity shall engage in the planning process on a regularly scheduled basis or when the situation has changed to put the accuracy of the existing plan into question.

5.8.1.3 Where applicable, the entity shall include key stakeholders in the planning process.

5.8.2 Common Plan Elements.

5.8.2.1 Plans shall have clearly stated objectives.

5.8.2.2 Plans shall identify functional roles and responsibilities of internal and external agencies, organizations, departments, and positions.

5.8.2.3 Plans shall identify lines of authority for these agencies, organizations, departments, and positions.

5.8.2.4 Plans shall identify logistics support and resource requirements.

5.8.2.5 Plans shall identify the process for managing an incident.

5.8.2.6 Plans shall identify the process for managing the communication and flow of information, both internally and externally.

5.8.3 Plans.

5.8.3.1* The program shall include a strategic plan, an emergency operations/response plan, a prevention plan, a mitigation plan, a recovery plan, and a continuity plan.

5.8.3.2* The plans developed shall be either individual or integrated into a single plan document, or a combination of the two.

5.8.3.3* The strategic plan shall define the vision, mission, goals, and objectives of the program. (*See Section 4.1.*)

5.8.3.4* The emergency operations/response plan shall assign responsibilities for carrying out specific actions in an emergency.

5.8.3.5 The prevention plan shall establish interim and long-term actions to eliminate hazards that impact the entity.

5.8.3.6 The mitigation plan shall establish interim and long-term actions to reduce the impact of hazards that cannot be eliminated.

5.8.3.7* The recovery plan shall provide for short-term and long-term priorities for restoration of functions, services, resources, facilities, programs, and infrastructure.

5.8.3.8* The continuity plan shall identify stakeholders that need to be notified, the critical and time-sensitive applications, alternative work sites, vital records, contact lists, processes, and functions that shall be maintained, as well as the personnel, procedures, and resources that are needed while the entity is recovering.

5.8.3.9 The entity shall make appropriate sections of the plans available to those assigned specific tasks and responsibilities therein and to other stakeholders as required.



5.9 Incident Management.

5.9.1* The entity shall develop an incident management system to direct, control, and coordinate response and recovery operations.

5.9.2* The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.

5.9.3 The entity shall establish applicable procedures and policies for coordinating response, continuity, and recovery activities with stakeholders directly involved in response, continuity, and recovery operations.

5.9.4 The entity shall establish applicable procedures and policies for coordinating response, continuity, and recovery activities with appropriate authorities and resources, including activation and deactivation of plans, while ensuring compliance with applicable statutes or regulations.

5.9.5* Emergency operations/response shall be guided by an incident action plan or management by objectives.

5.10 Communications and Warning.

5.10.1 Communications systems shall be established and regularly tested to support the program.

5.10.2 Communication procedures shall be established by the entity and regularly exercised to support the program.

5.10.3* The entity shall develop and maintain the capability to alert officials and emergency response personnel.

5.10.4 Emergency communications and warning protocols, systems, processes, and procedures shall be developed, periodically tested, and used to alert people potentially impacted by an actual or impending emergency.

5.10.5 The entity shall determine communication needs, provide capabilities to execute plans, and review and address the interoperability of multiple responding organizations.

5.11* Operational Procedures.

5.11.1 The entity shall develop, coordinate, and implement operational procedures to support the program and execute its plans.

5.11.2* Procedures shall be established and implemented for response to and recovery from the consequences of those hazards identified in Section 5.3 and shall address health and safety, incident stabilization, operational/business continuity, property conservation, and protection of the environment under the jurisdiction of the entity.

5.11.3 Procedures, including life safety, incident stabilization, operational/business continuity, and property conservation, shall be established and implemented for response to, and recovery from, the consequences of those hazards identified in Section 5.3.

5.11.4* Procedures shall be in place to conduct a situation analysis that includes a needs assessment, damage assessment, and the identification of resources needed to support response and recovery operations.

5.11.5 Procedures shall allow for concurrent recovery and mitigation activities during emergency response.

5.11.6 Procedures shall be established for succession of management/government as required in 5.8.3.8.

5.12 Facilities.

5.12.1* The entity shall establish a primary and an alternate emergency operations center, physical or virtual, capable of managing continuity, response, and recovery operations.

5.12.2 Facilities capable of supporting continuity, response, and recovery operations shall be identified.

5.13 Training.

5.13.1 The entity shall develop and implement a training/educational curriculum to support the program.

5.13.2 The objective of the training shall be to create awareness and enhance the skills required to develop, implement, maintain, and execute the program.

5.13.3 Frequency and scope of training shall be identified.

5.13.4 Personnel shall be trained in the entity's incident management system.

5.13.5 Training records shall be maintained.

5.13.6 The training and education curriculum shall comply with all applicable regulatory requirements.

5.14 Exercises, Evaluations, and Corrective Actions.

5.14.1 The entity shall evaluate program plans, procedures, and capabilities through periodic reviews, testing, and exercises.

5.14.2 Additional reviews shall be based on post-incident analyses and reports, lessons learned, and performance evaluations.

5.14.3* Exercises shall be designed to test individual essential elements, interrelated elements, or the entire plan(s).

5.14.4* Procedures shall be established to take corrective action on any deficiency identified.

5.15 Crisis Communication and Public Information.

5.15.1* The entity shall develop procedures to disseminate and respond to requests for pre-incident, incident, and post-incident information, as well as to provide information to internal and external audiences, including the media, and deal with their inquiries.

5.15.2* The entity shall establish and maintain an emergency public information capability that includes the following:

- (1) A central contact facility for the media
- (2) A system for gathering, monitoring, and disseminating emergency information
- (3) Pre-scripted information bulletins
- (4) A method to coordinate and clear information for release
- (5) The capability of communicating with special needs populations
- (6) Protective action guidelines/recommendations (e.g., shelter-in-place or evacuation)

5.15.3 Where the public is potentially impacted by a hazard, a public awareness program shall be implemented.

5.15.4 The entity shall develop procedures to advise the public, through authorized agencies, of threats to people, property, and the environment.

5.16* Finance and Administration.

5.16.1* The entity shall develop financial and administrative procedures to support the program before, during, and after an emergency or a disaster.

5.16.2 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels and fiscal policy.

5.16.3 The procedures shall include the following:

- (1) Establishment and definition of responsibilities for the program finance authority, including its reporting relationships to the program coordinator
- (2) Program procurement procedures
- (3) Payroll
- (4) Accounting systems to track and document costs
- (5)*Management of funding from external sources

Annex A Explanatory Material

Annex A is not a part of the requirements 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 The emergency management and business continuity community comprises many different entities including the government at distinct levels (e.g., federal, state/provincial, territorial, tribal, indigenous, and local levels); business and industry; nongovernmental organizations; and individual citizens. Each of these entities has its own focus, unique missions and responsibilities, varied resources and capabilities, and operating principles and procedures. Each entity can have its own definition of disaster. Examples of disaster definitions used by entities include the following:

- (1) An occurrence or imminent threat to the entity of widespread or severe damage, injury, or loss of life or property resulting from natural or human causes
- (2) An emergency that is beyond the normal response resources of the entity and would require the response of outside resources and assistance for recovery
- (3) A suddenly occurring or unstoppable developing event that does the following:
 - (a) Claims loss of life, suffering, loss of valuables, or damage to the environment
 - (b) Overwhelms local resources or efforts
 - (c) Has a long-term impact on social or natural life that is always negative in the beginning

A.1.3 An example of a specific industry application of the framework in the public sector is the Emergency Management Accreditation Program (EMAP). EMAP uses NFPA 1600 as the basis for guidelines that are used to accredit state, local, and tribal emergency management programs. Accreditation involves review of documentation, observations, and interviews with program officials (e.g., officials with the emergency management agency and from partner agencies, such as transportation, health, utilities, environmental, and law enforcement).

NFPA 1600's comprehensive framework has also been applied to standards for hospitals. The 2005 revision to NFPA 99, *Standard for Health Care Facilities*, Chapter 12, Health Care Emergency Management, incorporated the "program" emphasis of NFPA 1600, serving to differentiate an "emergency management program" for health care systems from the current emphasis by other hospital standards on an "emergency management plan."

A.3.2.1 Approved. The National Fire Protection Association does not approve, inspect, or certify any installations, proce-

dures, 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.3.3.1 Business Continuity. In the public sector, this phrase is also known as *continuity of operations* or *continuity of government*. Mission, vision, and strategic goals and objectives are used to focus the program.

A.3.3.6 Impact Analysis [Business Impact Analysis (BIA)]. This analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions concerning hazard mitigation, recovery strategies, and continuity planning.

A.3.3.8 Incident Management System (IMS). The incident command system (ICS) is a component of an overall incident management system.

A.3.3.10 Mutual Aid/Assistance Agreement. The term *mutual aid/assistance agreement* as used herein includes cooperative agreements, partnership agreements, memoranda of understanding, intergovernmental compacts, or other terms commonly used for the sharing of resources.

A.3.3.12 Prevention. Activities, tasks, programs, and systems intended to avoid or intervene in order to stop an incident from occurring. Prevention can apply both to human-caused incidents (such as terrorism, vandalism, sabotage, or human error) as well as to naturally occurring incidents. Prevention of human-caused incidents can include applying intelligence and other information to a range of activities that includes such countermeasures as deterrence operations, heightened inspections, improved surveillance and security operations, investigations to determine the nature and source of the threat, and law enforcement operations directed at deterrence, preemption, interdiction, or disruption.

A.3.3.13 Recovery. Recovery programs are designed to assist victims and their families, restore institutions to suitable economic growth and confidence, rebuild destroyed property, and reconstitute government operations and services. Recovery actions often extend long after the incident itself.

Recovery programs include mitigation components designed to avoid damage from future incidents.

A.3.3.15 Response. The response of an entity to a disaster or other significant event that might impact the entity. Activities, tasks, programs, and systems can include the preservation of life, meeting basic human needs, preserving business operations, and protecting property and the environment. An incident response can include evacuating a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an entity to a more stable status.

A.4.1(3) The common criteria of the standard can be organized in a chronological order to form a program development schedule to include the following steps:

- (1) Establish leadership and direction for the program. (Form an Advisory Committee, designate a program coordinator, conduct a program assessment, define the program policy, and develop and approve a strategic administrative plan.)
- (2) Identify hazards and take actions to eliminate or reduce their impacts. (Conduct a hazards identification, risk assessment and impact analysis; develop prevention, mitigation, and continuity plan(s); and establish a public education program.)
- (3) Prepare the entity for response and recovery operations. (Develop the emergency operations/response and recovery plan(s); establish operational procedures; define facilities; establish communications and warning systems; engage in resource management and logistics and mutual aid/assistance activities; conduct ongoing education, training, and exercise activities; and maintain a corrective action program.)

A.4.2 The program coordinator should ensure the preparation, implementation, evaluation, and revision of the program. It is not the intent of this standard to restrict the users to program coordinator titles. It is recognized that different entities use various forms and names for their program coordinator that performs the functions identified in the standard. An example of a title for the public sector is emergency manager, and an example of a title for the private sector is business continuity manager. A written position description should be provided.

A.4.3 Members of the advisory committee should participate with the clear understanding that the objective is to minimize turnover of committee members to maintain an effective committee. Within the private sector, representatives can include, but are not limited to, information technology and communications, plant operations, transportation, maintenance, engineering, personnel, public relations, environment, legal, finance, risk management, health and safety, security, stakeholders, and fire fighting/rescue. Within the public sector, representatives can include police, fire, emergency medical services, engineering, public works, environmental protection, public health, finance, education, emergency management, legal, transportation authorities, homeland security, stakeholders, and the military (e.g., the National Guard). When determining the representation on the committee, consideration should be given to public sector representation on a private sector committee and vice versa. This will help to establish a coordinated and cooperative approach to the program.

A.4.3.1 Although the program coordinator has the final authority in deciding the course of the program through its day-to-day administration, it is encouraged that major decisions be made in consultation with the advisory committee. The program coordinator and the advisory committee should be in agreement concerning priorities and resource allocation in the day-to-day operations of the program.

Decisions made and actions taken in the day-to-day administration of the program crucially affect the ultimate implementation of the program in times of emergency. Therefore, because the advisory committee is composed of those representing key functional areas, both within and external to the entity, it is encouraged that the program coordinator and the advisory committee consult together on important administrative matters to ensure the goals of the program are indeed met.

All state and local emergency management entities report to a higher authority. States report to governors, adjutant generals, chief law enforcement officers, county commissions, or city commissions. These authorities set the agendas for emergency management activities. Having an advisory committee might or might not be encouraged. Mandating that an entity must have an advisory committee will, in many cases, violate the authorities under which the emergency management entity is established. Those organizations that can have, or want to have, an advisory committee that will provide advice and guidance should be encouraged to do so.

A.5.1 See Table A.5.1.

A.5.1.2 Key program elements cross boundaries during prevention, mitigation, preparedness, response, and recovery. Each element should be considered interrelated and can be considered concurrently. The use of the terms *phases*, *elements*, or *components* varies from program to program.

A.5.2.1 Industry codes of practices and guidelines should also be considered.

A.5.2.2 If, through exercise or incident analysis, program evaluation, and corrective action, limitations in the necessary laws and applicable authorities are discovered, a formal process should exist to amend them.

In the case of public entities, consideration should be made for periodic review of existing legislation, regulations, codes, and authorities to determine whether adequate flexibility exists to accommodate evolving programmatic policy or if new legislation should be developed and introduced through a legislative initiative. This is particularly relevant as program requirements change to comply with changing roles and relationships in and among varying levels of government.

For example, the entity might have the appropriate authority to conduct emergency operations but lack authority to take action prior to an event to mitigate the occurrence or the recurrence of an emergency. In other cases, additional authorities could be needed to generate the necessary revenue to sustain a viable program, and additional authority could be required to create a standing contingency fund to adequately support a disaster operation. In the private sector, the governing factors can be industry codes of practice or regulations rather than statutory restrictions. A process should be established for periodic review of industry practices for compliance with the strategy, goals, and objectives of the entity. Evolving best practices should be incorporated into industry codes as applicable.

Table A.5.1 NFPA 1600, BCI & DRII Professional Practices, and DHS/FEMA's FPC 65 COOP Elements Crosswalk

NFPA 1600 Chapter/Section	BCI & DRII Professional Practices (Subject Area)	DHS/FEMA FPC 65 COOP Elements
4, Program Management	1, Project Initiation and Management	—
5.2, Laws and Authorities	9, Public Relations and Crisis Coordination 10, Coordination with Public Authorities	—
5.3, Risk Assessment	2, Risk Evaluation and Control	—
5.4, Incident Prevention	2, Risk Evaluation and Control	—
5.5, Mitigation	2, Risk Evaluation and Control	—
5.6, Resource Management and Logistics	3, Business Impact Analysis	Human Capital
5.7, Mutual Aid/Assistance	4, Developing Business Continuity Strategies	—
5.8, Planning	1, Project Initiation and Management 2, Risk Evaluation and Control 3, Business Impact Analysis 4, Developing Business Continuity Strategies 5, Emergency Response and Operations 6, Developing and Implementing Business Continuity Plans	Plans and Procedures Essential Functions Orders of Succession Delegations of Authority Vital Records and Databases Human Capital
5.9, Incident Management	5, Emergency Response and Operations 6, Developing and Implementing Business Continuity Plans	Devolution of Control and Direction
5.10, Communications and Warning	5, Emergency Response and Operations 6, Developing and Implementing Business Continuity Plans	Interoperable Communications
5.11, Operational Procedures	5, Emergency Response and Operations 6, Developing and Implementing Business Continuity Plans	Plans and Procedures Orders of Succession Delegations of Authority Vital Records and Databases Reconstitution
5.12, Facilities	4, Developing Business Continuity Strategies 6, Developing and Implementing Business Continuity Plans	Alternate Operating Facilities
5.13, Training	7, Awareness and Training	Tests, Training and Exercises
5.14, Exercises, Evaluations, and Corrective Actions	7, Awareness and Training 8, Maintaining and Exercising Business Continuity Plans	Tests, Training and Exercises
5.15, Crisis Communication and Public Information	9, Public Relations and Crisis Coordination	—
5.16, Finance and Administration	1, Project Initiation and Management	—

BCI: Business Continuity Institute. DRII: Disaster Recovery Institute International.

DHS: Department of Homeland Security. FEMA: Federal Emergency Management Agency.

A.5.3 A comprehensive risk assessment identifies the range of possible hazards, threats, or perils that have or might impact the entity, surrounding area, or critical infrastructure supporting the entity. The potential impact of each hazard, threat, or peril is determined by the severity of each and the vulnerability of people, property, operations, the environment, and the entity to each threat, hazard, or peril. The risk assessment should categorize threats, hazards, or perils by both their relative frequency and severity, keeping in mind that there might be many possible combinations of frequency and severity for each. The entity should attempt to mitigate, prepare for, plan to respond to, and recover from those threats, hazards, or perils that are able to

significantly impact people, property, operations, the environment, or the entity itself.

A.5.3.1 A number of methodologies and techniques for risk assessment exist that range from simple to complex. These techniques and associated amplifying information include, but are not limited to, the following:

- (1) “What-if”: The purpose of the what-if analysis is to identify specific hazards or hazardous situations that could result in undesirable consequences. This technique has limited structure but relies on knowledgeable individuals who are familiar with the areas/operations/processes. The value of the

end result is dependent on the team and the exhaustive nature of the questions they ask regarding the hazards.

- (2) **Checklist:** A specific list of items is used to identify hazards and hazardous situations by comparing the current or projected situations with accepted standards. The value of the end result is dependent on the quality of the checklist and the experience/credentials of the checklist user.
- (3) **What-if/checklist:** This technique is a combination of the what-if and checklist techniques, and uses the strength of both techniques to complete the risk assessment. The what-if questions are developed and the checklist(s) used to encourage the creativity of the what-if process, as well as fill in any gaps in the process of developing questions. The value of the end result is dependent on the team and exhaustive nature of the questions they ask regarding the hazards.
- (4) **Hazard and operability study (HAZOP):** This technique requires an interdisciplinary team that is very knowledgeable of the areas/operations/processes to be assessed. This approach is thorough, time-consuming, and costly. The value of the end result depends on the qualifications/experience of the team, the quality of the reference material available, the ability of the team to function as a team, and strong, positive leadership.
- (5) **Failure mode and effects analysis (FMEA):** Each element in a system is examined individually and collectively to determine the effect when one or more elements fail. This is a bottom-up approach; that is, the elements are examined and the effect of failure on the overall system is predicted. A small interdisciplinary team is required. This technique is best suited for assessing potential equipment failures. The value of the end result is dependent on the credentials of the team and scope of the system to be examined.
- (6) **Fault-tree analysis (FTA):** This is a top-down approach where an undesirable event is identified and the range of potential causes that could lead to the undesirable event is identified. The value of the end result is dependent on the competence in using the FTA process, on the credentials of the team, and on the depth of the team's analysis.

A.5.3.2 The hazard identification should include the following types of potential hazards. This list is not all-inclusive but reflects the general categories that should be assessed in the hazard identification.

- (1) Naturally occurring hazards that can occur without the influence of people and have potential direct or indirect impact on the entity (people, property, the environment), such as the following:
 - (a) Geological hazards (does not include asteroids, comets, meteors)
 - i. Earthquake
 - ii. Tsunami
 - iii. Volcano
 - iv. Landslide, mudslide, subsidence
 - v. Glacier, iceberg
 - (b) Meteorological hazards
 - i. Flood, flash flood, seiche, tidal surge
 - ii. Drought
 - iii. Fire (forest, range, urban, wildland, urban interface)
 - iv. Snow, ice, hail, sleet, avalanche
 - v. Windstorm, tropical cyclone, hurricane, tornado, water spout, dust/sand storm
 - vi. Extreme temperatures (heat, cold)
 - vii. Lightning strikes

- viii. Famine
- ix. Geomagnetic storm

(c) Biological hazards

- i. Emerging diseases that impact humans or animals [plague, smallpox, anthrax, West Nile virus, foot and mouth disease, SARS, pandemic disease, BSE (Mad Cow Disease)]
- ii. Animal or insect infestation or damage

(2) Human-caused events such as the following:

(a) Accidental

- i. Hazardous material (explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, radiological, corrosive) spill or release
- ii. Explosion/fire
- iii. Transportation accident
- iv. Building/structure collapse
- v. Energy/power/utility failure
- vi. Fuel/resource shortage
- vii. Air/water pollution, contamination
- viii. Water control structure/dam/levee failure
- ix. Financial issues, economic depression, inflation, financial system collapse
- x. Communications systems interruptions
- xi. Misinformation

(b) Intentional

- i. Terrorism (explosive, chemical, biological, radiological, nuclear, cyber)
- ii. Sabotage
- iii. Civil disturbance, public unrest, mass hysteria, riot
- iv. Enemy attack, war
- v. Insurrection
- vi. Strike or labor dispute
- vii. Disinformation
- viii. Criminal activity (vandalism, arson, theft, fraud, embezzlement, data theft)
- ix. Electromagnetic pulse
- x. Physical or information security breach
- xi. Workplace violence
- xii. Product defect or contamination
- xiii. Harassment
- xiv. Discrimination

(3) Technological-caused events that can be unrelated to natural or human-caused events, such as the following:

- (a) Central computer, mainframe, software, or application (internal/external)
- (b) Ancillary support equipment
- (c) Telecommunications
- (d) Energy/power/utility

A.5.3.3 The impact analysis is a broad description and quantification of a potential event that can impact an entity. This analysis should give a clear idea of what hazards are most likely to occur; what entity facilities, functions, or services are affected based on their vulnerability to that hazard; what actions will most effectively protect them; and the potential impact on the entity in quantifiable terms.

Within the impact analysis, the entity should consider the impact external to its area of influence that can affect the entity's ability to cope with an emergency. One example is the cascade effects of a hurricane. Direct impacts can include wind and flood damage. Secondary impacts can include communications, power, and transportation disruptions, both inside and outside

the direct impact area, and the potential impact on the entity in quantifiable terms.

A.5.3.3(3) In order to maintain continuity of operations, the entity should identify essential or critical functions and processes, their recovery priorities, and internal and external interdependencies, so that recovery time objectives can be set.

A.5.3.3(7) An economic and financial impact analysis allows the quantification of the impacts without considering the cause of the emergency. This analysis is closely related to the process of identifying essential or critical functions or processes and helps decide where to place the emphasis in planning efforts.

The analysis examines potential economic or financial loss resulting from disruption of the functions, processes, or services over time.

The purpose of an economic and financial impact analysis is to arrive at a general loss expectancy that demonstrates what is at risk and to guide measures to mitigate the effects of an emergency.

A.5.3.3(10) It is important to consider the regional, national, or international implications of a hazard's impact on a community, such as in New York City. A hazard that affects the New York Stock Exchange will have enormous national and international impacts that should be considered.

A.5.4.1 The prevention strategy should include the following:

- (1) Deterrence operations
- (2) Provision of protective systems or equipment for physical or cyber risks
- (3) Surveillance and security operations
- (4) Investigations to determine the full nature and source of the threat
- (5) Public health and agricultural surveillance and testing processes
- (6) Immunizations, isolation, or quarantine
- (7) Threat assessment documentation

Additional considerations for the prevention strategy could include the following:

- (1) Perimeter fence line and gates
- (2) Access control system, increased camera surveillance, intruder detection systems (motion-sensing cameras, infrared detectors)
- (3) Patrols (inside and outside) of facility and increased inspections of vehicles entering the facility
- (4) Background checks for personnel

A.5.4.2 Techniques to consider in a prevention strategy include the following:

- (1) Ongoing hazard identification
- (2) Threat assessment
- (3) Risk assessment
- (4) Impact analysis
- (5) Program assessment
- (6) Operational experience
- (7) Ongoing incident analysis
- (8) Information collection and analysis
- (9) Intelligence and information sharing

An impact analysis could include a cost-benefit analysis. The cost-benefit analysis should not be the overriding factor in establishing a prevention strategy.

A.5.5.1 The mitigation strategy should include the following:

- (1) Use of applicable building construction standards
- (2) Hazard avoidance through appropriate land use practices
- (3) Relocation, retrofitting, or removal of structures at risk
- (4) Removal or elimination of the hazard
- (5) Reduction or limitation of the amount or size of the hazard
- (6) Segregation of the hazard from that which is to be protected
- (7) Modification of the basic characteristics of the hazard
- (8) Control of the rate of release of the hazard
- (9) Provision of protective systems or equipment for both cyber and physical risks
- (10) Establishment of hazard warning and communication procedures
- (11) Redundancy or diversity of essential personnel, critical systems, equipment, information, operations, or materials
- (12) Acceptance/retention/transfer of risk (insurance programs)
- (13) Protection of competitive/proprietary information

A.5.5.2 The mitigation strategy should establish interim and long-term actions to reduce the risks from hazards.

A.5.6 The five key principles of resource management that underpin effective resource management are as follows:

- (1) **Advance Planning.** Entities work together in advance of an incident to develop plans for managing and employing resources in a variety of possible emergency circumstances.
- (2) **Resource Identification and Ordering.** Entities use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities.
- (3) **Categorizing Resources.** Resources are categorized by size, capacity, capability, skill, and other characteristics.
- (4) **Use of Agreements.** Mutual aid/assistance agreements and pre-incident agreements among all parties providing or requesting resources are necessary to enable effective and efficient resource management during incident operations.
- (5) **Effective Management of Resources.** Resource managers use validated practices to perform the following key resource management tasks systematically and efficiently:
 - (a) **Acquisition Procedures.** Used to obtain resources to support operational requirements.
 - (b) **Management Information Systems.** Used to collect, update, and process data; track resources; and display their readiness status.
 - (c) **Ordering, Mobilization, Dispatching, and Demobilization Protocols.** Used to request resources, prioritize requests, activate and dispatch resources to incidents, and return resources to normal status.

To the extent practical and feasible, an entity should type resources according to established definitions, such as utilizing the Department of Homeland Security/FEMA's National Mutual Aid and Resource Management Initiative Resource Type Definitions.

Resources for program administration as well as emergency operations should be specifically identified. These resources include, but are not limited to, the following:

- (1) The locations, quantities, accessibility, operability, and maintenance of equipment (heavy duty, protective, transportation, monitoring, decontamination, response, personal protective equipment)
- (2) Supplies (medical, personal hygiene, consumable, administrative, ice)
- (3) Sources of energy (electrical, fuel)



- (4) Emergency power production (generators)
- (5) Communications systems
- (6) Food and water
- (7) Technical information
- (8) Clothing
- (9) Shelter
- (10) Specialized personnel (medical, religious, volunteer organizations, emergency management staff, utility workers, morticians, and private contractors)
- (11) Specialized volunteer groups [Red Cross, amateur radio, religious relief organizations, charitable agencies, VOAD (Volunteer Organization Active in Disaster), COAD (Community Organization Active in Disaster), CERT (Community Emergency Response Team)]
- (12) External federal, state, provincial, tribal, territorial, and local agencies

A resource should be available in a timely manner and should have the capability to do its intended function. Restriction on the use of the resource should be taken into account, and application of the resource should not incur more liability than would failure to use the resource. Finally, the cost of the resource should not outweigh the benefit.

A.5.7 Mutual aid/assistance agreements between entities are an effective means to obtain resources and should be developed whenever possible. Mutual aid/assistance agreements should be in writing, be reviewed by legal counsel, be signed by a responsible official, define liability, and detail funding and cost arrangements. The term *mutual aid/assistance agreement* as used here includes cooperative assistance agreements, intergovernmental compacts, or other terms commonly used for the sharing of resources.

Mutual aid/assistance agreements are the means for one entity to provide resources, facilities, services, and other required support to another entity during an incident. Each entity should be party to a mutual aid/assistance agreement (such as the Emergency Management Assistance Compact) with appropriate entities from which they expect to receive or to which they expect to provide assistance during an incident. This would normally include all neighboring or nearby entities, as well as relevant private sector and nongovernmental organizations. States should participate in interstate compacts and look to establish intrastate agreements that encompass all local entities. Mutual aid/assistance agreements are also needed with private organizations, such as the International Red Cross, to facilitate the timely delivery of private assistance at the appropriate entity level during incidents. At a minimum, mutual aid/assistance agreements should include the following elements or provisions:

- (1) Definitions of key terms used in the agreement
- (2) Roles and responsibilities of individual parties
- (3) Procedures for requesting and providing assistance
- (4) Procedures, authorities, and rules for payment, reimbursement, and allocation of costs
- (5) Notification procedures
- (6) Protocols for interoperable communications
- (7) Relationships with other agreements among entities
- (8) Workers' compensation
- (9) Treatment of liability and immunity
- (10) Recognition of qualifications and certifications
- (11) Sharing agreements, as required

A.5.8.3.1 It should be noted that most entities engage in multiple planning activities (e.g., mitigation planning, land use planning). Coordination ensures nonduplication, improves

understanding, increases support, and assures that all stakeholders have a voice.

A.5.8.3.2 The extent of planning requirements will depend on the program's objectives, results of the hazard analysis, organizational culture and philosophy, regulations, and so on.

A.5.8.3.3 The plan should be reviewed annually and updated as necessary. It should also be re-evaluated when any of the following occur:

- (1) Regulatory changes
- (2) New hazards are identified or existing hazards change
- (3) Resources or organizational structures change
- (4) After tests, drills, or exercises
- (5) After emergency responses
- (6) Infrastructure, economic, and geopolitical changes
- (7) Funding or budget level changes

The strategic plan identifies the long-term goals, using broad general statements of desired accomplishments. The objectives developed from these goals include measurable activities that should be accomplished within identified time frames to meet those objectives.

A.5.8.3.4 The management functions of the incident command system (command, operations, planning, logistics, and finance/administration) can be used to structure the emergency operations/response plan. This approach can improve understanding and effective use of both.

A.5.8.3.7 A specific plan for all of the items might be impossible in advance of a disaster. A strategy for recovery covering all of the items in the standard might be more appropriate, based upon the entity.

In developing plans, short-term goals and objectives should be established and should include, but not be limited to, the following:

- (1) Vital personnel, systems, operations, records, and equipment identified in Section 5.6
- (2) Priorities for restoration and mitigation
- (3) Acceptable downtime before restoration to a minimum level
- (4) Minimum resources needed to accomplish the restoration

The recovery strategy should include provisions for the return of the following services, as applicable:

- (1) Critical infrastructure (water, gas, electricity, and waste management)
- (2) Telecommunications and cyber systems
- (3) Distribution systems or networks for essential goods (food, clothing, personal supplies, and services)
- (4) Transportation systems, networks and infrastructure
- (5) Built environment (including residential, commercial, and industrial uses)
- (6) Psychosocial services
- (7) Health services
- (8) Continuity of governance systems

In developing plans, consideration should be given to long-term goals and objectives, which should include, but not be limited to, the following:

- (1) The entity's strategic plan
- (2) Management and coordination of activities
- (3) Funding and fiscal management
- (4) Management of volunteer, contractual, and entity resources
- (5) Opportunities for disaster mitigation

A.5.8.3.8 Plans for business continuity, continuity of government, and continuity of operations are generally similar in intent and less similar in content. Continuity plans have various names in both the public and private sectors. These include business continuity plans, business resumption plans, disaster recovery plans, and so on.

In addition, within the public sector, continuity of operations plans might use business impact analysis to identify critical governmental functions.

Recovery planning for public sector normally includes bringing infrastructure and individuals back to pre-incident conditions, including implementation of mitigation measures, to facilitate short- and long-term recovery.

Business continuity planning in the private sector incorporates both the initial activities to respond to an emergency situation and the restoration of the business and its functions to pre-incident levels. As a result, there are both differences and similarities between public sector recovery plans and private sector business continuity plans.

Specific areas to consider in continuity plans include the following:

- (1) **Succession:** To ensure that the leadership will continue to function effectively under emergency conditions. When practical, there is a designation of at least three successors for each position. Provisions have been made to deal with vacancies and other contingencies such as absence or inability to act.
- (2) **Pre-delegation of emergency authorities:** To ensure that sufficient enabling measures are in effect to continue operations under emergency conditions. Emergency authorities have been enacted that specify the essential duties to be performed by the leadership during the emergency period and that enable the leadership to act if other associated entities are disrupted, and to re-delegate with appropriate limitations.
- (3) **Emergency action steps:** Actions that facilitate the ability of personnel to respond quickly and efficiently to disasters/emergencies. Checklists, action lists, and/or standard operating procedures (SOPs) have been written that identify emergency assignments, responsibilities, and emergency duty locations. Procedures should also exist for alerting, notifying, locating, and recalling key members of the entity. The SOPs and notification procedures should be integrated.
- (4) **Primary and alternate emergency operations centers:** A facility or capability from which direction and control is exercised in an emergency. This type of center or capability is designated to ensure that the capacity exists for the leadership to direct and control operations from a centralized facility or capability in the event of an emergency. (See A.5.12.1.)
- (5) **Alternate operating or backup facilities:** Provisions also exist for alternate site(s) for departments or agencies having emergency functions or continuing operations.
- (6) **Vital records:** The measures that are taken by the entity to protect the entity's vital records — for example, financial, data, personnel records, and engineering drawings — that the entity should have to continue functioning during emergency conditions and to protect the rights and interests of the entity. Procedures have been put in place to ensure the selection, preservation, and availability of records essential to the effective functioning of the entity under emergency conditions and to maintain the continuity of operations. Protection of records should comply

with applicable laws [Health Insurance Portability and Accountability Act (HIPAA) or other privacy laws].

- (7) **Protection of resources, facilities, and personnel:** The measures that are taken to deploy resources and personnel in a manner that will provide redundancy to ensure the entity can continue to function during emergency conditions. Plans and procedures are in place to ensure the protection of personnel, facilities, and resources so the entity can operate effectively. The entity should have the ability to allocate needed resources and restore functions during and after disasters/emergencies. Plans should address deployment procedures to relocate/replicate resources or facilities, increase protection of facilities, and inform and train personnel in protective measures. Preparedness should be increased based on the threat level. (See A.5.3.)

A.5.9.1 An example of an approved incident management system (IMS) would be NIMS, as used in the United States, the British equivalent, or the Continental European system, or their equivalent. (See Annex E.)

For specific information on communications and warning and emergency public information, see Sections 5.10 and 5.15.

A.5.9.2 In emergencies, an incident management system would be used to systematically identify management functions assigned to various personnel. The system used varies among entities and among jurisdictions within entities. In minor emergencies, incident management functions might be handled by one person, the incident commander or equivalent designation.

An incident management system is designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. It is normally structured to facilitate activities in five major functional areas: command, operations, planning, logistics, and finance and administration. See Annex E for detailed information on incident management systems (IMSs).

A.5.9.5 See Annex E for information on incident action plans.

A.5.10.3 Means of maintaining capability includes redundant or multiple systems.

A.5.11 Procedures should include, but not be limited to, the following:

- (1) Control of access to the area affected by the emergency
- (2) Identification of personnel engaged in activities at the incident
- (3) Accounting for personnel engaged in incident activities
- (4) Accounting for persons affected, displaced, or injured by the emergency
- (5) Mobilization and demobilization of resources
- (6) Provision of temporary, short-term, or long-term housing, feeding, and care of populations displaced by an emergency
- (7) Recovery, identification, and safeguarding of human remains (The National Foundation for Mortuary Care has recommended practices for mass casualty events.)
- (8) Provision for the mental health and physical well-being of individuals affected by the emergency
- (9) Provision for managing critical incident stress for responders

A.5.11.2 Property conservation, as used in 5.11.2, means minimizing property damage.



A.5.11.4 A needs assessment should include addressing the safety, health, and welfare of people, and the protection of property and the environment under the jurisdiction of the entity.

A.5.12.1 Emergency operations centers (EOCs) represent the physical location at which the coordination of information and resources to support incident management activities normally takes place. The Incident Command Post (ICP) located at or in the immediate vicinity of an incident site, although primarily focused on the tactical on-scene response, can perform an EOC-like function in smaller-scale incidents or during the initial phase of the response to larger, more complex events. Standing EOCs, or those activated to support larger, more complex events, are typically established in a more central or permanently established facility at a higher level of organization within a jurisdiction.

EOCs can be organized by major functional discipline (fire, law enforcement, medical services, and so on), by jurisdiction (city, county, region, and so on), or, more likely, by some combination thereof.

Department Operations Centers (DOCs) normally focus on internal agency incident management and response and are linked to and, in most cases, are physically represented in a higher level EOC. ICPs should also be linked to DOCs and EOCs to ensure effective and efficient incident management.

For complex incidents, EOCs can be staffed by personnel representing multiple jurisdictions and functional disciplines and a wide variety of resources. For example, a local EOC established in response to a bioterrorism incident would likely include a mix of law enforcement, emergency management, public health, and medical personnel (representatives of health care facilities, pre-hospitalization emergency medical services, patient transportation systems, pharmaceutical repositories, laboratories, and so on).

EOCs can be permanent organizations and facilities or can be established to meet temporary, short-term needs. The physical size, staffing, and equipping of an EOC will depend on the size of the jurisdiction, resources available, and anticipated incident management workload. EOCs can be organized and staffed in a variety of ways. Regardless of the specific organizational structure used, EOCs should include the following core functions: coordination; communications; resource dispatch and tracking; and information collection, analysis, and dissemination.

EOCs can also support multiagency coordination and joint information activities as discussed subsequently. On activation of a local EOC, communications and coordination have to be established between the Incident Command (IC) or Unified Command (UC) and the EOC when they are not collocated. ICS field organizations have to also establish communications with the activated local EOC, either directly or through their parent organizations. Additionally, EOCs at all levels of government and across functional agencies have to be capable of communicating appropriately with other EOCs during incidents, including those maintained by private organizations. Communications between EOCs has to be reliable and contain built-in redundancies. The efficient functioning of the EOCs most frequently depends on the existence of mutual aid/assistance agreements and joint communications protocols among participating agencies.

Facilities should be capable of accommodating any combination of essential representatives who are identified in the entity's plan. Facilities should have adequate workspace, com-

munications, and back-up utilities and should meet other basic human needs for each representative. Essential functions include gathering essential information capable of providing centralized direction and control, and warning for response and recovery actions. Facilities should be located so that they are not impacted by the same event. (See A.5.8.3.8.)

With the increased usage of virtual or mobile EOC capabilities, entities using this mode of operation should still meet the criteria in this section.

An emergency operations center would include an emergency coordination center or its equivalent.

A.5.14.3 Exercises should include, but not be limited to, tabletops, simulations, and full operational exercises.

A.5.14.4 A Corrective Action Program is a process that follows an actual occurrence or exercise to identify program shortfalls and necessary corrective actions to address those shortfalls. The Corrective Action Program provides the techniques to manage the capabilities improvement process.

The Corrective Action Program begins following the "after-action" discussion/critique of the incident or exercise. The Corrective Action Program might also begin during the incident if a lengthy or extended event is being managed. During the evaluation, process deficiencies are noted that require improvement. Some corrective actions might not be taken immediately due to constraints, such as budgets, staffing, or contracts, and might be deferred as part of the long-range project. However, temporary actions should be taken to implement the desired option.

Typically, those process deficiencies fall within one or more of the 13 program elements found in the standard. There are three categories of corrective actions, listed as follows:

- (1) Plan or standard operating procedures (SOP) revisions
- (2) Training
- (3) Equipment additions or modifications and facilities

A task group is assigned to each identified area of noted deficiency to develop the necessary actions for improvement and a time schedule for development of the necessary corrective action is established.

The task group should do the following:

- (1) Develop options for appropriate corrective action
- (2) Make recommendations for a preferred option
- (3) Develop an implementation plan, which could include training
- (4) Ensure that during the next exercise the corrective action be evaluated to determine if the corrective actions have been successful

There are eight components in the Corrective Action Program, as follows:

- (1) Develop a problem statement that states the problem and identifies its impact
- (2) Review the past history of corrective action issues from previous evaluations and identify possible solutions to the problem
- (3) Select a corrective action strategy and prioritize the actions to be taken, as well as an associated schedule for completion
- (4) Provide authority and resources to the individual assigned to implementation so that the designated change can be accomplished
- (5) Identify the resources required to implement the strategy